RFID – present & future

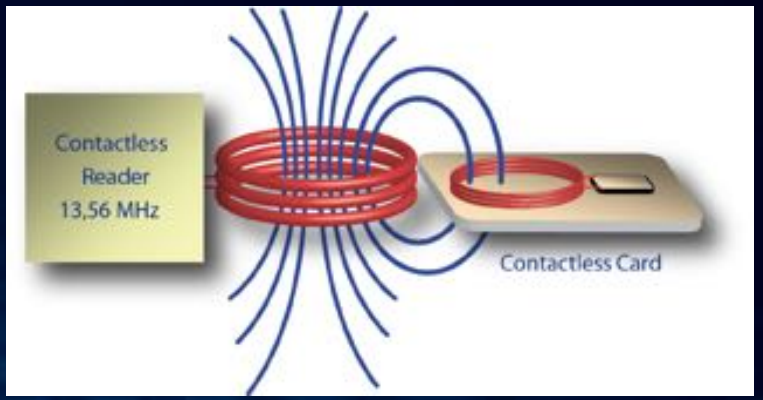
Marc Heijligers
2 maart 2015

What is RF-ID?

What is RFID (Radio Frequency IDentification)?

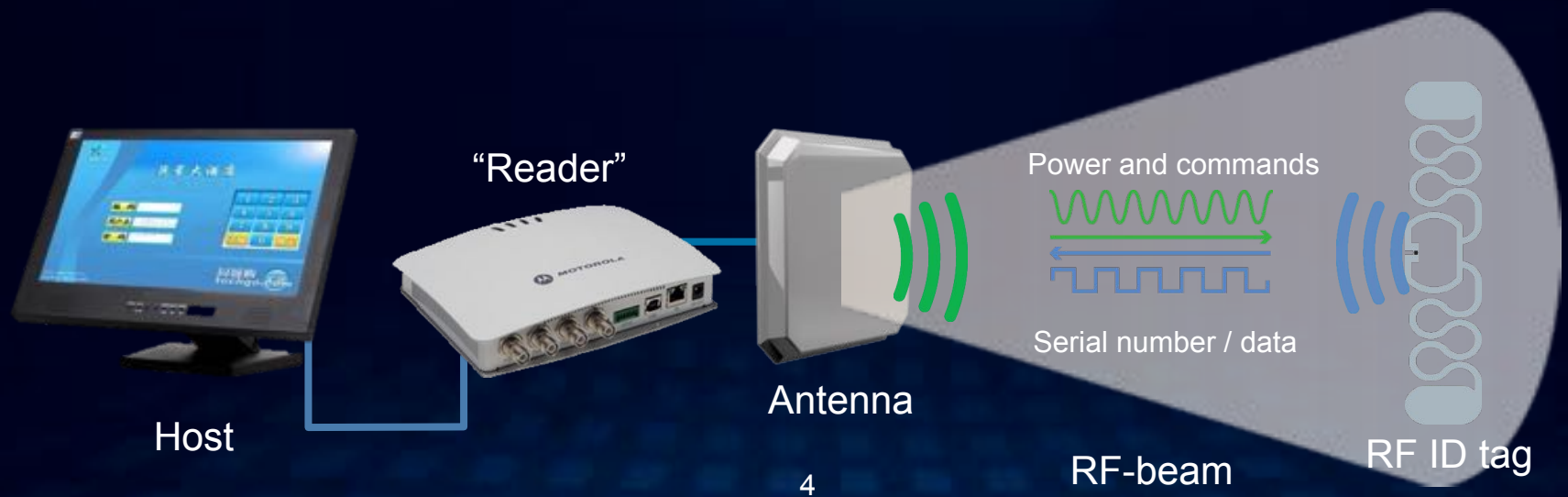
- Like a wireless memory stick with a unique serial number to identify items

- Passive technology
  - Tag no battery
  - “Reader” provides power to the tag
  - Tag “harvests” power from the RF “beam”



RFID communication

- “Reader” (interrogator) requests for data
- Energized tag responds with data
- “Reader” passes data on to a host



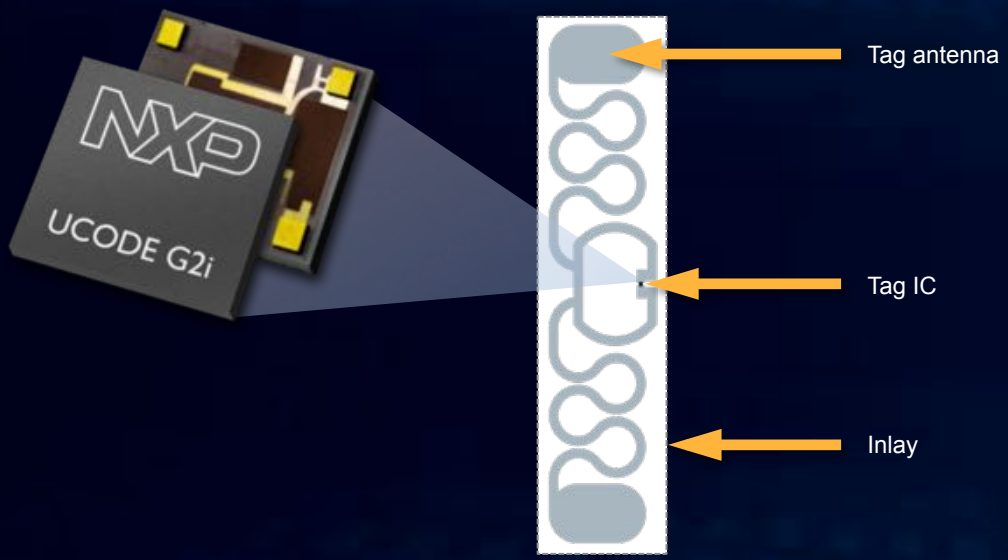
RFID compared to other communication standards

Table 1 Wireless connectivity tradeoffs

	WiFi	ZigBee (802.15.4)	Bluetooth	NFC
Network topology	Star	Mesh	Point-to-point	Point-to-point
Range	30-100 m	10-20 m	10 m	< 0.1 m
Discovery	Broadcast	Broadcast	Broadcast	Response to field
Power	High	Low	Classic: Mid LE/Smart: Low	Tag: Zero Reader: Very low
Privacy	Low	Mid	Mid	High

(*) NFC = RFID with P2P communication

RF ID tag anatomy



Tag IC

The heart of the tag – the RFID silicon chip

Tag antenna

Antenna pattern on a substrate

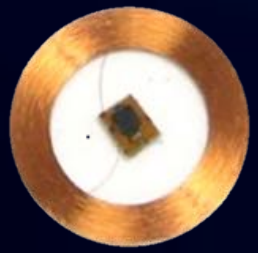
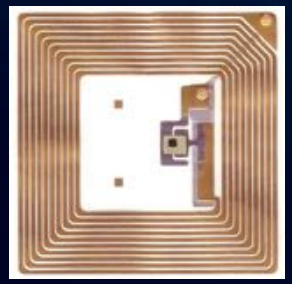
Inlay

An antenna with an IC attached

A functional RFID transponder in the most rudimentary state

Different kinds of RFID

- Three primary frequencies

Low Frequency (LF)	High Frequency (HF)	Ultra High Frequency (UHF)
~134,2 kHz	~13,56 MHz	~433 MHz
		

- Various implementations
  - Smart Card
  - Labels & Tags
  - Mobile Devices

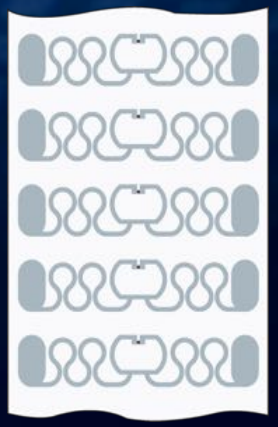
Inlay conversion

- **Dry Inlay**
  - Continuous roll of un-singulated antennas + ICs.
  - Generally reserved only for converter partners.

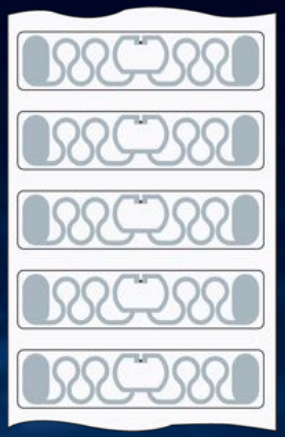
- **Wet Inlay**
  - Singulating the dry inlay and adding an adhesive to the back for an easy “peel and stick” solution.

- **Tags**
  - Singulated, typically not in label format, but rather embedded in a protective encapsulated. Generally reserved for non-disposable applications.

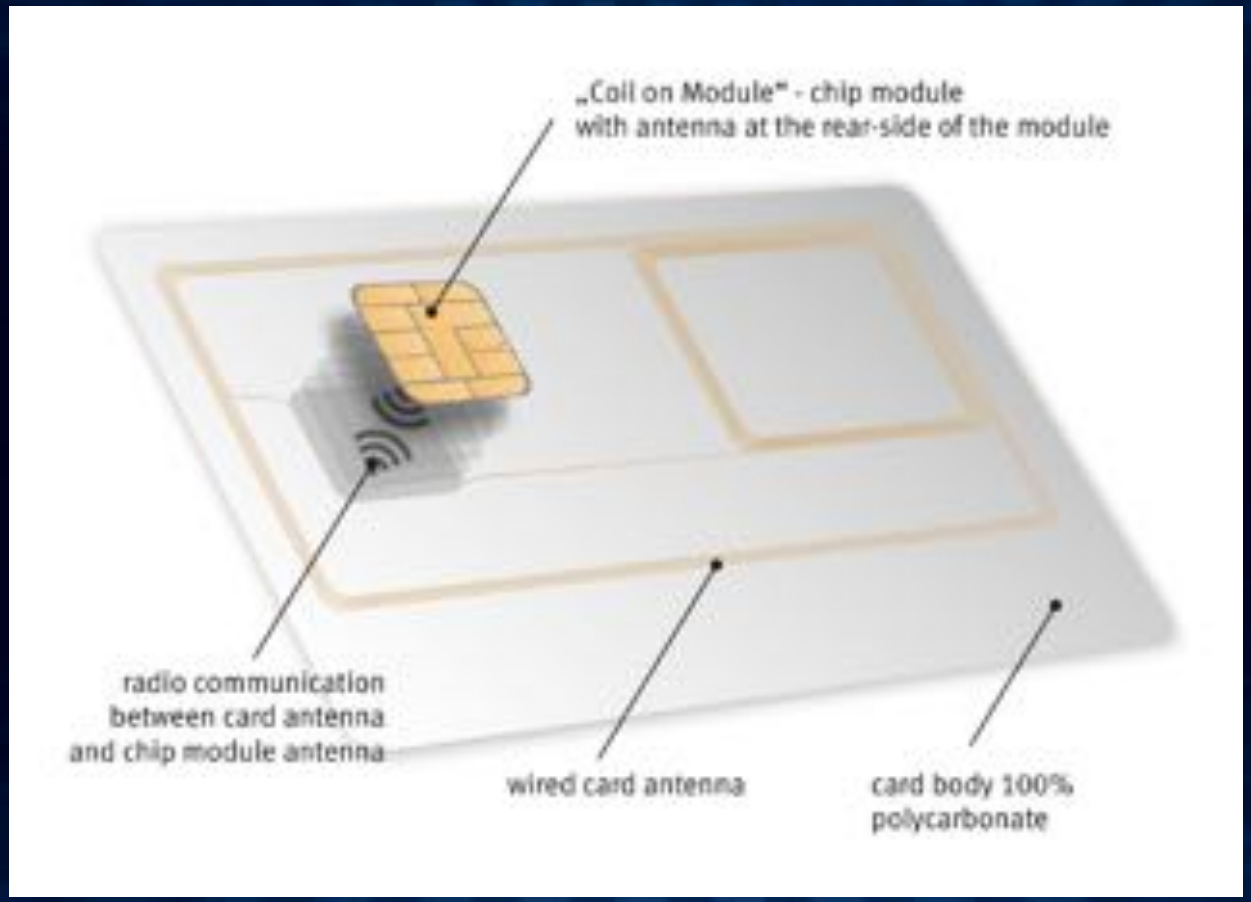
Dry Inlay



Wet Inlay



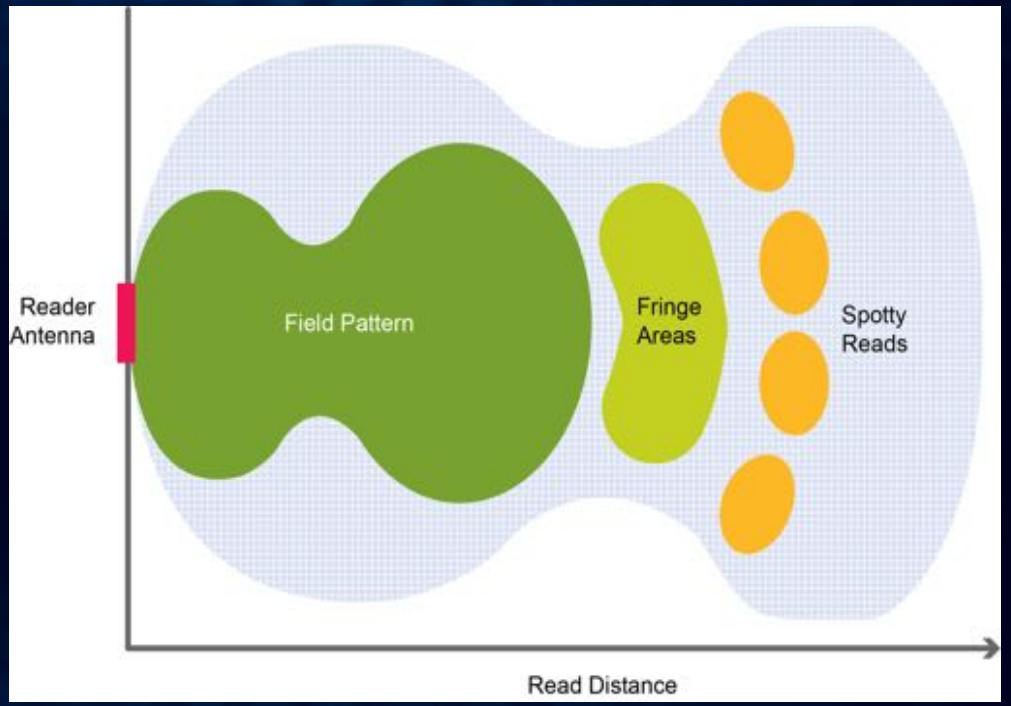
RFID card


„Coil on Module" - chip module
with antenna at the rear-side of the module
radio communication
between card antenna
and chip module antenna
wired card antenna
card body 100%
polycarbonate

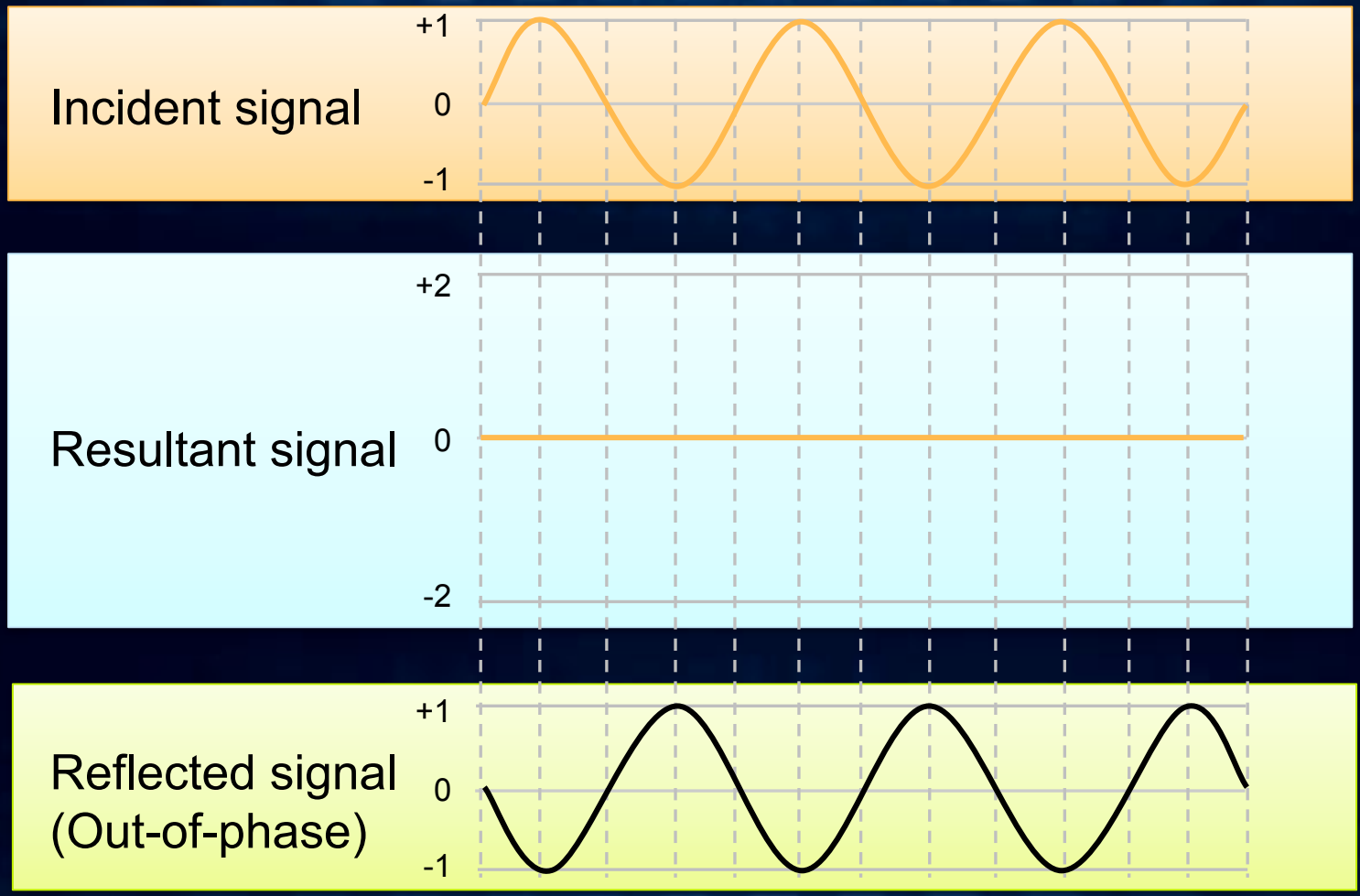
RFID design challenges

Typical UHF read field

- Field may be long and wide, but there are nulls and weaker read zones, depending upon:
  - Environmental surroundings
  - Tag orientation and height
  - Reader antenna type and height
  - Distance from tag to antenna
  - Etc.
- Movement of tags helps
- Frequency hopping assists with nulls

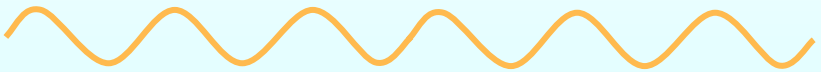


Out-of-phase reflections



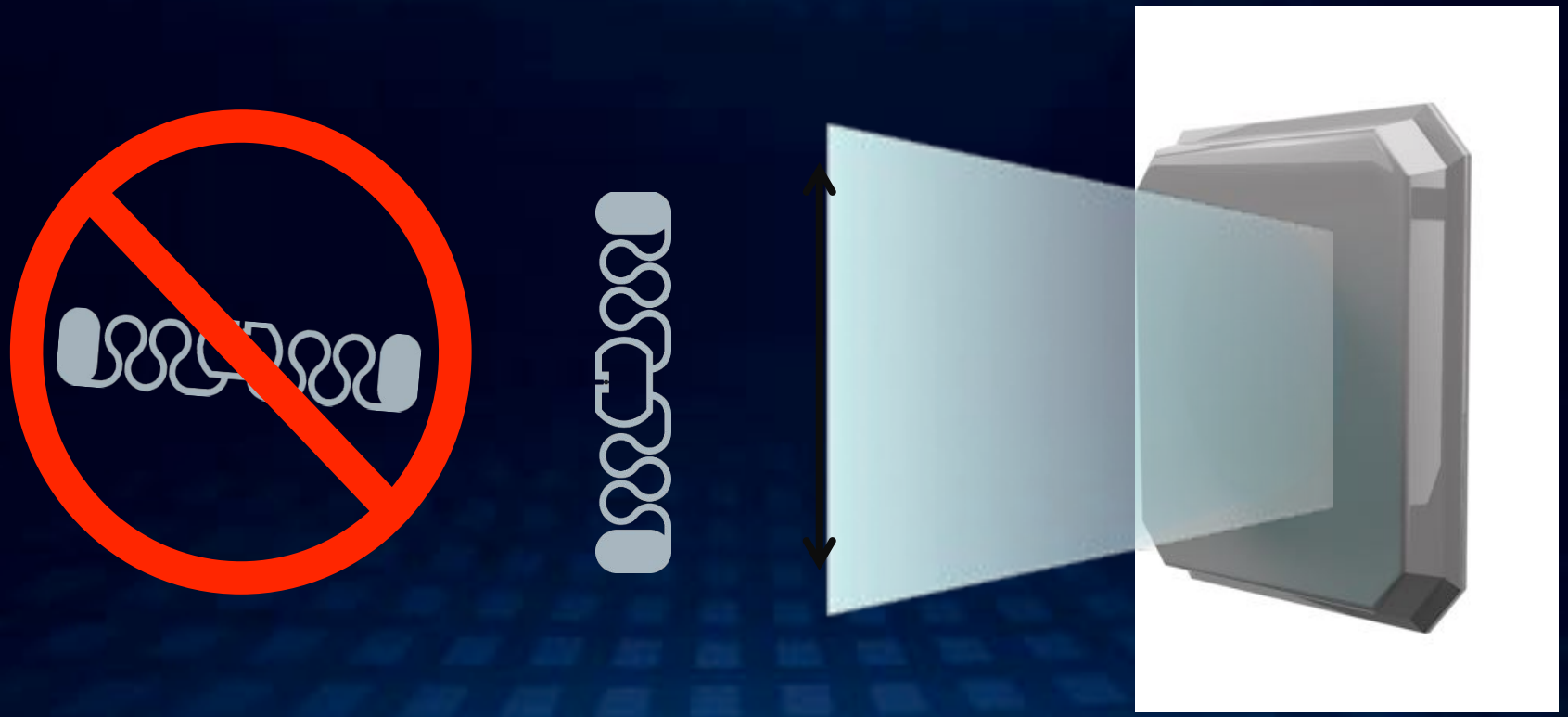
Frequency hopping

- Frequency hopping helps alleviate nulls
- At certain distances from the reader, a tag could be in a null at a certain frequency
- But as the wavelength changes, the null position “moves”
- This often helps resolve nulls

Frequency	Full wavelength (Inches)	Relative frequency	Sample waveform (depicting 6 cycles each) (nulls vary with frequency)
902 MHz	13.09	Slower	
915 MHz	12.90		
928 MHz	12.72	Faster	

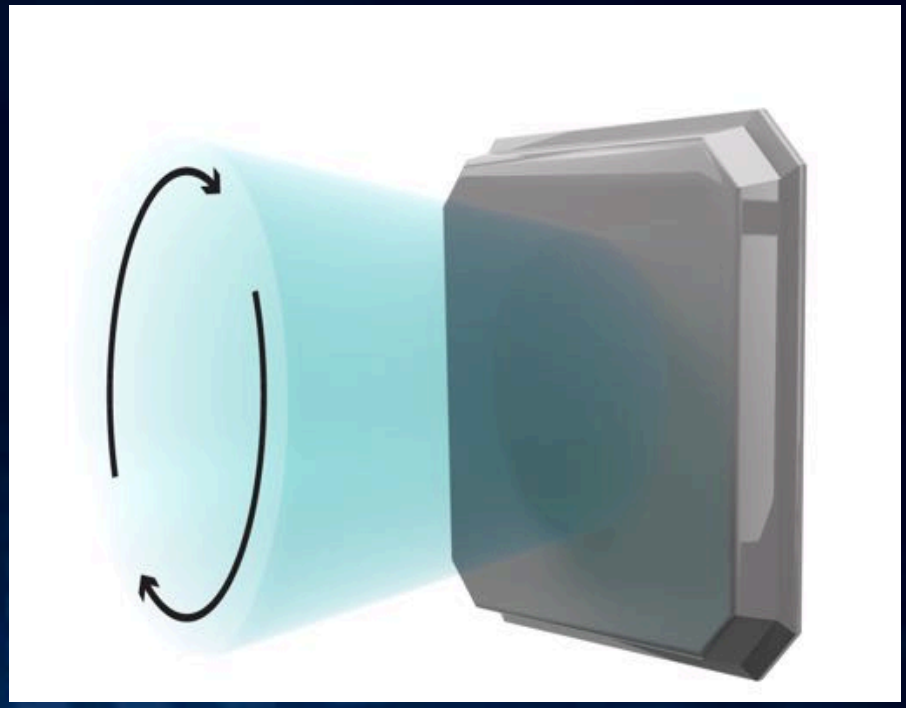
Linearly polarized antennas

- RF energy radiates from antenna in a linear pattern
- Field is concentrated in one primary orientation



Circular polarized antennas

- RF energy radiates from antenna in a circular pattern
- Designed to increase signal reception in presence of multi-path and high scattering
- More tag orientation insensitivity



Material considerations






RF-lucent materials

- RF energy penetrates relatively easily
  - Paper, most plastics, cloth, cardboard

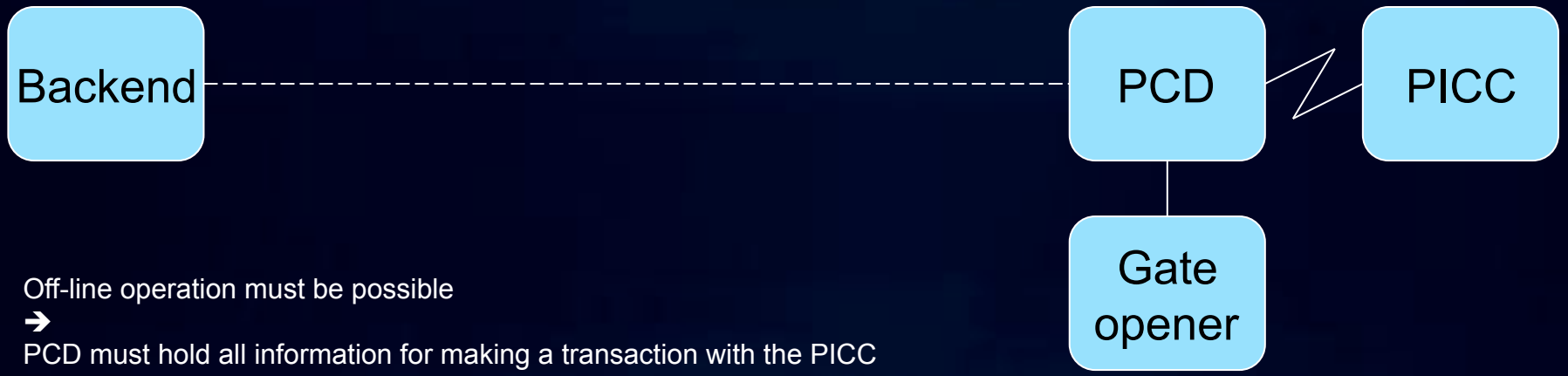
RF-opaque materials

- Conductive materials
  - Block or reflect RF energy
  - Metal, metallized plastic / paper, some liquids, pastes, carbon-impregnated plastic (black), conductive plastics, foil lined packaging
- Absorptive materials
  - Weaken RF energy
  - Most liquids & moist fibers (e.g. green wood, moist wipes, damp paper)

RFID → Secure ID

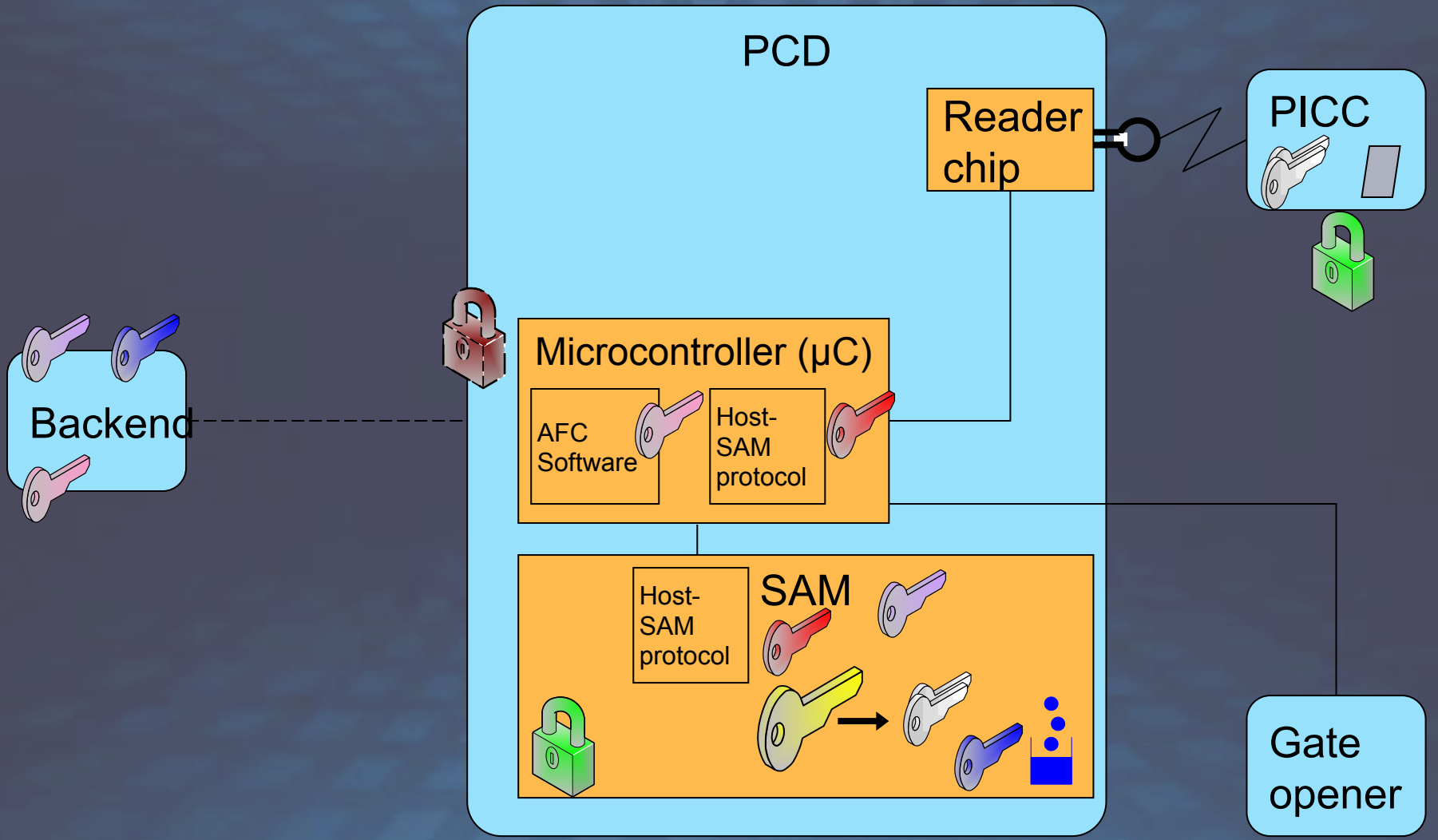
Generalized AFC architecture

PICC = Proximity Integrated Circuit Card = Contactless Card
PCD = Proximity Coupling Device = Reader device = Terminal



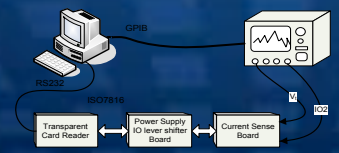
Off-line operation must be possible
➔
PCD must hold all information for making a transaction with the PICC

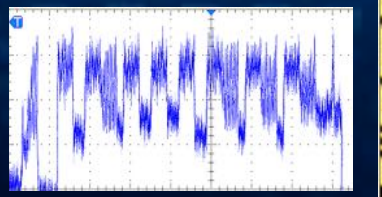
Keys and encryption

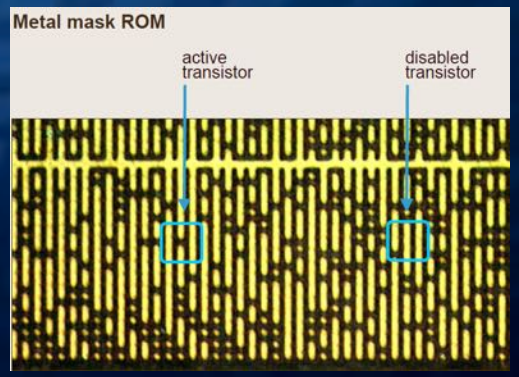


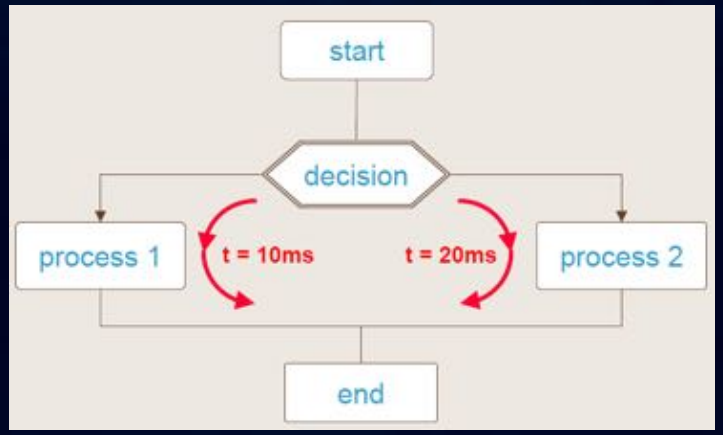
Security threats

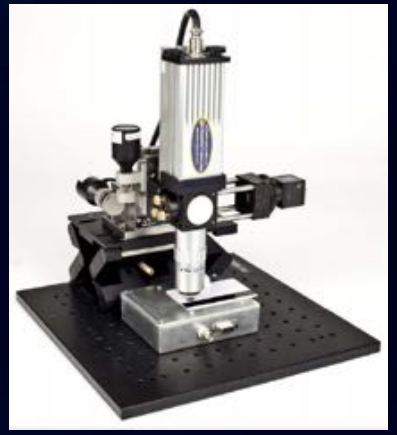
- Side channel leakage
  - Timing analysis
  - Simple power analysis
  - Differential power analysis
  - Electro-magnetic emission
- Fault injection attacks
  - Light attacks
  - Glitch attacks
  - Physical manipulation
- Reverse engineering
- Probing

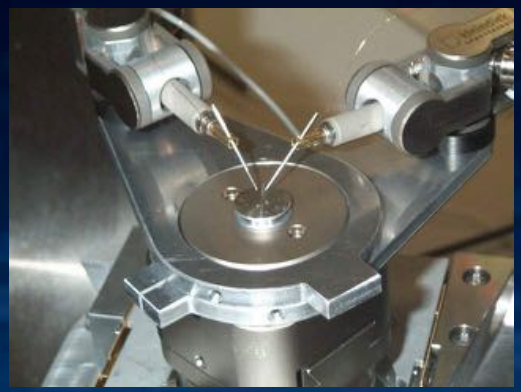


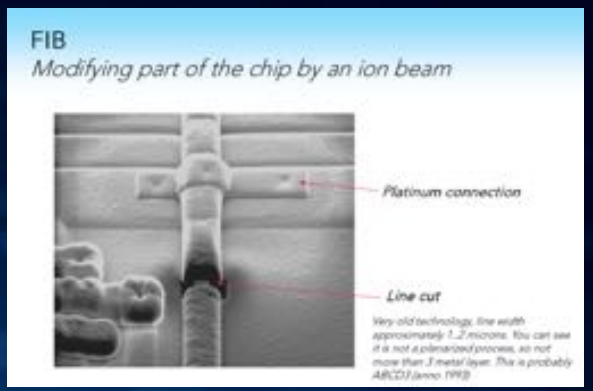




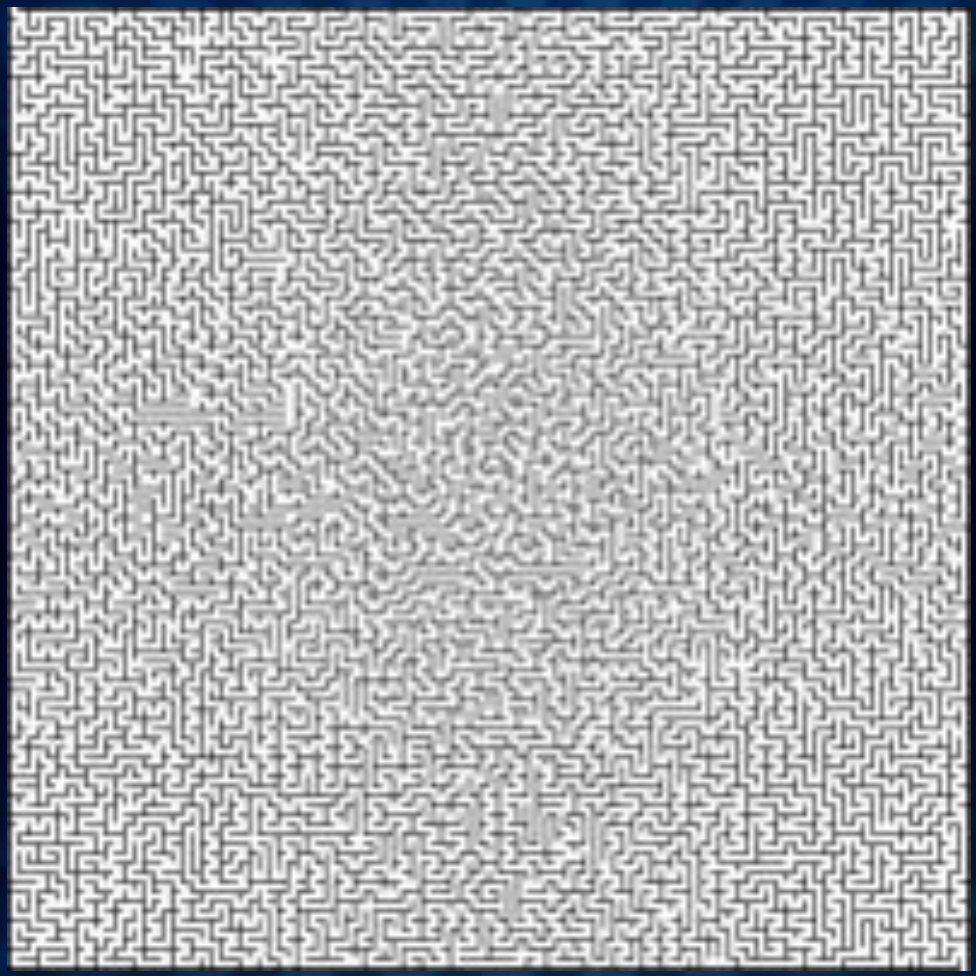








Passive Shield



Security by obscurity

Active Shield Example

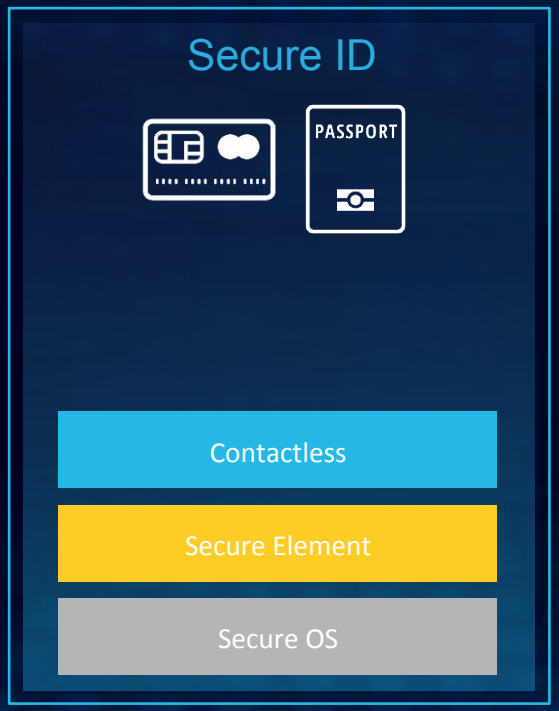
Mesh based active shield

Pictures courtesy of www.flylogic.net

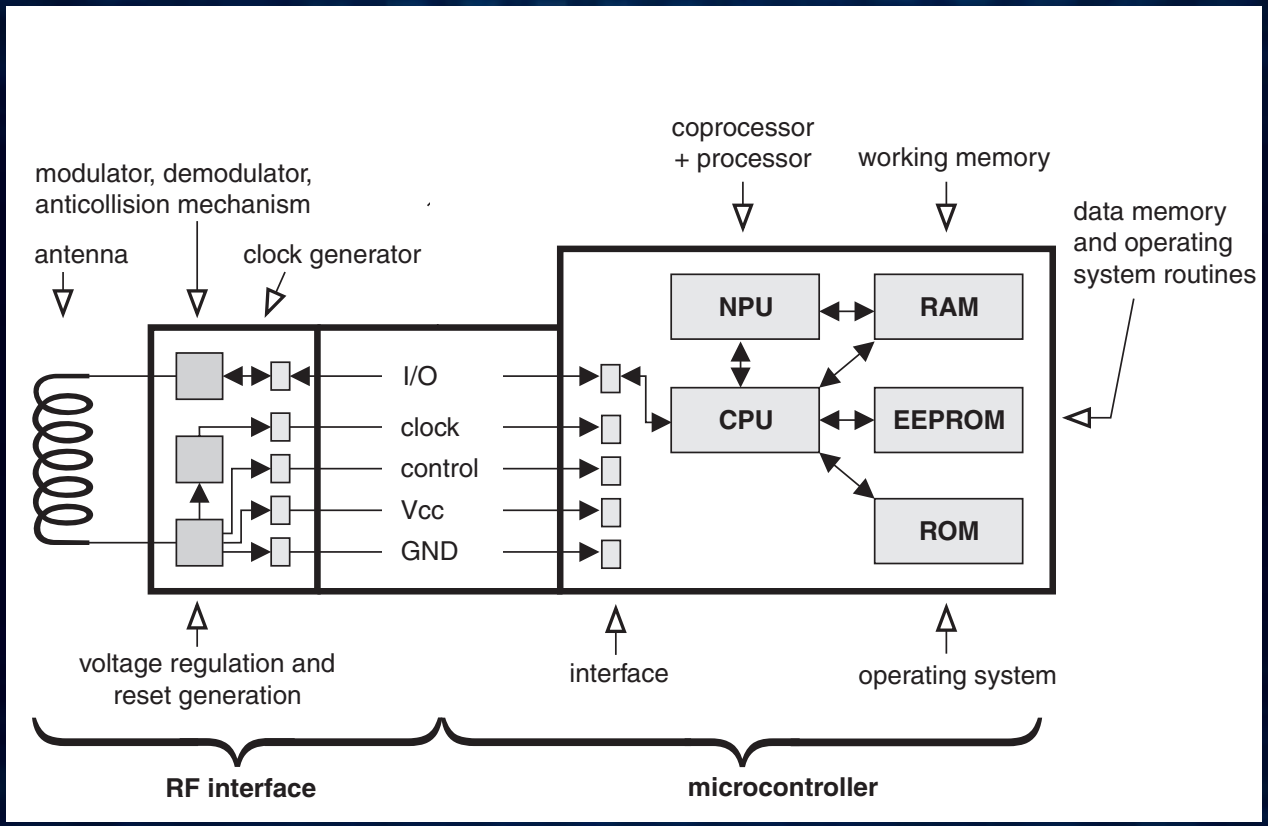
Sensors

- Light Sensors
  - Recognition of light (e.g. laser) attacks
  - Can be replaced by plain circuitry
- Voltage Sensors (a.k.a. rail sensors)
  - Detects over- voltage or under-voltage of power glitch attacks.
- Spike Sensors
  - Detect attacks on power lines.

From RF-ID to Secure ID → Secure Element

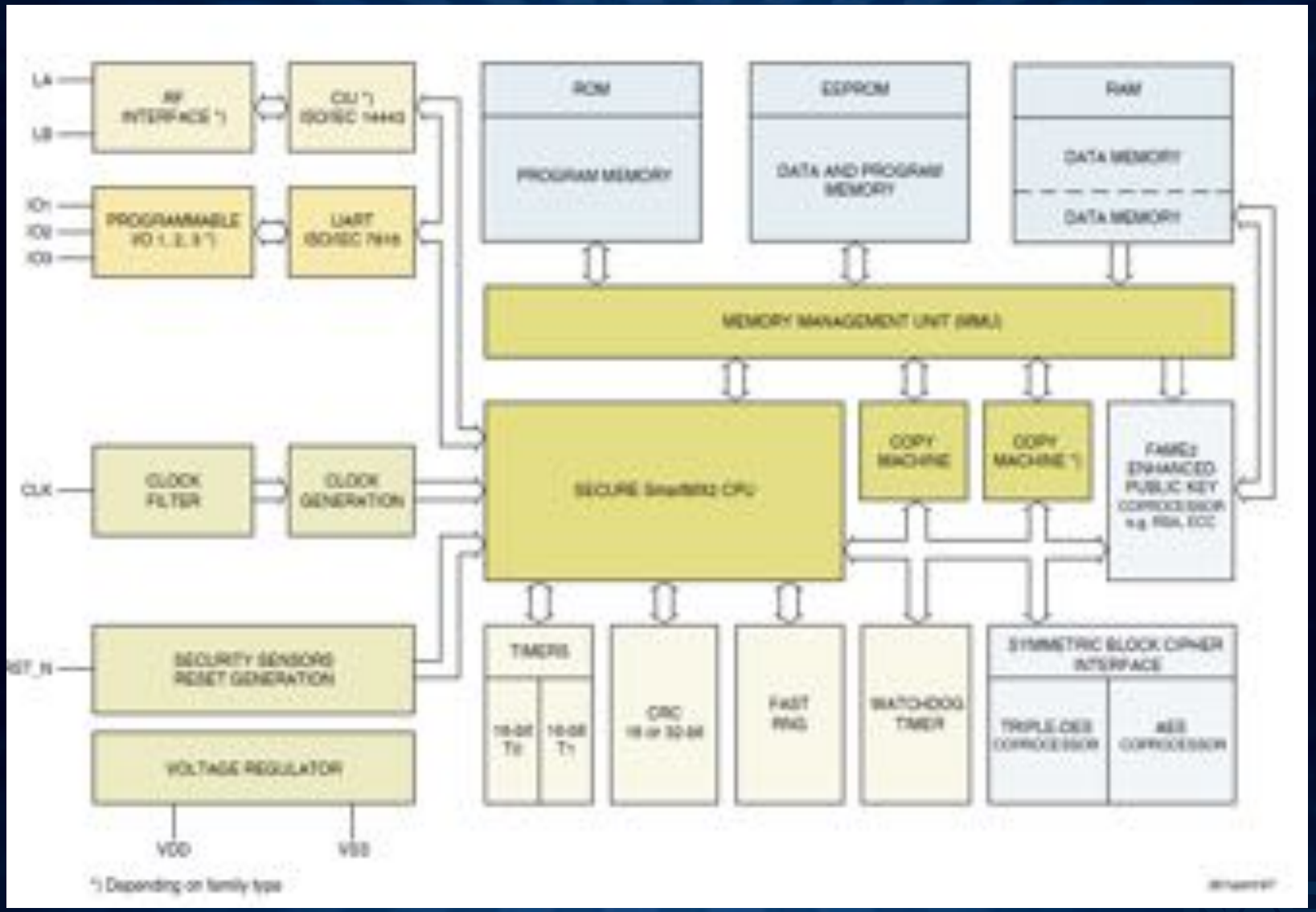


From RF-ID to Secure ID

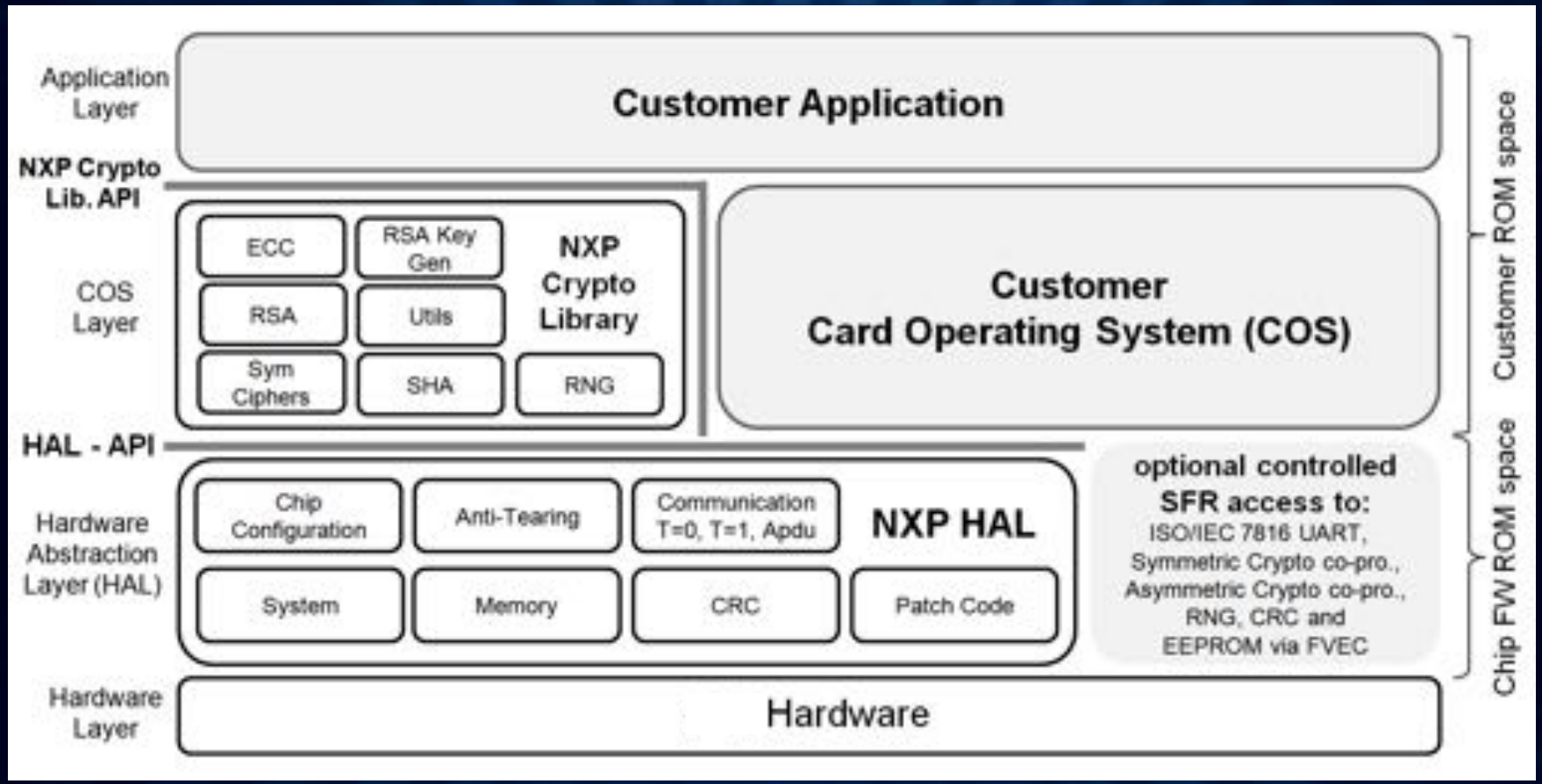


From: Wolfgang Rankl - Smart Card Handbook

From RF-ID to Secure ID – SmartMX2



From RF-ID to Secure ID



Enabling many applications

Digitization of Documents

government + healthcare ID cards going digital

* Assumes 1/4" thick passport stacked

Urbanization & Smart Cities

50% in urban centers

67% in urban centers

Sources: Population Reference Bureau, United Nations

Banking System Security

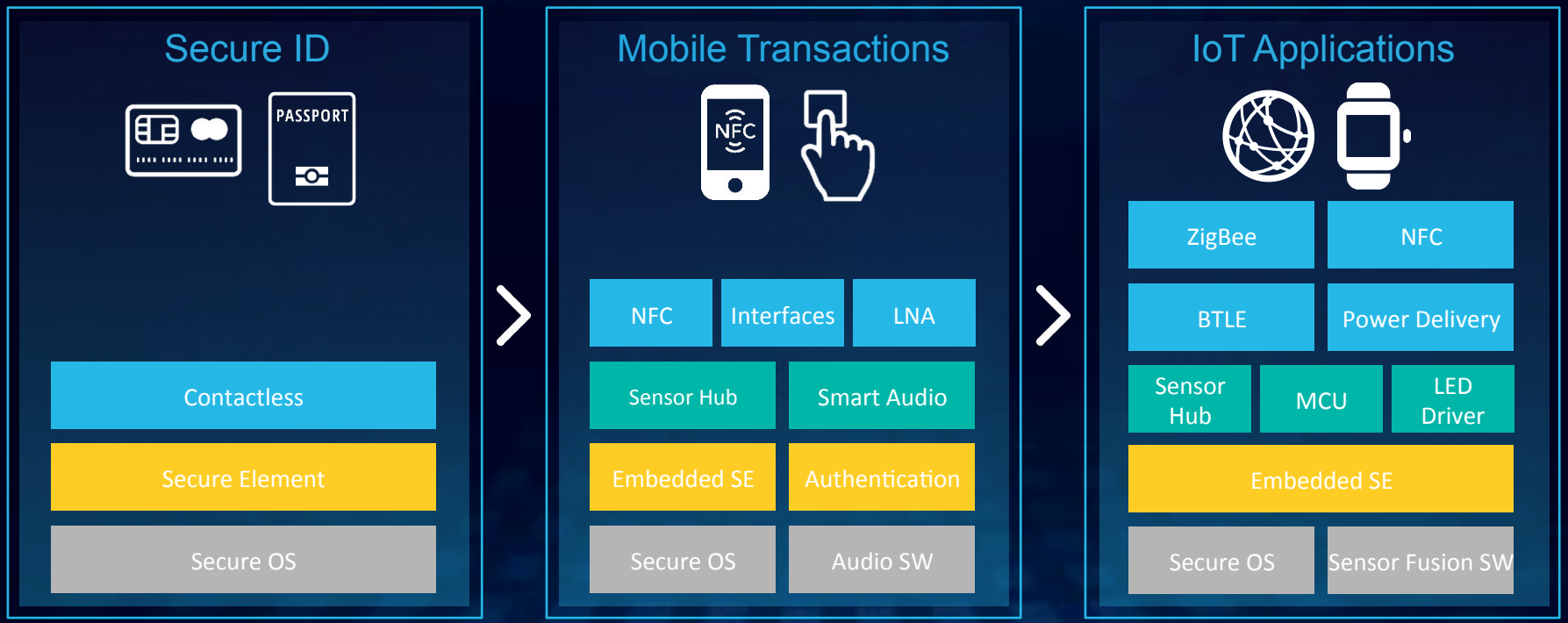
Smart Phone Adoption

China, India, and Brazil in top five for smartphone shipments by 2016

Source: Gartner (Oct 2011)

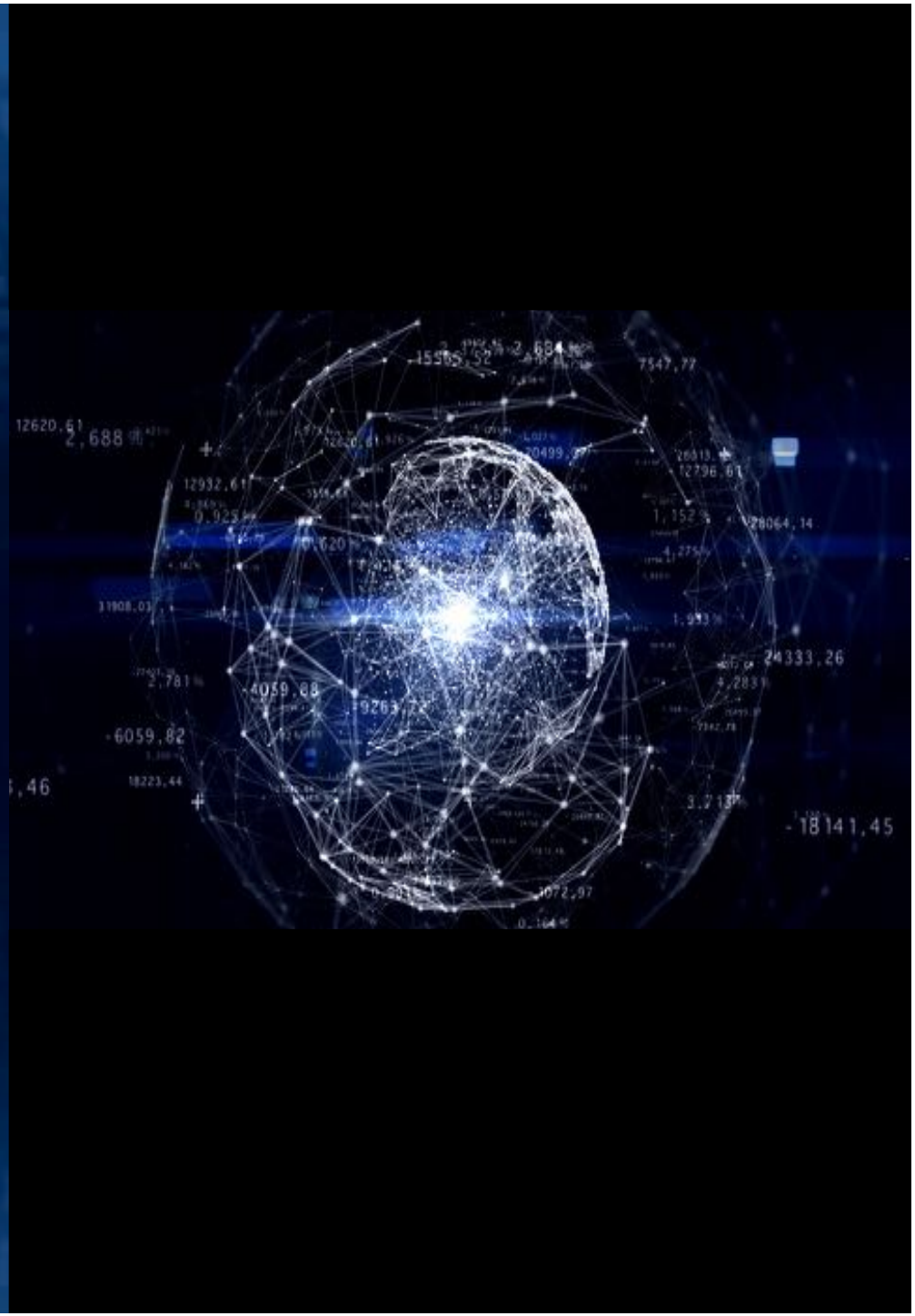
RFID future

Scale from Secure ID to Connected Devices



Security challenges of the IoT

- The Internet of Things is facing major security challenges
- Connected Systems are increasingly prone to Security Threats
- This exposes device manufacturers and infrastructure owners to high financial risks and reputational damages



Internet of Things …Needs enhanced security

Beckstrom's Laws of Cyber Security*

1. Everything that is connected to the Internet can be hacked
2. Everything is being connected to the Internet
3. Everything else follows from the first two laws

*Rod Beckstrom, CEO and President of ICANN, former Director of the National Cyber Security Center

IoT application areas

■ Security ■ Connectivity ■ Sensing / Control

RFID for retail market

Those retailers have something in common…

…they have

- …all sizes and colors of the portfolio available on the shelf.
- …customers that find what they look for
- They manage store inventory with RFID

How does RFID help ?

- Shop inventory management is traditionally done by database model.
  - Reported received products minus reported sold products results in anticipated store inventory " ..,the system says this product should be in the store…"
  - This method contains many sources of errors
    - Wrong deliveries due to picking errors of the supplier
    - Employee theft (in store and along the supply chain)
    - Customer theft
    - Product should be on shelf but stays in back room (NOSBOS)
    - Misplaced product – it is somewhere in the store, but location is unknown
- Frequent store inventory counts (Weekly, Bi-Weekly) are solving this problem.
  - With RFID labels and scanners, inventory counts becomes affordable
  - Barcode scanners: One person can only scan max **400** items per hour
  - RFID Readers : One Person scans max **19000** items per hour

How does RFID help ?

Fast Inventory Check in store

RFID Antennas check what leaves the store

Distribution Center:
Automated income inspection

How does RFID help ?

Best In Class RFID Solutions - Motorola and NXP_DVD.wmv

Thank you!