This lecture is being recorded

18-452/18-750
Wireless Networks and Applications
Lecture 22: RFID and NFC

Peter Steenkiste

CS and ECE, Carnegie Mellon University

Spring Semester 2022

http://www.cs.cmu.edu/~prs/wirelessS22/

Announcements

- I have added the survey schedule to the web page
  - Slots will be 18 minutes long - talks should be 15 minutes
  - For these two lectures, we will need the full length of the lecture time slot
  - Note that the material presented as part of the surveys is part of the syllabus
- I will post requirements for P2 CP1 on piazza

Some Thoughts about Surveys

- **Outline generally looks like:**
  - **Background: why useful, challenges, design options, etc.**
  - **Discussion on the three papers:**
    - **What is the key idea – this should be clear (figure!)**
    - **Some sample results illustrating benefits**
    - **Do not use terminology specific to the paper**
  - **Personal opinion on pros or cons (global or per paper)**
- **Many students use the google templates – that is fine but do it wisely!**
- **Common problems (24 pt)**
  - **No slide numbers**
  - **Tiny font sizes (12pt) – you want it to be bigger! (18pt)**
  - **50%-80% of the slide is empty - use the space wisely!**

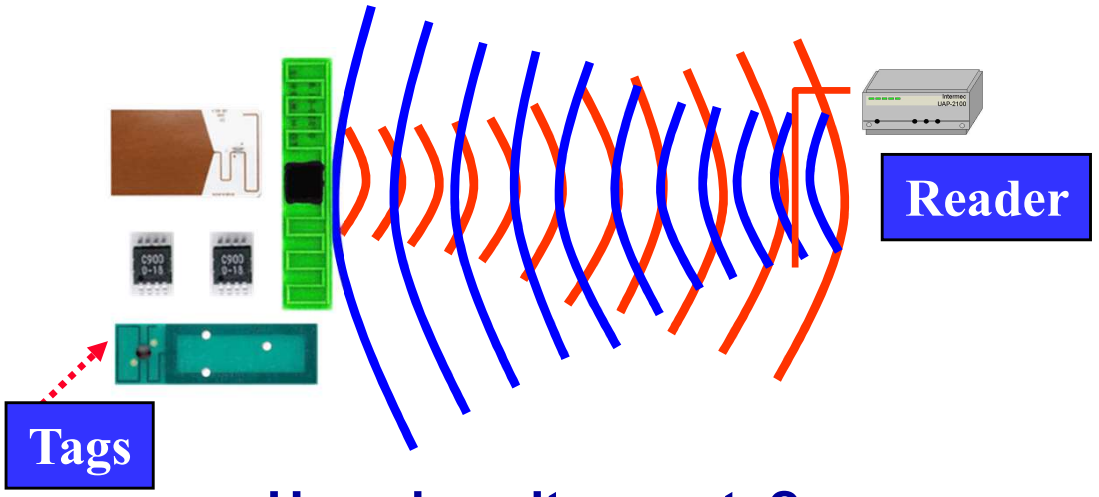
Outline

- **RFIDs**
  - **Concept and applications**
  - **EPC and backend processing**
  - **PHY and MAC**
  - **Security**
- **Near Field Communication**
- **Battery-less devices**

What is RFID ?

- Radio Frequency IDentification (RFID) is a method of remotely storing and retrieving data using devices called RFID tags and RFID Readers
- An enabling technology with many applications
  - Data can be stored and retrieved from the tag automatically with a Reader
  - Tags can be read in bulk
  - Tags can be read without line of sight restrictions
  - Tags can be write once read many (WORM) or rewritable
  - Tags can require Reader authentication before exchanging data
  - Other sensors can be combined with RFID
- Technology has been around for a long time
- Also has critics, e.g. privacy concerns

How Does It Work?



How does it operate?

- RFID tags are affixed to objects and stored information may be written and rewritten to an embedded chip in the tag
- Tags can be read remotely when they receive a radio frequency signal from a reader and use the energy to respond
- Can operate over a range of distances
- Readers display tag information or send it over the network to back-end systems

What is RFID?

- A means of identifying a unique object or person using a radio frequency transmission
- Tags (or transponders) store information, that can be retrieved wirelessly in an automated fashion
- Readers (or interrogators), either stationary and hand-held, can read/write information from/to the tags

Applications

- **Operational Efficiencies**
  - Shipping and Receiving
  - Warehouse management
  - Distribution
  - Asset management
- **Total Supply Chain Visibility**
  - Inventory visibility in warehouses
  - In-transit visibility, asset tracking
  - Pallet, case level
  - Item, instance level
- **Shrinkage, counterfeit**
  - Reduce internal theft
  - Reduce process errors
  - Avoid defensive merchandizing
  - Product verification
  - Origin, transit verification
- **Security, Regulations**
  - Total asset tracking
  - Defense supplies
  - Container tampering
  - Animal Tracking

Automated Identification Technology Suite

Linear Bar Code

CMB
Contact Memory Button

2D Symbol
QR Code

Smart Card/CAC

OMC
Optical Memory Card

RFID - Active
Radio Frequency ID

STS

Satellite-Tracking Systems

RFID- Passive
Radio Frequency ID

RF ID Types

- **Passive Tags: rely on an external energy source to transmit**
  - » In the form of a reader that transmits energy
  - » Relative short range
  - » Very cheap
- **Active Tags: have a battery to transmit**
  - » Has longer transmission range
  - » Can initiate transmissions and transmit more information
  - » A bit more like a sensor
- **Battery Assisted Passive tags are a hybrid**
  - » Have a battery transmit
  - » But need to be woken up by an external source

A Bit of History

- **Early technology was developed in the 40s**
  - » Originally used as eaves dropping devices
  - » Used reflected power to transmit (transponder), e.g. the membrane of a microphone
- **First RF IDs were developed in the 70s**
  - » Transmission based on reflected energy using information in memory – readers can now distinguish devices
- **Dramatic growth since then driven by industry**
  - » Potential for significant gains in areas
  - » Big organizations (DOD, Walmart) requiring the use of RFIDs from their vendors for easy inventory control
- **Set of applications expanded rapidly**

Standards

- Passive tags operate in the LF, HF, and UHF unlicensed spectrum
  - 30-300 KHz, 3-30 MHz, 300-3000 MHz
  - Distance drop with frequency
- Transmission consists of a bit stream and CRC
- Many standards exist, mostly incompatible
  - » Early standards mostly defined by the ISO
  - » Widely used standard: ISO/IEC14443
- In 2003 EPCGlobal was formed to promote RFID standards
  - » Defined a standard for the Electronic Product Code (EPC)
  - » Also defined standards for coding and modulation

Primary Application Types

Identification and Localization

- **Readers monitoring entering and exiting a closed region**
  - » **Security (RFID in identification cards)**
  - » **Merchandise in stores**
  - » **NFC in phones**
- **Readers tracking an RFID-tagged object**
  - » **Business process monitoring (RFID tags on pallets)**
- **Tags marking a spatial location**
  - » **An NFC enabled mobile phone passes tags in the infrastructure whose location is known**

Example: Smart Card

Public transport system in Singapore

- **FeliCa Smart Card**
- **2001 – 2009**
- **Faster boarding times**
- **Other uses**
  - **small payments retail**
  - **identification**
- **Replaced by contactless card (RFID)**

How Smart are RFIDs?

- Basic tags simply reply with a fixed bit string – "read" the tag
  - » "I am Groot"
  - » Already useful!
- Gradual move to richer functionality
  - » Changing the state on the tag – "write"
    - – E.g., keep track of a balance
  - » Privacy and security: encryption, access control, …
    - – E.g., different parties and read and write the tag
  - » Add computing capabilities (more general than crypto)
- Next step is processors that operate entirely based on harvested ambient energy
  - » Vibrations, RF, solar, …

Example "Oyster" Card

- Balance is maintained on the card
  - » Cryptographically secured
- The "reader" updates the balance as you enter/leave the metro station
  - » Enter: record when and where you boarded
  - » Leave: update balance on the card
  - » These operations are local
- Readers record all trips and periodically send information to servers
  - » Auditing trail, lost cards, etc.
  - » Riders can check their balance online

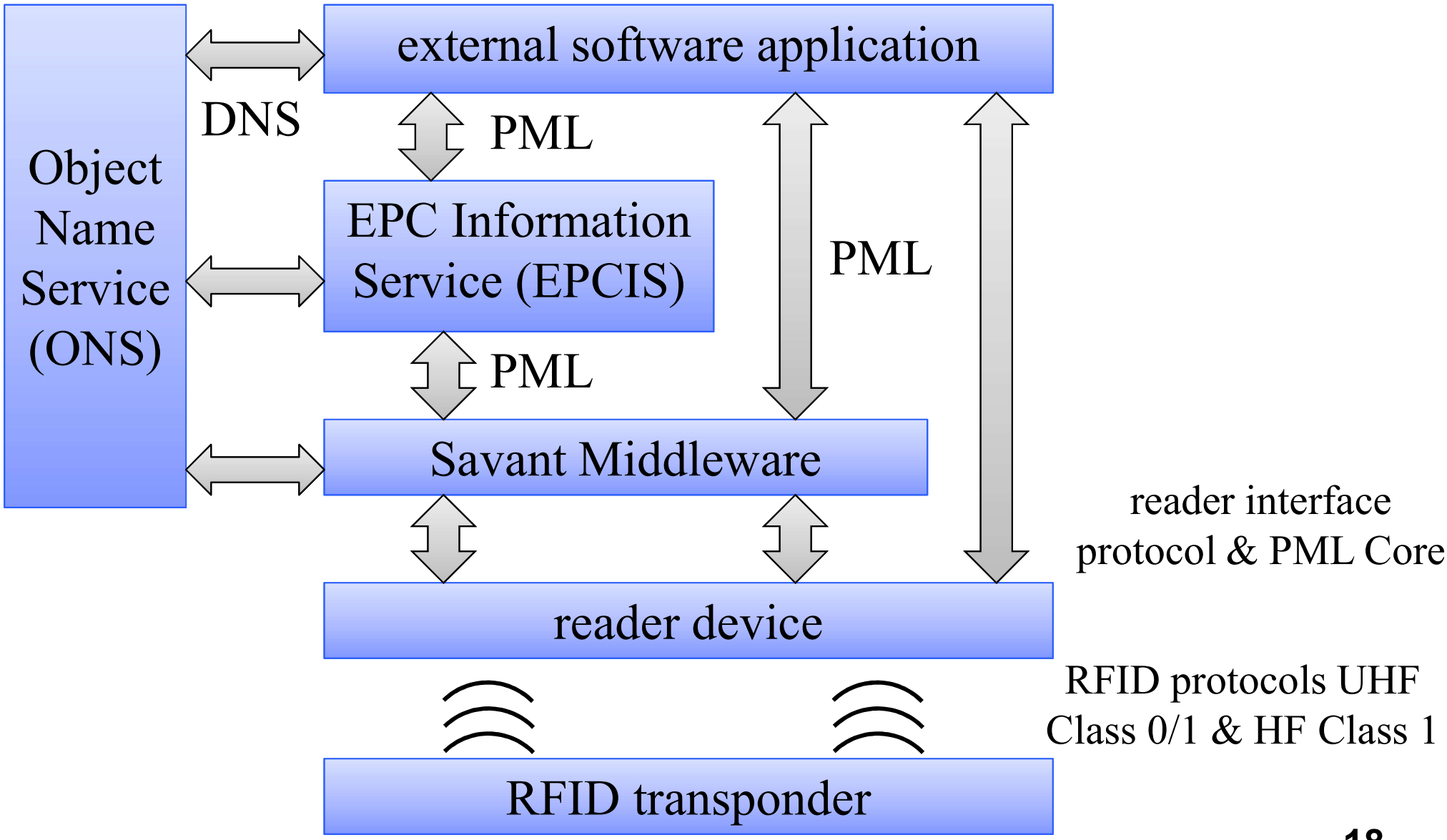
Outline

- **RFIDs**
  - **Concept and applications**
  - **EPC and backend processing**
  - **PHY and MAC**
  - **Security**
- **Near Field Communication**
- **Battery-less devices**

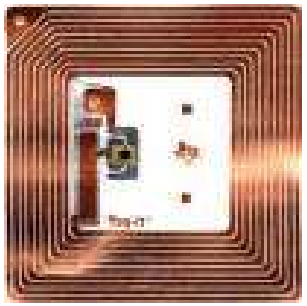
Electronic Product Code (EPC)

- "A Universal identifier for physical objects"
  - » Designed to be unique across all physical objects in the world, over all time, and across all categories of objects.
  - » Intended for use by business applications that need to track all diverse physical objects, whatever they may be.
  - » urn:epc:id:sgtin:0614141.012345.6285210cc Syringe #62852 (trade item)
- Combined multiple components
  - » EPC data located on the RFID tag
  - » Reader's middleware
  - » Locate EPC Information Services (EPCIS), using Web Services like SOAP and WSDL
- Not exciting but standardization is critical to wide-spread adoption

EPC Network Concept (2001)



What information does an RFID tag contain?



Gen 2 tags have four memory banks

Bank 0	Bank 1	Bank 2	Bank 3
Reserved Memory •32-bit Kill Password •32-bit Access Password *(64 bits)*	EPC Memory •16-bit CRC •16-bit Protocol Control •96-bit EPC *(128 bits)*	Tag Identification Memory * •8-bit Class Identifier •12-bit Tag Designer •12-bit Tag Model Number •32-bit Serial Number (optional) *(0, 32, or 64 bits)*	User Memory * •User-defined format *(0 or more bits)*

The CBP "GDTI-96" bit unique number

A 64-bit TID memory bank contains a tag serial number that uniquely identifies a tag.

* *TID and User Memory banks are not initialized on some Gen 2 tags*

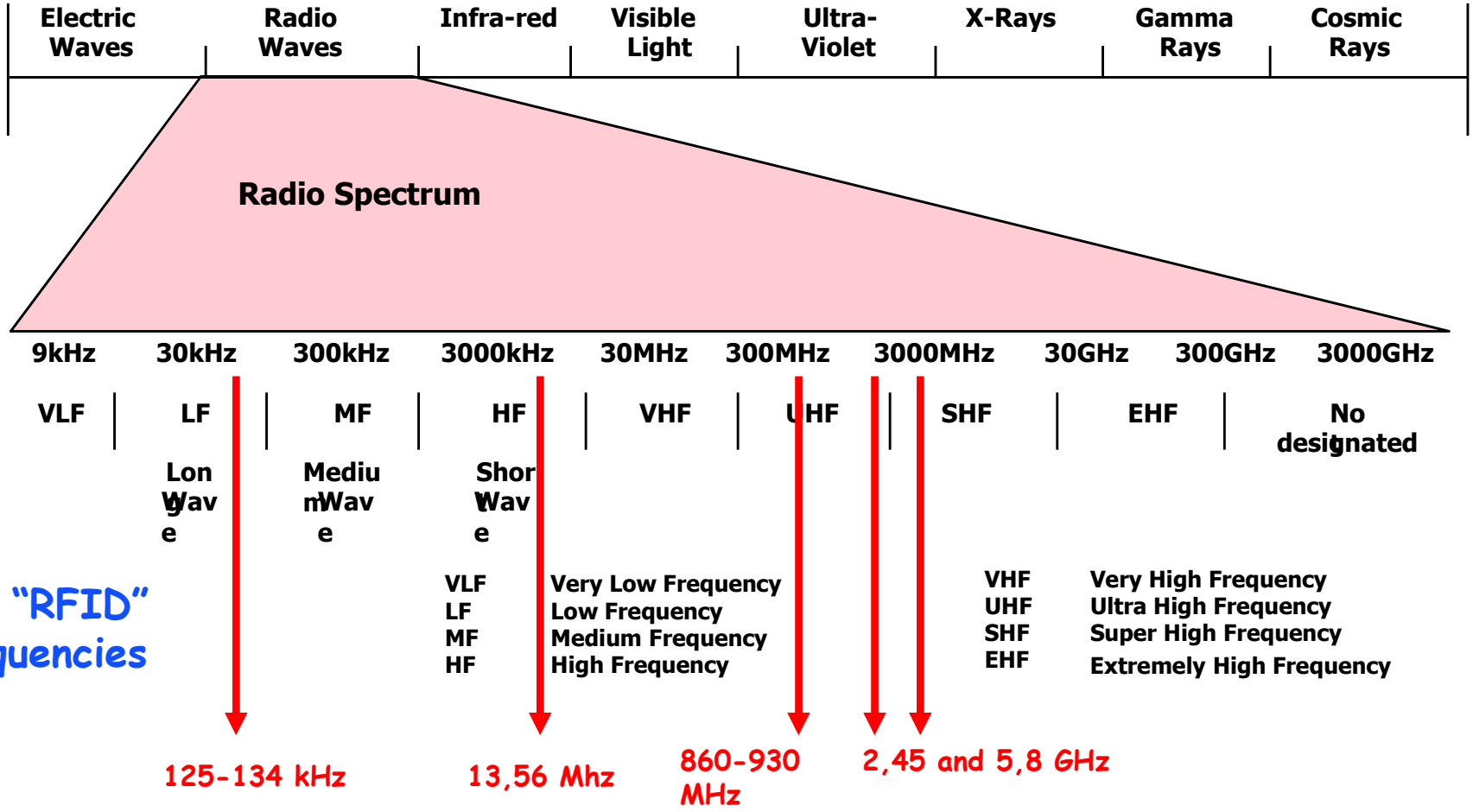
Example to illustrate concept

Passive RFID Tags

- **Power supply**
  - » passive: no on-board power source, transmission power from signal of the interrogating reader
  - » semi-passive: batteries power the circuitry during interrogation, once woken up by external signal
  - » active: batteries power transmissions (can initiate communication, ranges of 100m and more, 20$ or more)
- **Frequencies**
  - » low frequency (LF): 124kHz – 135 kHz, read range ~50cm
  - » high frequency (HF): 13.56 MHz, read range ~1m
  - » ultra high-frequency (UHF): 860 MHz – 960 MHz (some also in 2.45GHz), range > 10m

Frequency Bands
Passive RFID Tags

Electromagnetic Spectrum

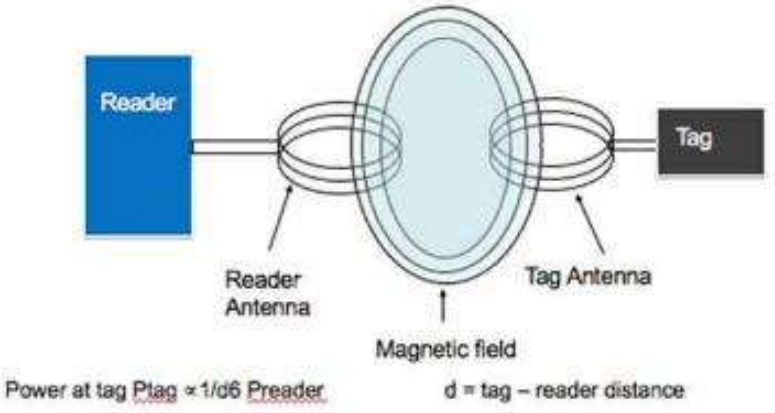


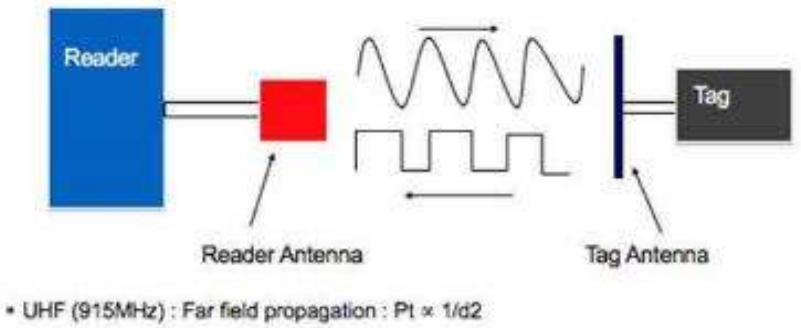
Standards

- ISO 18000: multipart standard for protocols in LF, HF, and UHF bands
- For example, HF:
  - ISO 14443 (A and B) for "proximity" RFID
  - ISO 15693 for "vicinity" RFID (basis for ISO 18000 part 3)
- Two classes:
  - Class 0: read only
  - Class 1: read/write, can for example be used for tracking
- Many more standards exist!

Transmission methods

- **LF and HF: inductive coupling**
  - » Coil in the reader antenna and a coil in the tag antenna form an electromagnetic field
  - » Tag changes the electric load on the antenna.
- **UHF: propagation coupling: backscatter**
  - » Tag gathers energy from the reader antenna
  - » Microchip uses the energy to change the load on the antenna and reflect back an altered signal
  - » Different modulations used by reader and tag

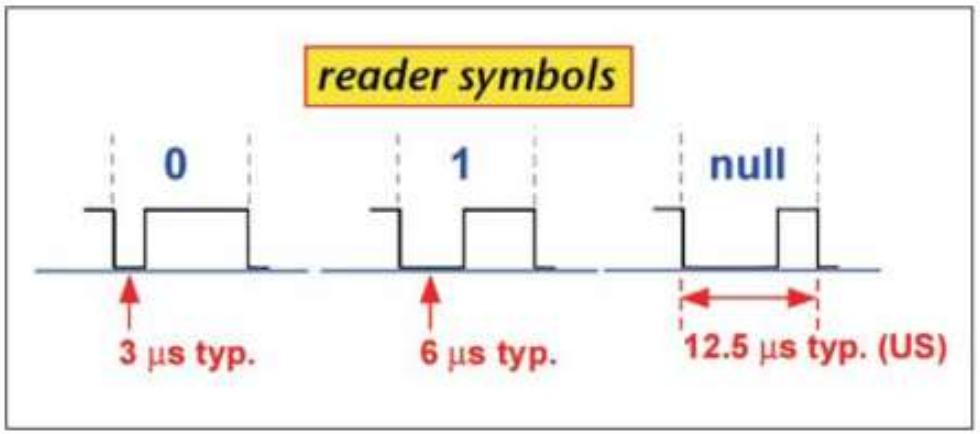


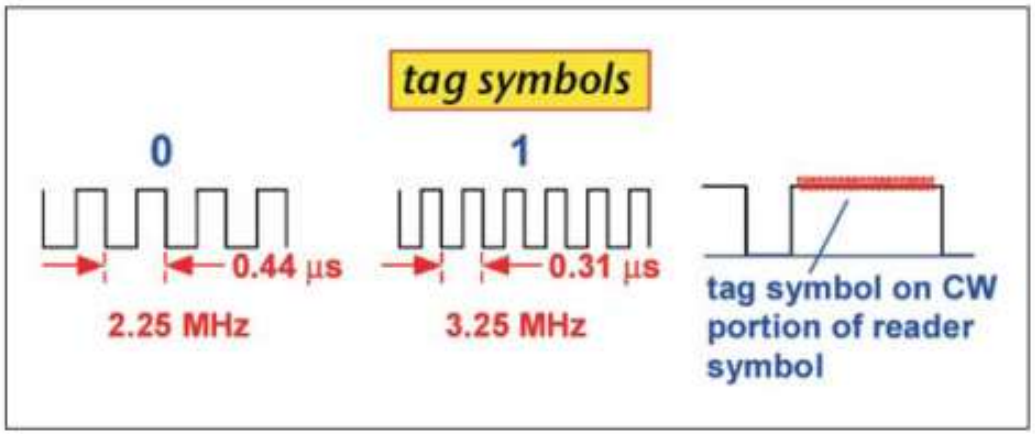


From: http://www.highfrequencyelectronics.com/Archives/Aug05/HFE0805_RFIDTutorial.pdf
https://rfid4u.com/rfid-basics-resources/inductive-and-backscatter-coupling/

PHY Layer

- Depends on the frequency band used
- Different modulations used by reader and tag
  - » Different constraints, e.g. power and complexity
  - » E.g. cannot used amplitude modulation for HF tag (why?)
- Example of EPCGlobal symbols for UHF





From: http://www.highfrequencyelectronics.com/Archives/Aug05/HFE0805_RFIDTutorial.pdf

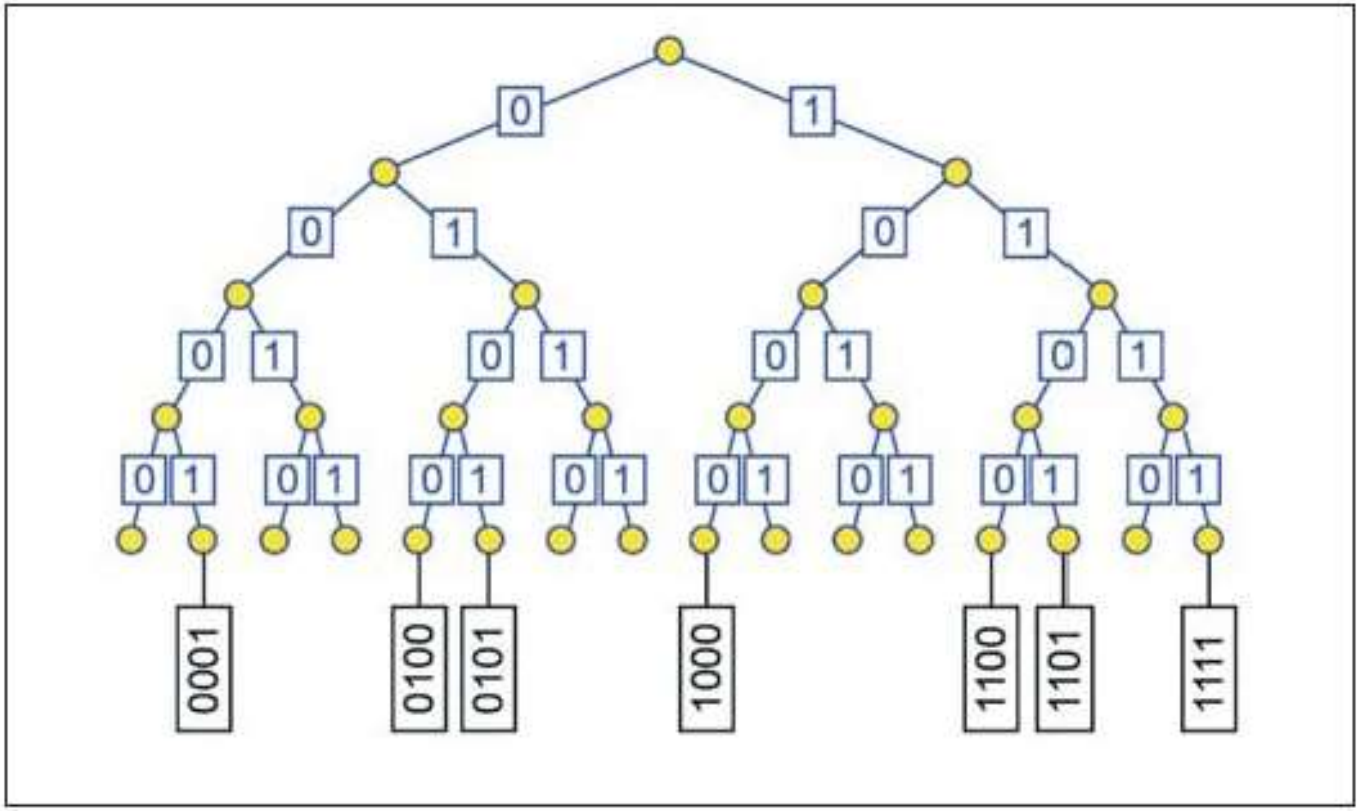
What does an RFID tag look like inside a card?

MAC Layer

- **Typically assumed that only one reader is present, i.e. no need for MAC on the reader**
  - » **Multiple readers: can use different frequency bands**
- **MAC for tags is a challenge: very high concentrations of tags are present in many contexts**
  - » **And tags are dumb, i.e. cannot have sophisticated protocols (carrier sense, RTS/CTS, ..)**
  - » **Must also deal with multiple readers operating in the same environment**
- **Two types of schemes used (standard):**
  - » **Binary tree resolution: reader explores a tree of tag values**
  - » **Aloha: tags transmit with a random backoff**

Binary Tree Resolution

- Send requests to tags with ids that start with a certain string
- Narrow down search until one tag responds



General Security Concerns

- **RFID tags raise a number of security concerns:**
  - **Privacy risks, e.g., eavesdropping**
  - **Cloning and forging of tags**
- **Specific disadvantages due to tag limitations**
  - **Some encryption algorithms may be too complex to be implemented on tags**
- **But also specific advantages:**
  - **Tags are slow to respond, maximum no. of read-out operations**
  - **Short transmission range means that an adversary has to be physically close**

Privacy for Business Networks

- **Major concern for industry:**
  - » **Supply chain visibility**
  - » **Supply chains and business networks are business assets**
- **Example provenance checking: competitors may be able to get a lot of information**
  - » **Depending on how detailed the information associated is:**
    - – **Where an object and its parts where manufactured**
    - – **When it was manufactured**
    - – **By which sub-contractors**
  - » **Who are the suppliers of a company**
  - » **Which companies are the customers of a company**

Reading Ranges

- Controlling reading range can limit privacy risk
- Nominal read range (RFID standards and product specifications):
  - » 10cm for contactless smartcards (ISO 14443)
- Rogue scanning range: sensitive reader with more powerful antenna or antenna array
  - » 50cm
- Tag-to-reader eavesdropping range: need to power the tag limits range for passive RFIDs
  - » Eavesdropping on communication while another reader is powering the smartcard: > 50cm
- Reader-to-tag eavesdropping: readers transmit at much higher power

Outline

- **RFIDs**
  - **Concept and applications**
  - **EPC and backend processing**
  - **PHY and MAC**
  - **Security**
- **Near Field Communication**
- **Battery-less devices**

Near Field Communication (NFC)

- One device combines the functionality of
  - An RFID reader device
  - An RFID transponder (tag)
  - Bit rates ranging from 106 Kbs to 424 Kbs
- Integral part of mobile devices (e.g. mobile phones) NFC components can be accessed by software to
- Operates at 13.56 MHz (High frequency band) and is compatible to international standards:
  - ISO/IEC 18092 (also referred to as NFCIP-1),
  - ISO/IEC 14443 (smart card technology, "proximity coupling devices"),
  - ISO/IEC 15693 ("vicinity coupling devices").
- Use of NFC is growing fast
  - Driven by NFC Forum (founded by Nokia, Philips, and Sony in 2004)
  - http://www.nfcworld.com/nfc-phones-list/#available

N-Mark trademark of NFC Forum

NFC Devices

Example: contactless payment applications
- Sony FeliCa, Asia
- MIFARE, Europe
- Google Wallet

(c) Google

Modes of operation

- **Smart Card emulation (ISO 14443):**
  - » Phone can act as a contactless credit card
  - » Information can be generated rather than pre-stored
- **Reader mode**
  - » Allows NFC devices to access data from an object with an embedded RFID tag
  - » Enables the user to initiate data services, i.e., retrieval of rich content, advertisements, ..
- **Peer-to-peer (ISO 18092)**
  - » Allows two way communication between NFC devices
  - » NFC can act as smart tag, i.e., generates information

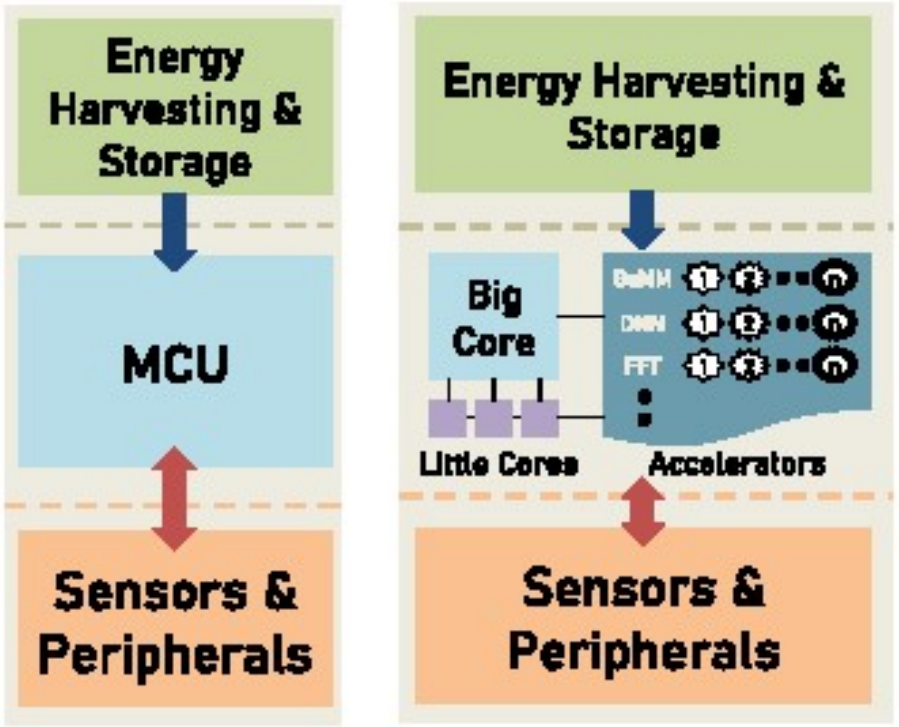
Active and Passive Communication Modes

- **Passive communication: one device acts as a reader and the other as a tag**
  - » **Reader generates a field while the other responds**
  - » **The second device can be a tag or another NFC device**
- **Active communication: both devices alternatively act as readers**
  - » **Allows fairly general two way communication**
  - » **Both devices must have a battery**
- **Since NFC devices can read and write, they must check for collisions**
  - » **Compare received signal with transmitted signal**

Outline

- **RFIDs**
  - **Concept and applications**
  - **EPC and backend processing**
  - **PHY and MAC**
  - **Security**
- **Near Field Communication**
- **Battery-less devices**

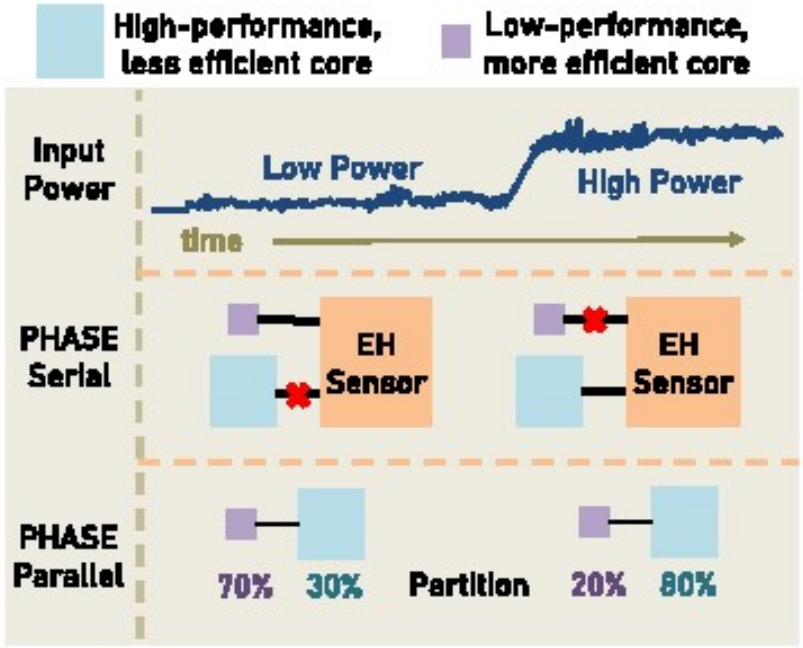
What is Next: Battery-less Devices



- Devices rely entirely on energy harvesting
  - » Solar, RF, …
- Battery can store limited amount of power
  - » Can be used when harvesting is slow or not possible
- Different architectures are being explored
- Goal is to have fairly general architectures

From: A Power-Aware Heterogeneous Architecture Scaling Model for Energy-Harvesting Computers, Desai, Lucia, IEEE Computer Architecture Letters, https://ieeexplore.ieee.org/document/9078058

Example Design



- Adapt level of activity to the available power
- For example, use simple but efficient cores when power levels are low
- Power hungry operations may have to wait
  - » E.g., send data