# Identity Management

ID management for people and objects

- System accessible assigned *tokens*
- *Token* means something you *have.*
- This is separate from something you *know* or you *are*.

- Things you carry and perform sensing or actuating
- Infrastructure beacons on objects
- Systems and issues

# What identity management is

Identity Management is the process concerned with identity collection, storage, retrieval, communication and policy enforcement.  It applies to objects as well as people.

This takes into account:

- Sensing
- Representing
- Security
- Privacy
- Trust
- Usage
- Escrow

It's a lot more than just sensing.  It includes communication, utilities and other services.  It is an active area of academic research.

# Assigned ID Tokens

## Your KTH ID Card is a multimodal example of one

Identity data collection

- Photo, magnetic stripe, PIN (after 17:00), RFID (not all).
- Everything on it is machine readable including the photo.

Some interesting questions to ask when looking at the KTH Card:

- Why are there so many ID modalities? Why not just 1?
- From a performance/watt/euro viewpoint, mag stripe would seem to win. Why not just use that?
- From a performance/watt/euro, what really happens when you lose your KTH ID card?
- The KTH card is supposed to identify me and it does. Everywhere. Is that a good idea?
- What does the KTH card really ‘know’ about me? Should it know more? Can it compute?
- What if the KTH had 50,000 students? Does it ‘scale’?

# Metrics that describe ID tokens

## ID tokens represent ID management based on something you *have*

It's how to get the *who* into the system and application of interest. One way is to use a token. The token ranges from simple forms to extreme devices to ultimately just yourself, where you are the token. (Instead of something you have it is something you *are*.)

What the application is, ie personalization, authentication, authorization, tracking, e-commerce, accountability …will dictate what performance your token needs to have. Factors of cost, power and usability will follow.

- Amount of data it can store
- Cost per bit
- Mode. Read only, read/write, write once, contact, contactless
- Bit rate
- Infrastructure cost
- Standardization
- Security requirements
- Use model
- Risks

# Apply this to bar code

There are two kinds of bar codes out there. Linear, or 1D, and 2D. Examples:


1D: 10 characters

2D: 62 characters

- Cost per bit: From 0.1 to less than 0.001 euro cents.
- Mode: Read Only, contactless
- Bit rate: Depends on the reader
- Infrastructure cost: Readers are a few tens of euros to a few hundred
- Standardization: Standards exist for 1D and 2D print format.
- Security Requirements: You can encrypt the data. No standard specified.
- Use Model: Requires use of a scanner. May be non-obvious to some.
- Risks: Loss. No control by owner. Can be duplicated.

# Writable formats are more interesting

## Example: The magnetic stripe on the back of some ID Cards.


- Capacity is a few hundred bytes.
- Cost per bit: From 0.1 to 1 Euro cent.
- Mode: Read/Write, contact
- Bit rate: Depends on the reader
- Infrastructure cost: Readers are a few tens of euros to a few hundred
- Standardization: Standards exist for recording and in some cases data format.
- Security Requirements: You can encrypt the data. No standard specified.
- Use Model: Requires use of a scanner. May be non-obvious to some.
- Risks: Loss. Little control by owner. Can be duplicated or hacked.

# An example of data field standardization can be found on mag-stripe cards for banking

A standard card may have any of three tracks, or a combination of these tracks.

Track 1 was developed by the International Air Transportation Association and is reserved for their use. It is 210 bpi with room for 79 characters. It includes the primary account number (up to 18 digits) and the name (up to 26 alphanumeric characters).

Track 2 was developed by the American Bankers Association for on-line financial transactions. It is 75bpi with room for 40 numeric characters. It includes the account number (up to 19 digits).

Track 3 is also used for financial transactions. The difference is its read/write ability. It is 210bpi with room for 107 numeric digits. It includes an enciphered PIN, country code, currency units, amount authorized, subsidiary account information and other information such as postal codes.

# Radio Frequency Identification

- This is an popular technology for ID management.  Radio as a sensor.
- Right now it is a significant growth area.
- A lot of new technology is emerging in the RFID space.
- Includes diverse sensors, infrastructure and protocols.
- Equally diverse applications.
- ID management for people and objects.

# Modern Passive RFID

These overcome many of the shortcoming of simple passive RFID by using modulation techniques on a single frequency and by using circuits and memory in the token.

They are called ‘passive’ because they have no active power supply. They scavenge power from the RF signal.

There are a number of different ways they can operate. Many common RFID tags today use a technique called *inductive coupling* to report back data.

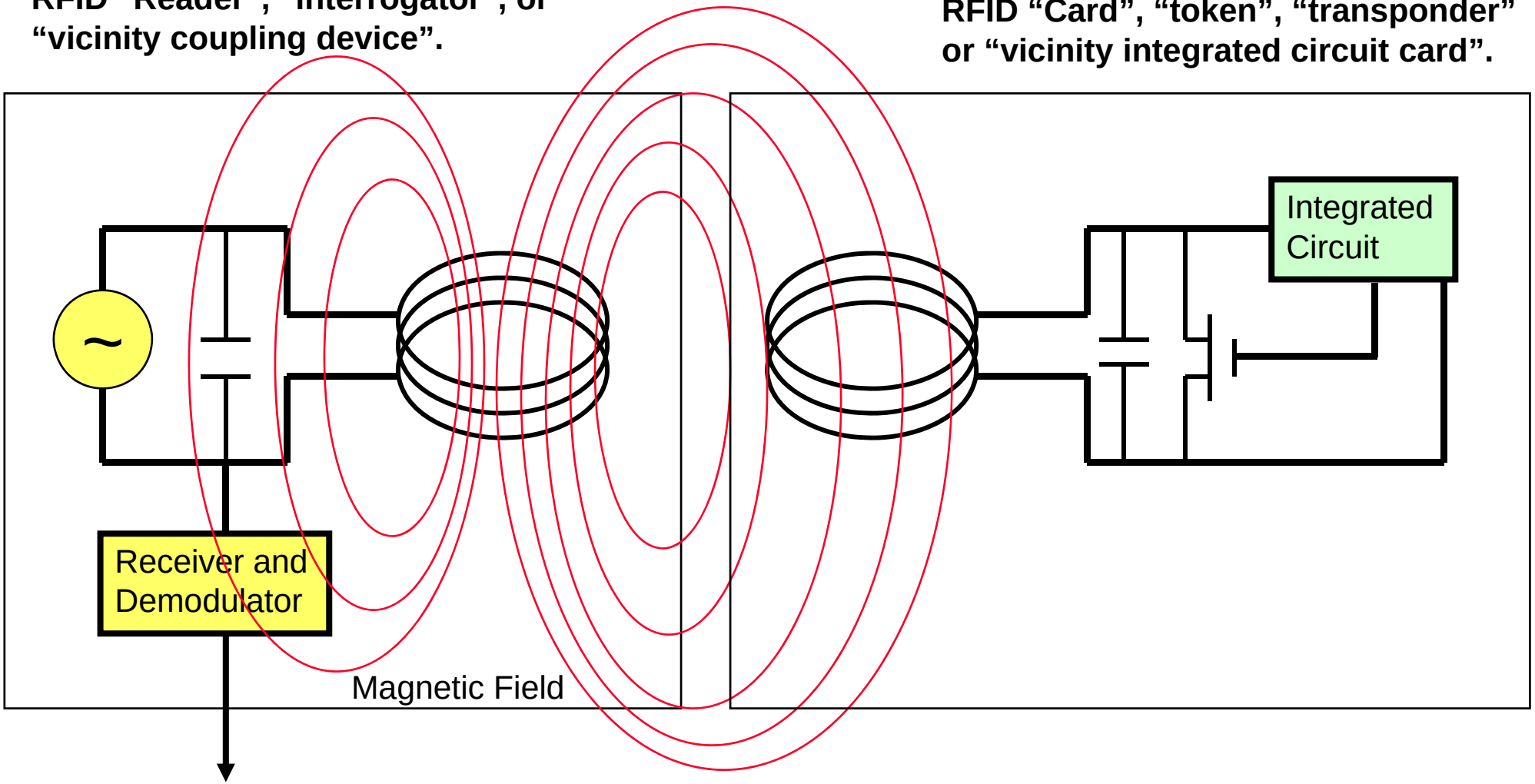
How data is encoded is often proprietary, which is partly responsible for slow market uptake in the past. Standards have now emerged.

- ISO/IEC 14443
- ISO/IEC 15693
- EPC 0, 1 and 2

# Inductively Coupled RFID Example: ISO/IEC 15693

**RFID "Reader", "interrogator", or "vicinity coupling device".**

**RFID "Card", "token", "transponder" or "vicinity integrated circuit card".**



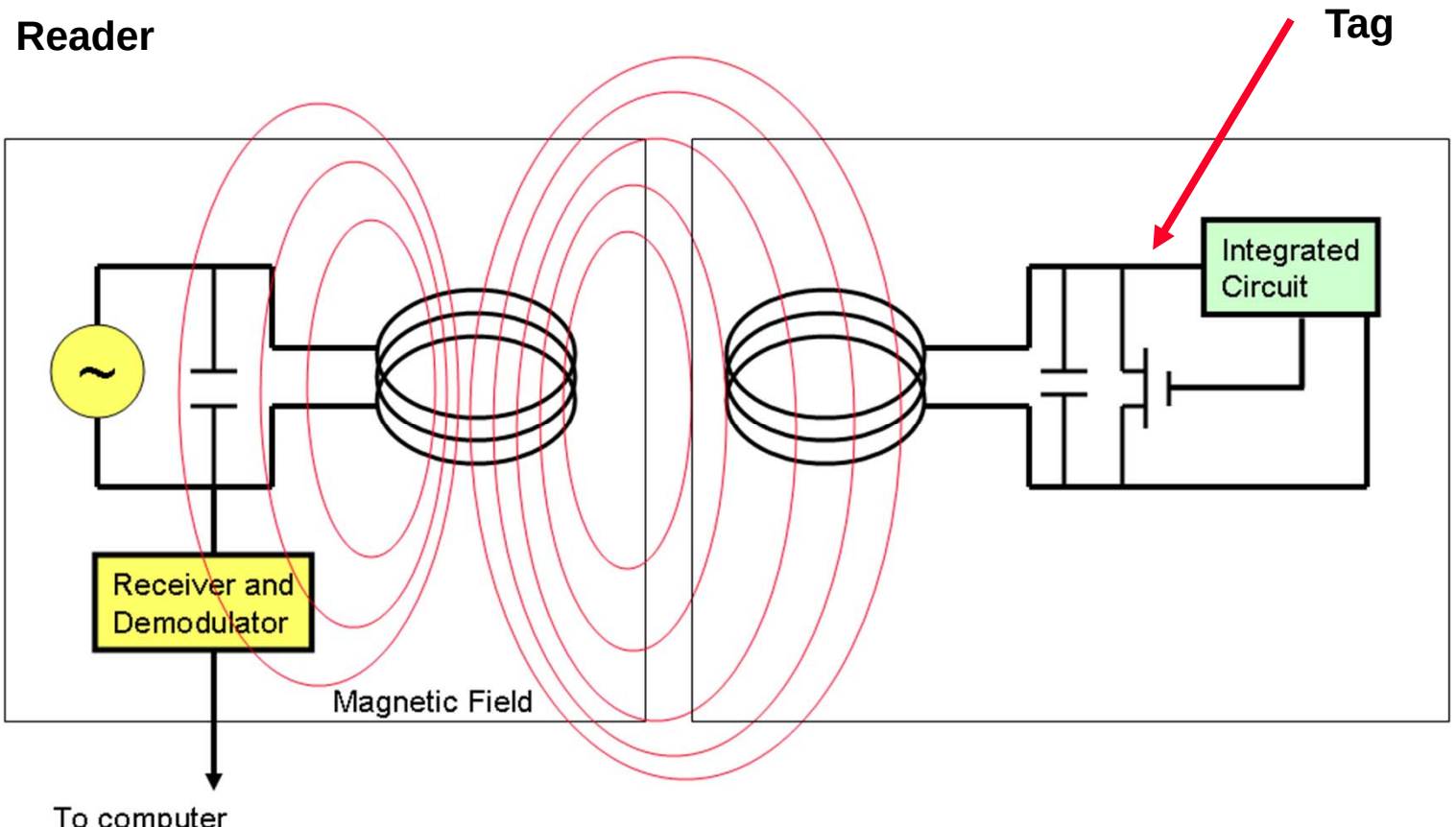

**A good analogy for how modulation in either direction works is to compare the RF voltage link between the reader and the RFID tag as weakly coupled transformer coils.**

# Modulation from the tag to the reader

The tag are reader communicate using *inductive coupling*

To produce modulation in order to signal back to the reader, the RFID tag coil is momentarily shorted by a low resistance. This results in a change in the magnetic field sensed in the reader's coil. This change represents how data is sent back from the tag.

In the circuit here, the RFID tag coil is short circuited using a FET.



# Multiple Tokens

- In a lot of applications there will exist the need for multiple tokens to be in the reader's field at the same time.
- There needs to be some form of multiple access control in order to allow multiple tokens to coexist in the same reader field, and for the reader to be able to interact with all of them.
- These *anti-collision* techniques are often proprietary, but in many ways are related to similar techniques from network physical layer design.
- The emerging standards also define how anti-collision works.

- We get into this in detail in RFID Systems (IS2500).

# Approximate ISO/IEC 15693 performance

- Cost: From about 0.50 to about 2.00 USD per tag, depending on capacity.
  - Cost goal is to manufacture tokens for less than 1 cent
- Mode: Read Only, Read/Write, contactless
- Bit rate:
  - Reader to Token: 1.65 kbits/sec or 26.48 kbits/sec depending on mode
  - Token to Reader: From 6.62 kbits/sec or 26.69 kbits/sec depending on mode
- Infrastructure cost: Readers are a few hundred USD
- Standardization: Standard exists.
- Security Requirements: You can encrypt the data. No standard yet specified.
- Use Model: Requires use of a scanner. Very easy compared to bar code or magnetic stripe.
- Risks: Loss. No control by owner. Can be duplicated with effort.

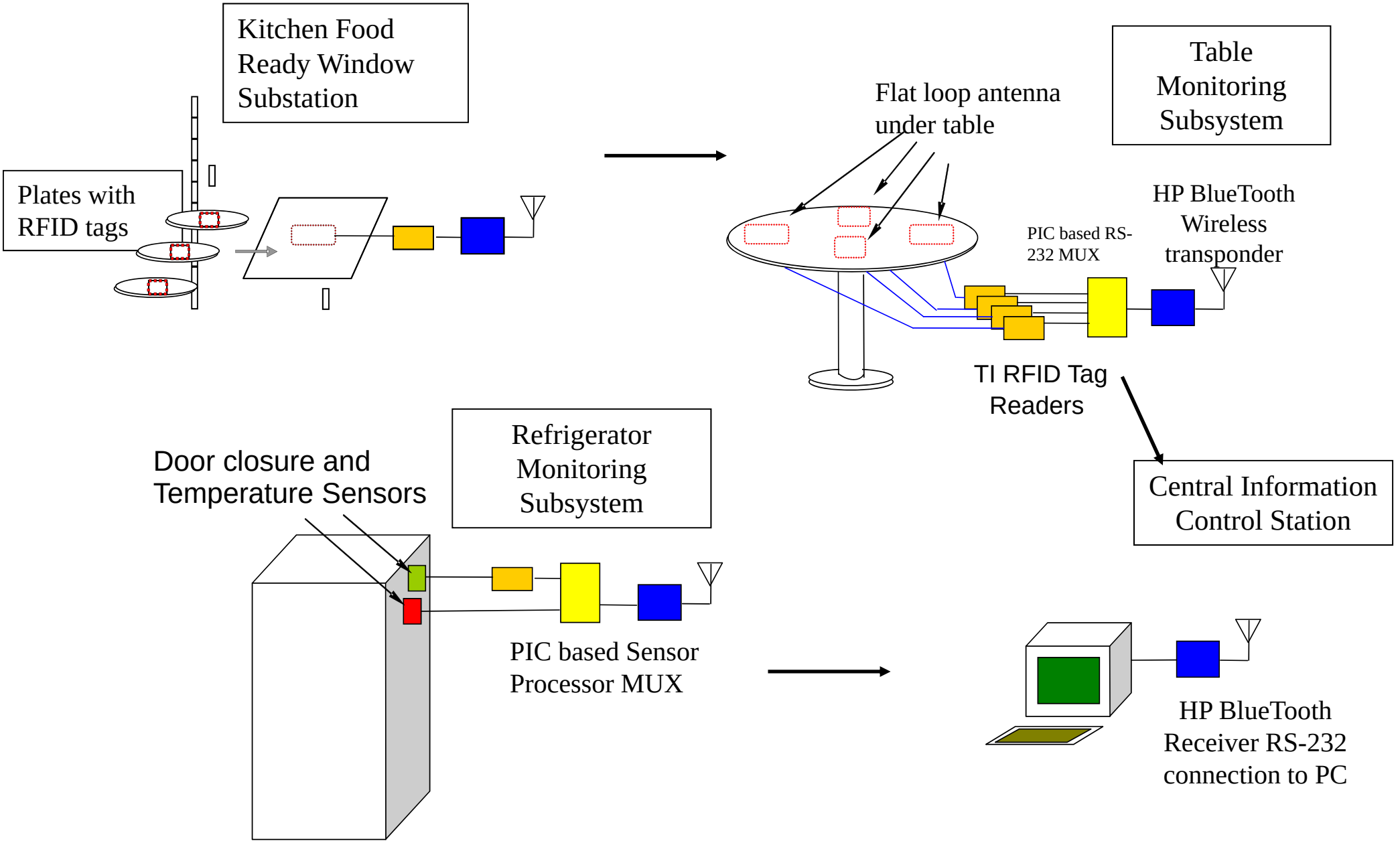
# Example system: Restaurant efficiency

In a 2003 national design competition sponsored by Boeing and SWE, a team from Cal Poly Tech designed an RFID based system for optimizing restaurant processes. Requirements were:

- Obtain accurate real time information on the activity levels in the restaurant.
- Use sensors compatible with the restaurant industry (ie washable) and would not invade privacy of workers or customers.
- Optimize food path from storage though kitchen to customer.
- Optimize service from when customer arrives to when they leave.
- Give a single metric reflecting restaurant operating efficiency.
- Present data to owner anywhere using a simple interface
- Cheap, simple, re-deployable

# Cal Poly – SLO Team Tech 2003

## Restaurant Real-time logistics support system



# Shortcomings of the inductive RFID design

- Still too expensive for mass deployment.  Cost reductions possible.
- Bit rate still isn’t very high for some applications.
- Sensing range is short.  But, this can be an advantage!
- Security model still isn’t complete.
- Privacy concerns are starting to emerge.
- These problems are being addressed in standards such as EPC2 and support standards such as NFC.

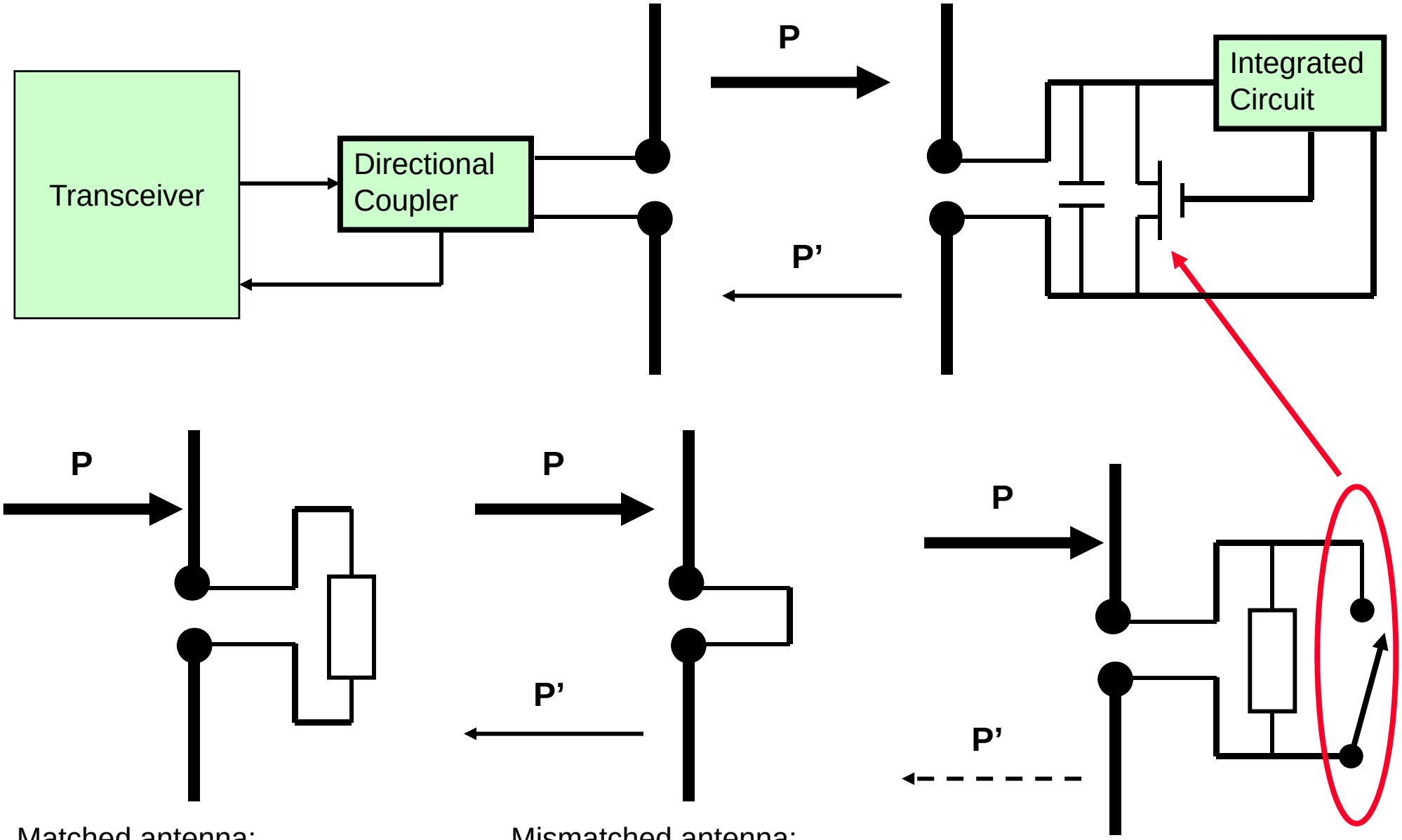
# Radiative

- *Radiative* RFID methods are the only practical solution to obtain greater range up to kilometers. Over these ranges the inductive coupling model of RFID no longer holds. There are two broad categories here.

1. Radiative Passive and Semi-Passive Scattering RFID
2. Active Transponders

- Both techniques involve use of radio propagation.
- Because a radiative model applies, these tags can use much higher RF frequencies in the microwave regions of the spectrum. Small antennas can be highly efficient here.

# Reflection or Re-radiation




Matched antenna: complete absorption

Mismatched antenna: complete reflection

Modulate using a switch

# Fully active RFID

- Passive scattering RFID is useful over a few meters. Much better range than passive load modulated RFID.
- There are some applications where even this isn't enough. RFID used in vehicles to pay road tolls is a good example.
- In those cases, *fully active* or *active transponder* RFID. Larger versions are used in other radar applications, such as aviation and maritime use.
- These RFID tags look for a signal from the reader. When they see it they actively transmit back a reply with the requested data.
- They don't use reflections. They have to have a complete transmitter and receiver in every token.
- They are big, use relatively lots of power, and they are correspondingly expensive. But, they have their niche.

# Shortcomings of the active RFID

- Too expensive for mass deployment unless the customer pays for the token, in which case it must have direct benefit like not stopping to pay tolls.
- Bit rate still isn’t very high for some applications.
- Security model still isn’t complete.
- Privacy concerns are becoming a major problem.

# NFC

NFC stands for *Near Field Communication*.

- At the radio layer, it is just passive inductive RFID. Not new.

- The differences and additions are at higher function levels.
- There are at least 3 major differences:

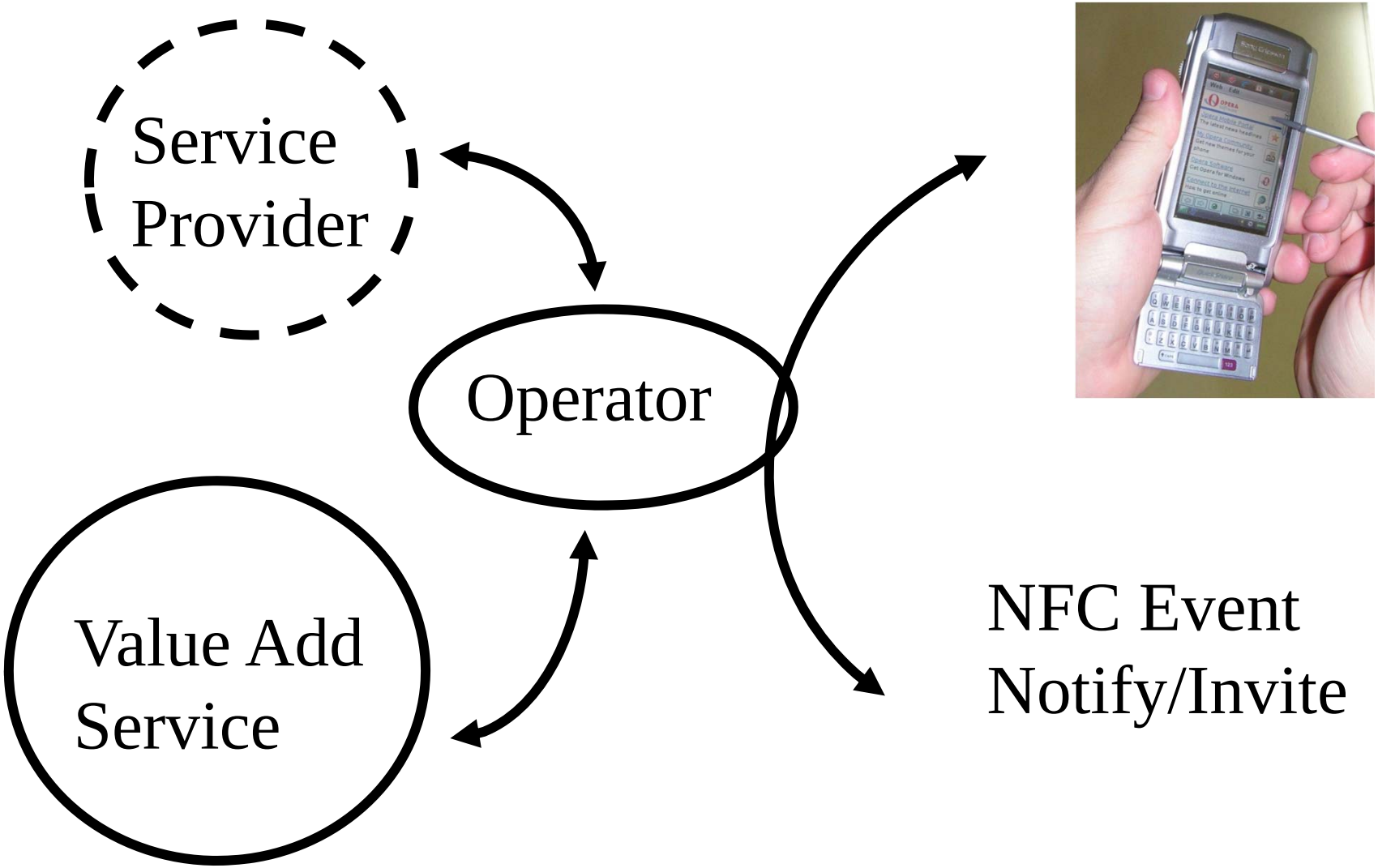
1. A reader can optionally emulate a tag. This means that two readers can in a peer to peer manner exchange data.
2. How data is formed and exchanged is formalized using *NFC Data Exchange Format* (NDEF). This standardizes data exchange.
3. An *element* for secure transactions. Similar to a Smart Card.

- Electronic payment applications are driving this, although other secure applications can benefit.

# Sony-Ericsson NFC Phone

- **Note the coil antenna right over the battery.**
- **Normal operation is a “touch” model.**
- **Has all the range properties of inductive RFID.**
- **However, the phone can act as a reader!**
- **This means phone to phone data transfer is possible.**
- **In effect, peer-2-peer RFID.**

# NFC Transactions and Events




**Could a model like this involve privacy problems or other threats?**

The next step in addressing these problems is to look at Biometrics.