londonknowledgelab

RFID: Applications, Operation, Numbering and Lookups

Mobile and Ubiquitous Computing

George Roussos
g.roussos@bbk.ac.uk

Birkbeck
UNIVERSITY OF LONDON

uID Center

Overview

- RFID applications
- RFID principle of operation
- Types of tags
- Addressing
- Lookups

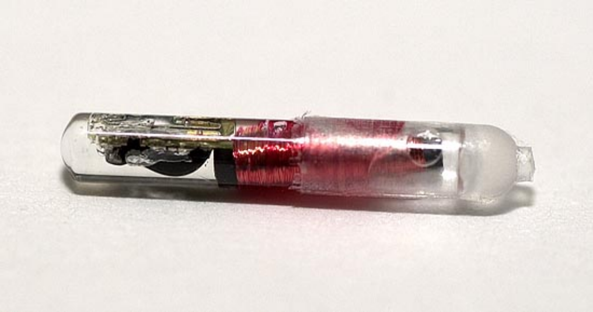
Identification Friend or Foe

- Introduced during WWII to distinguish between own and enemy aircraft
- Uses the Radar system
- In common use today for air traffic management
- Employs the secondary surveillance radar
- Air traffic management uses Mode 3/A or S
- Uses a lot of power

Automated Toll Collection

- Automated collection of motorway toll fees
- Battery powered device on the vehicle
- Interrogator installed at the toll portal
- Credit stored in the tag and fees deducted at every passage

Tag people



- Verichip RFID tag FDA approved for use with humans
- Many applications claimed:
  - Medical, medication, surgery
  - Kidnap victims
  - Nightlife
  - Track offenders (150k people currently tagged in the UK)
  - Identification
- Highly hackable (more on this at the end)

Retail

- Consumer applications: smart self, smart shopping cart, inventory tracking
- Large scale trials (Metro Supermarket, Germany)
- Actual implementations (Mitsukoshi Department Stores in Japan)
- Makes sense for high-value items only
- Passive (no battery) tags should cost less than 5 cents

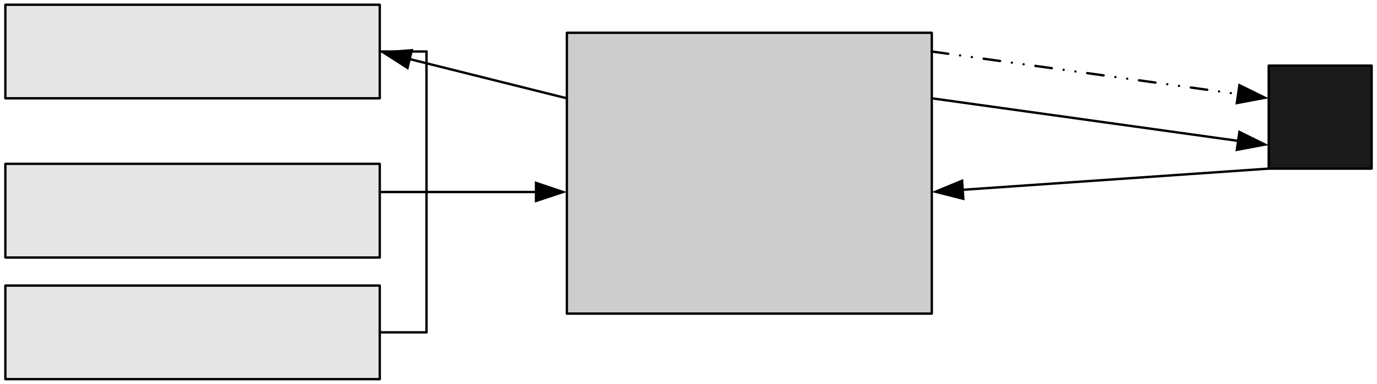
Pharmaceuticals

- Anti-counterfeiting a priority
- Additional applications
  - correct medication
  - inventory management
  - recall
- Issues related to effects of radiation on drugs

RFID Basics

- AC oscillation at the end-points of an antenna creates magnetic and electric fields
- RFID uses these fields to transmit energy and for communication
- Depending on which field is used and how the transmitted energy is used we get different types of RFID systems

Sequence of events



Middleware

5

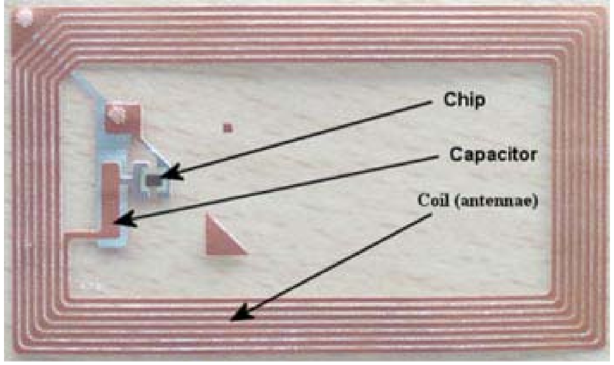
1

Network management

Reader management

1. reader configured with operational parameters
2. reader creates field that powers up the tag
3. reader initiates communication
4. tag responds
5. information returned to middleware/applications after possible additional processing step

Tag components



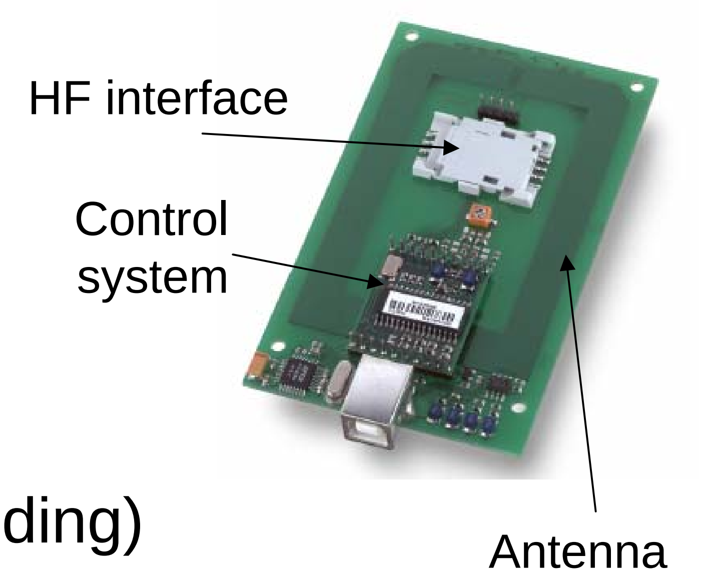
Tag internals

Typical polymer enclosure

- Antenna (different types according to coupling method used)
- Chip (for passive tags this is a simple state machine)
- Capacitor (to store transmitted power)
- Enclosure

Reader components

- HF interface
  - transmitter/receiver
  - separate pathways
- Control system
  - microcontroller
  - ASIC module (crypto, signal coding)
  - network module
- Antenna
  - integrated/external
  - one or many



Component roles

- High-frequency interface
  - – generates transmission power to activate tag
  - – modulates transmission/demodulates tag signal
- Control system
  - – control communication with tags
    - anti-collision, data crypto, authentication
  - – signal coding and decoding
  - – interact with network services
- Multiple antennas are seen as one (cf. tag orientation issues later)

Near and Far Field

- <100Mhz magnetic, inductive or near-field coupling
  - – Near field means that the wavelength is several times greater than the distance between the reader and tag
  - – Examples: 128 kHz and 13.56 MHz
  - – Same principles as the transformer
  - – Electric component is not involved
- >100Mhz capacitively or far-field coupling
  - – Examples: 915MHz and 2.45 GHz
  - – Same principle as the Radar
  - – Magnetic field is not involved

Active versus Passive

- Power to operate the chip
- Active tags:
  - Use battery to power up the chip
- Passive tags:
  - Power up using the coupling effect
  - Essentially the reader transmits power used by the tag
- Semi-passive tags
  - Use battery to operate the chip
  - Antenna optimized for data transmission

Active Tags

- Advantages
  - Transmit at higher power levels
  - Longer range
  - More reliable communication
  - Can operate in challenging environments (e.g. around water)
  - Can have additional sensing capability (e.g. temperature)
  - Can initiate transmissions
- Limitations
  - Stop when their battery expires (10 years at best)
  - More expensive
  - Larger size (to accommodate the battery)

Passive Tags

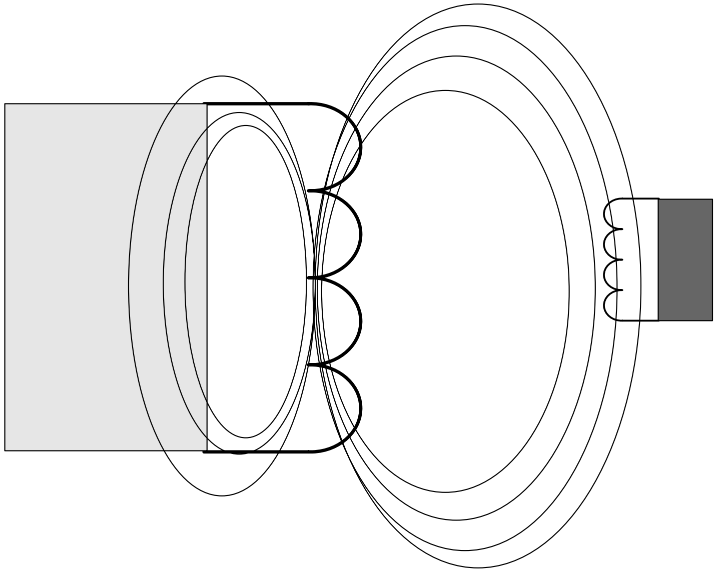
- Advantages
  - Low cost
  - No battery, so they do not expire (unless damaged)
  - Small size
  - Increasingly printable
- Limitations
  - Restricted processor, memory and communications
    - Functionality has to be offloaded to the network
    - Limited capability to protect themselves
  - Only operate in the vicinity of readers
  - Harder to operate in harsh environments

Passive Tag Implications

- Manufacture at less than 5 cents per tag by 2010
  - not counting royalties and other IPR!
- Major interest in logistics
  - industry backing
- Massive investment by semiconductor industry
  - rapid progress on many fronts
- Key idea:
  - store only a Universally Unique Identifier in the tag
  - carry out all related processing on the network

Near Field Coupling

- Employs magnetic induction
  - Same idea as the transformer
  - Coil-shaped antenna
- AC at coil->current at antenna
- Charge stored in tag capacitor
- Powers up chip
- Tag changes impendence at coil affecting current drawn by coil
- Reader decodes change via the potential variation in its resistance
- Process called load modulation



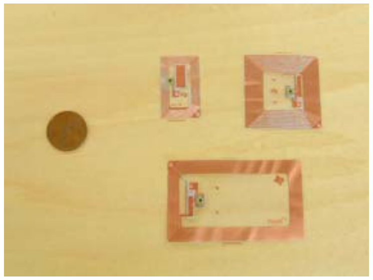
Near Field Coupling

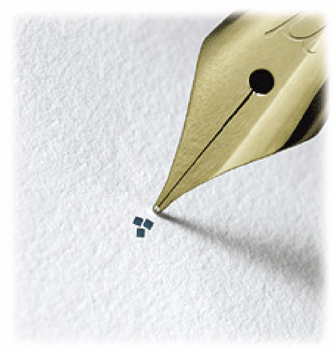
- Coils of reader and tag separated in space
- Coupling requires that magnetic field of reader intersects the tag coil
- This is the near field of the EM field created by AC oscillation
- Strength of field falls proportionally to 1/d^3
  - center of reader coil to tag

Near Field Coupling

- Size of field depends on frequency of current and limited within $2D^2/\lambda$
  - after this, the far field starts
- Examples:
  - ISO 14443 operates at 13.56MHz, NF is 3.6 meters
  - UHF 915Mhz NF is 6cm
- Larger antennas can help
- In practice most systems work in 1-30cm range

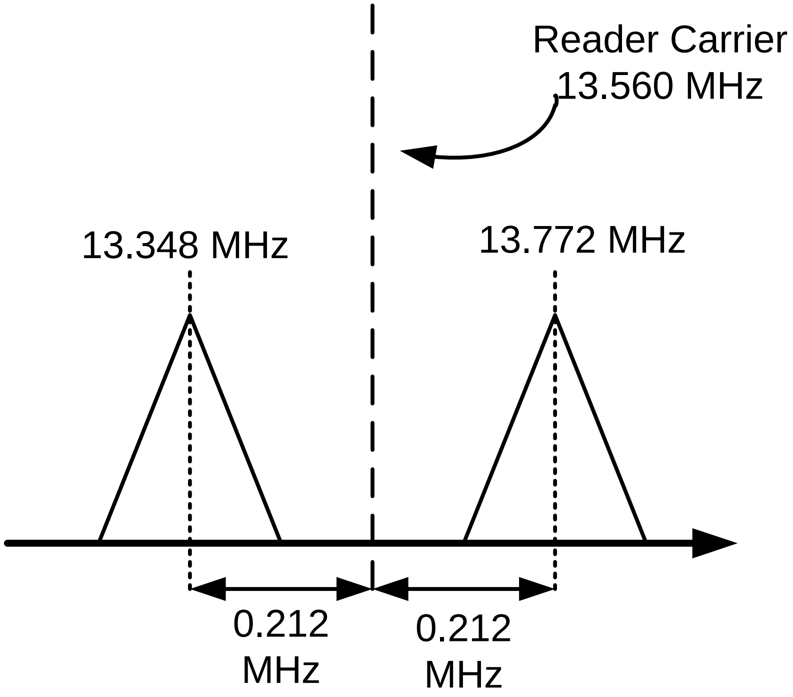
NF Tag examples





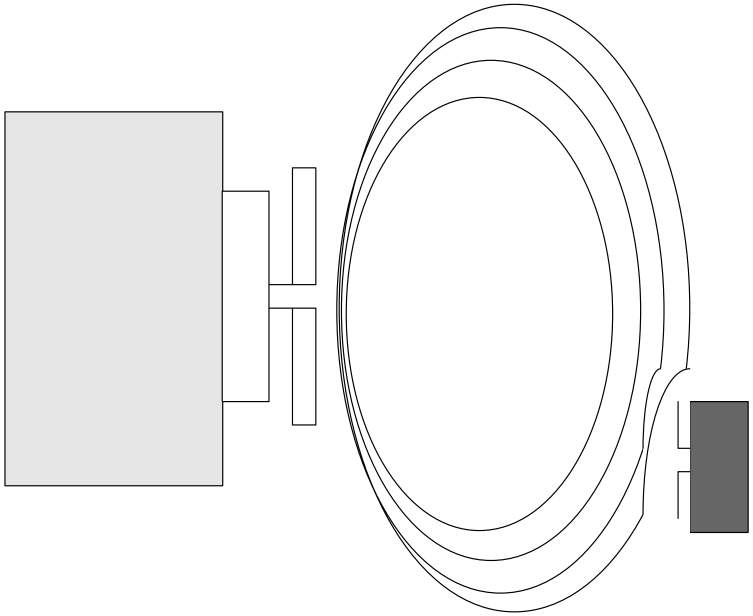
Communication with load modulation

- Voltage fluctuation at reader antenna as result of tag resistor change is tiny
  - e.g. 100V reader to 10mV signal
- Detecting this signal is a problem
- Load modulation using the subcarriers is one solution
- Load resistor of transponder switched on/off at frequency f_s then two spectral lines at $f_r \pm f_s$
- Data transmitted using this frequency



Far Field Coupling

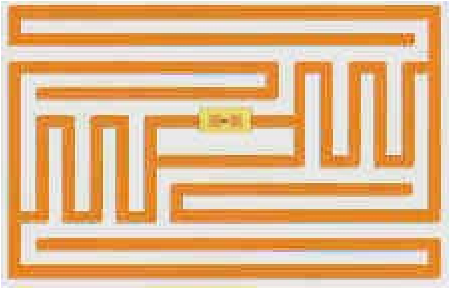
- Antenna is a dipole
- RF backscatter rather than induction
- Backscatter: reflect back some part of reader RF signal
- Reader decodes reflections as variation in amplitude
- Reader must have very sensitive receiver:
  - energy attenuation reduces by $1/d^2$
  - so reflections $1/d^4$ of original power
  - d separation of tag and reader

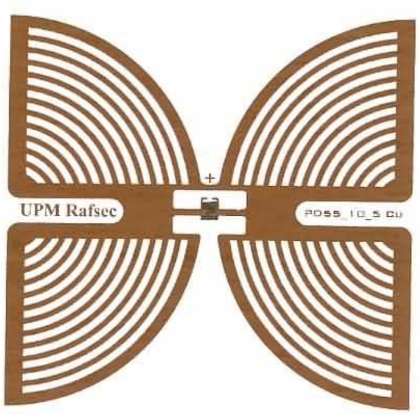


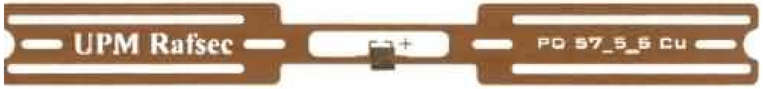
Far Field Coupling

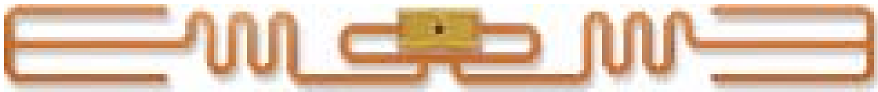
- Backscatter is the radar principle
  - electromagnetic waves are reflected by objects greater than ½ of the wavelength
- *The reflection cross section (*the signature of the object) can be modified by altering the load connected to the antenna of the tag
  - switching the tag resistor on and off creates the data stream
- Effective range of reading is typically 3-4 meters
- Reader sensitivity one microwatt
- Tags benefit from Moore’s law
  - less energy needed to power up the tag

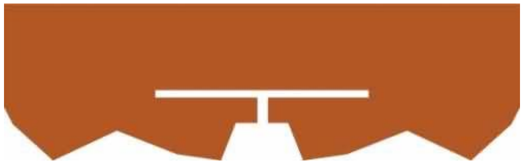
FF Tag examples











Tag orientation effects

- Alignment of tag antenna is second most important factor in effectiveness (after distance)
- In either near field or far field systems tag must NOT be perpendicular to reader antenna
  - Tag fails to be read
- (Partial) solution to this problem:
  - Antenna design or many antennas with different alignments
  - Multiple readers (but beware of reader collisions)

Influence of Objects and Environment

- Inductive systems
  - Unaffected by dielectric or insulator materials e.g. paper, plastics, masonry, ceramics
  - Metals weaken the field (depending how ferrous they are)
  - May also detune tags if they work at a resonant frequency
- Electric
  - Can penetrate dielectric material
  - Water molecules absorb energy
  - Metals reflect or scatter and can completely cloak tag
  - Tag on tag effect are also very strong in higher densities

RFID Addressing

- Identifiers in RFID
- A brief history of object numbering schemes
- Object identifiers
  - EPCglobal Electronic Product Code
  - Ubiquitous ID
  - Other object numbering schemes
- Addressing objects
- The Internet of Things

Identifiers in a Gen2 tag

- Tag identification (TID) memory bank
  - An 8-bit ISO 15963 allocation class identifier
    - For EPCglobal Tags it is 0xE2
  - A 12-bit Tag mask-designer ID
  - A 12-bit Tag model number.
  - Manufacturers can also include other information if required e.g. tag serial number
- EPC in EPC memory bank
- User memory bank may contain additional application specific IDs

ISO 14443 IDs

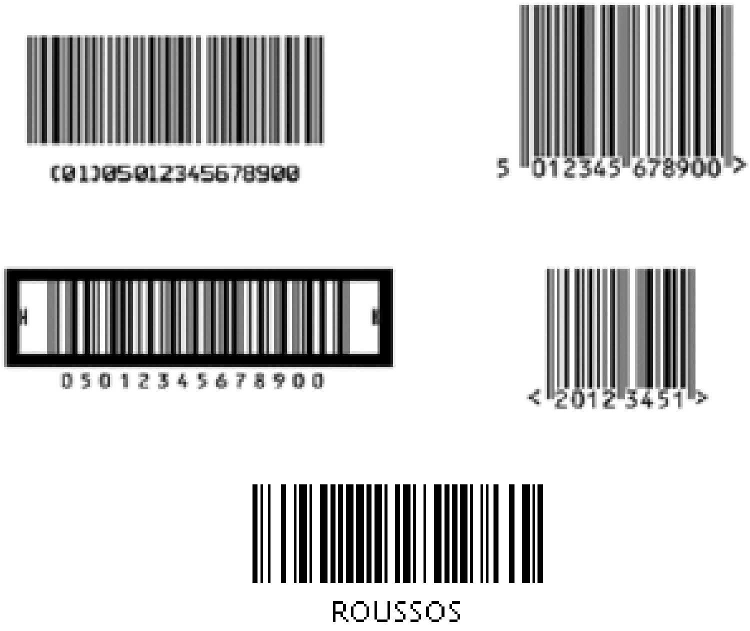
- ISO 14443-A requires fixed Card Identifier (CID)
- CID uniquely related to tag chip
  - Application Family Identifier (AFI) defines separate spaces for CID
- Used by reader to address a specific card
  - Also used in groups to keep specific cards in a particular state
- In ISO 14443-B can be pseudo –random number
- Application layer identifiers are contained in user data space
  - e.g. Oyster card customer number different from ISO ID

Addressing objects

- User-space object ID
- Generally no additional context data on tag
- Characteristics
  - Universally unique
  - Sub-domain structure
  - Registrar
  - Ownership
  - Mechanisms for mapping to metadata
- There are already some candidates!

Numbering Systems for Objects

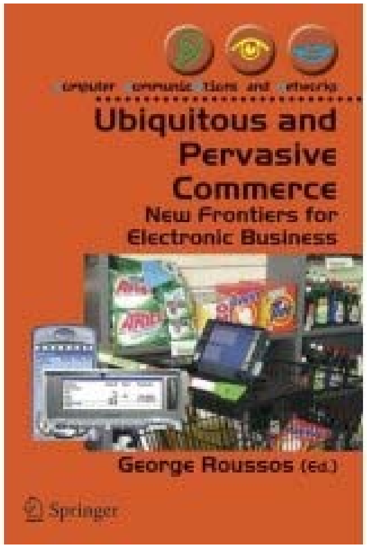
- Barcodes
  - many different types!
- IPv6 addressing
  - too much functionality for objects in many cases
  - requires superior processing capability and >100KB stack)
- Internet 0
  - reduced IP stacks with ISO-1800/IRDA etc link layer
  - Asymmetric, no end-to-end
- Other MAC addresses
  - embedded Zigbee, Bluetooth



UCC/EAN-128, EAN-13, EAN-8, ITF 14.

Multiple identifiers

- Objects can have multiple IDs in different schemes
  - 658.05 UBI (Dewey Classification Scheme)
  - 1846280354 (ISBN)
  - 9781846280351 (EAN)
  - 6602940 (LIBRI)


Computer Communications and Networks
Ubiquitous and Pervasive Commerce
New Frontiers for Electronic Business
George Roussos (Ed.)
Springer

Objects are also products

- Object manufacturer well positioned to embed ID
- Has been done before at global scale
- Major perceived business benefits in the supply chain
  - logistics, inventory, anti-counterfeiting, demand forecasting, shrinkage
- Possible consumer applications
  - smart things, smart selves, product recalls
- Major technology investment

Barcodes and the SG1 system

- UPC created in 1973 the first American 10-digit barcode standard (uniform and then Universal product code)
- European Article Numbering introduced in 1977 extended the scheme to the needs of a global market
  - first to separate the data from the data carrier
- Two systems became interoperable in 2005 as EAN.UCC and later SG1 (One Global Standard)
- Under SG1 a variety of standardization activity including RFID within EPCglobal
  - ebXML, Global Data Synchronization Network, Global Standards Management Process, Global Product Classification

EPC Identifiers

- A global identifier scheme is needed
  - Address allocation, coordination of address space, address semantics, resolution
- EPC is part of SG1 and so has to accommodate existing EAN and related identifiers
- Management of the scheme is via a SG1 subsidiary called EPCglobal Inc
- Protocols are developed in the Auto-ID network of research laboratories

EPC structure

- EPC tag data standards define “pure identifiers” which are abstract object addresses
- Pure identifiers are stored following the related “physical realization” and “encoding” protocols on the tag
- *Header data* identifies the particular scheme employed in a specific EPC and thus the semantics of the digits
- Current schemes are specific to SG1 and DoD requirements and there is also a general ID

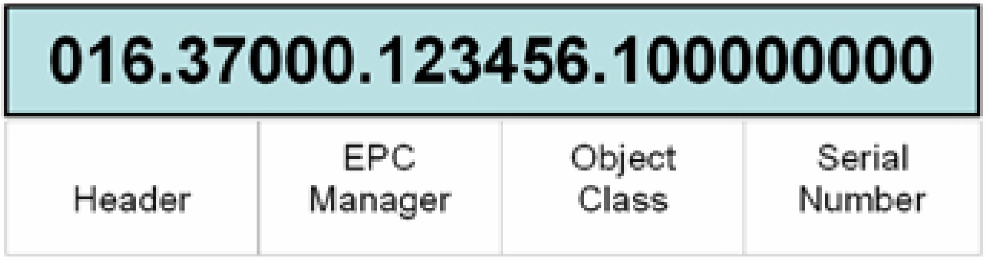
Encoding schemes

- General Identifiers (GID-96)
- System Identifiers
  - GS1 Global Trade Item Number (GTIN) SGTIN-96 SGTIN-198
  - GS1 Serial Shipping Container Code (SSCC) SSCC-96
  - GS1 Global Location Number (GLN), SGLN-96 SGLN-195
  - GS1 Global Returnable Asset Identifier (GRAI) GRAI-96 GRAI-170
  - GS1 Global Individual Asset Identifier (GIAI) GIAI-96 GIAI-202
- DoD construct (DoD-96) cf. www.dodrfid.org

Types of data

- Serialized Global Trade Item Number (SGTIN) -On item packaging for items where a serial number is used for the unique identification of trade items worldwide within the UCC.EAN System.
- Global Returnable Asset Identifier (GRAI)-On item packaging for items (reusable package or transport equipment).
- Global Individual Asset Identifier (GIAI) -On item packaging for items (used to uniquely identify an entity that is part of the fixed inventory of a company -GIAI can be used to identify any fixed asset of an organization).
- Serialized Shipment Container Code (SSCC)-Items shipped as either pure or mixed case, pallet, (SSCC can be used by all parties in the supply chain as a reference number to the relevant information held in computer database or file).

Electronic Product Code



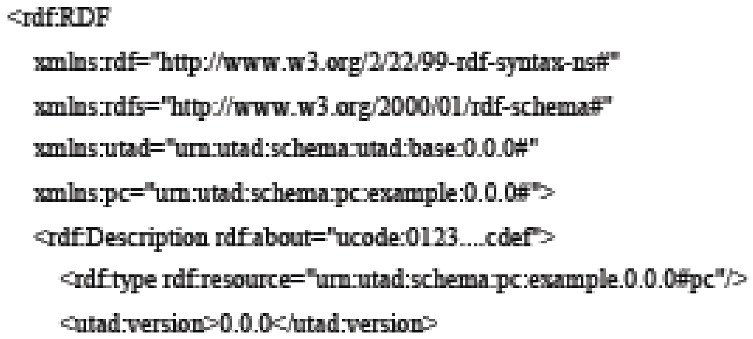
016.37000.123456.100000000			
Header	EPC Manager	Object Class	Serial Number

- *Header:* identifies the length, type, structure, version and generation of EPC
- *Manager Number:* which identifies the company or company entity (today: same as EAN)
- *Object Class:* similar to a stock keeping unit or SKU
- *Serial Number:* which is the specific instance of the Object Class being tagged

ucode

- Not specifically related to supply chain applications
- ucode is a 128-bit number
- It is a meta-ID because it can incorporate other numbering schemes
  - provides bindings for JAN, UPC, EAN.UCC, ISBN
- It can be abbreviated for use with low-capacity carriers
  - uses context code
- Distinct domain levels, managed independently
- Registrar is Ubiquitous ID Centre
  - T-Engine Forum, University of Tokyo

uID technologies



```
<rdf:RDF
  xmlns:rdf="http://www.w3.org/2/22/99-rdf-syntax-ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:utad="urn:utad:schema:utad:base:0.0.0#"
  xmlns:pc="urn:utad:schema:pc:example:0.0.0#">
  <rdf:Description rdf:about="ucode:0123....cdef">
    <rdf:type rdf:resource="urn:utad:schema:pc:example.0.0.0#pc"/>
    <utad:version>0.0.0</utad:version>
```

- Defines specific tag classes
  - also incorporates barcodes
  - microwave, HF and UWB tags
- Defines reader device called the uID Communicator
- Defines software platform
  - Based on TRON
- Address resolution points to uTAD record with object details

ucode structure

Length (bits)	4	16	4	variable	variable	
	ver.	TLD	CC	DC	IC	Total 128 bits

- version
- Top Level Domain code
- Class Code specifies the boundary between DC and IC
- Domain Code specifies the type of IC
  - e.g. JAN, ISBN, EPC etc
- Identification Code is the actual object identifier

RFID Directory

- The role of networked services
- Directories and Lookup
- Object Naming Service operation
- ONS and DNS

Network RFID

- Tags have to minimize cost:
  - very limited storage, i.e. contain ID only
  - very limited computational power
- IDs by themselves are not useful
- Tradeoff: ID is the key to query the network for information
- Need:
  - directory,
  - lookup service
  - (federated) database to hold info
  - associated protocols
- Employ internet and web standards where possible
- Cost and interoperability

EPCglobal NRFID architecture

Discovery	Object Naming Service (ONS)	Discovery of authoritative object manufacturer information
	EPC Discovery Service	Track-and trace chain information discovery (pointers to)
Storage	EPC Information Service	Store and retrieve item and class level usage information
Authentication	EPC Trusted Services	Authentication, authorization and access control

Directory

- Map IDs to service locations
  - e.g. map product ID to web service that can be queried for its expiration date
  - does NOT include serial number
- It also maps EPC Manager IDs to EAN.UCC Company prefix
- Requirements: global directory on the internet
- Obvious candidate: Domain Name System

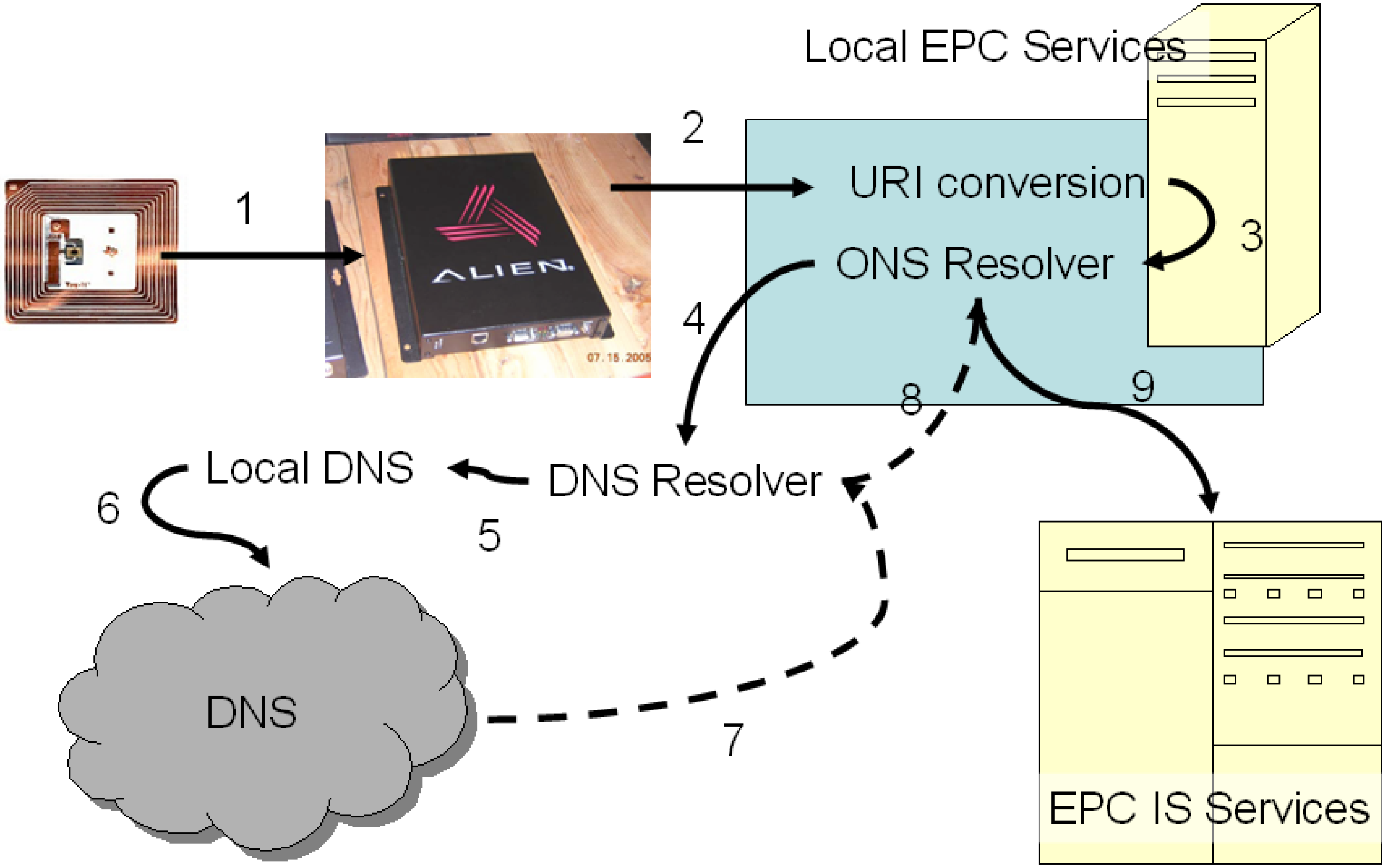
DNS and X.500

- DNS maps IP numbers to names and vice versa
- In fact, it maintains general Resource Records
- Extensible using NAPTR records
- Well established API and tools
- Efficient lookups, global reach
- Decentralized: location, administration (hierarchical)
- X.500 (ITU) free search but less efficient
- White pages, yellow pages
- Update protocol, security

ONS lookups

- Using the usual DNS tools
- Two types of DNS resource records
  - NAPTR for EPC codes
  - TXT for company code tables
- Translating the ID into a DNS query
- Follows path to (local to authoritative) onsepc.com through DNS
- Follows path within onsepc.com from root to ID custodian local server

Query sequence



Translation

EPC 64-bit Format:

[10 000 00000000000000 00000000000000011000 0000000000000000110010000]

Step 1: Reader captures and sends to EPC event manager

10 000 00000000000000 00000000000000011000 0000000000000000110010000

Step 2: EPC EM creates URI following Tag Data Standard:

urn:epc:id:sgtin:0614141.000024.400

Step 3: To local ONS resolver:

urn:epc:id:sgtin:0614141.000024.400

Step 4: ONS resolver concerts the URI to the equivalent DNS NAPTR query

000024.0614141.sgtin.id.onsepc.com

Step 5: DNS returns result set (redirect to manager domain)

Birkbeck UNIVERSITY OF LONDON

uID Center

ONS Resolver

- Remove URI pre-fix

urn:epc:id:sgtin:0614141.000024.400 → 0614141.000024.400

- Remove Serial Number

0614141.000024.400 → 0614141.000024

- Invert

0614141.000024 → 000024.0614141

- Append ONS root

000024.0614141 → 000024.0614141. sgtin.id.onsepc.com

- Issue DNS query e.g.

nslookup 000024.0614141. sgtin.id.onsepc.com (set type=NAPTR)

ictx.getAttributes(epcDomainName, new String[]{"NAPTR"}); (javax.naming)

NAPTR

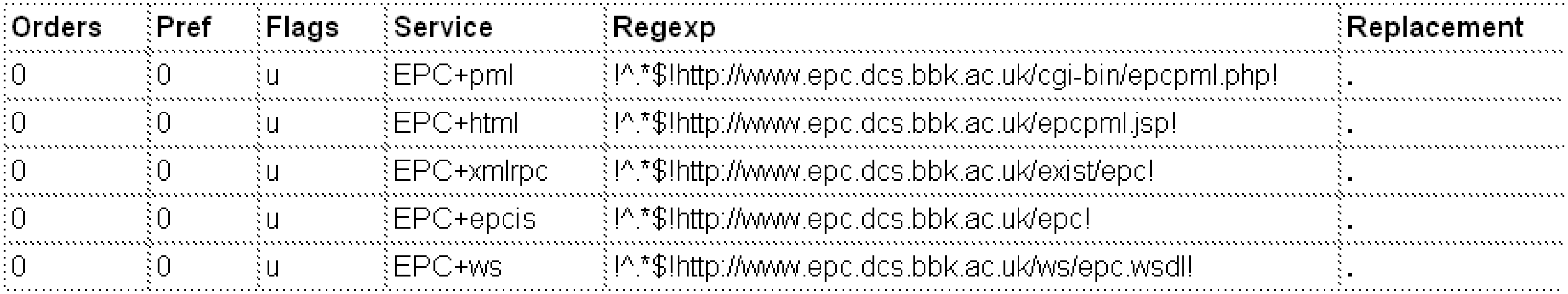
- Naming Authority Pointer (NAPTR) is a type of DNS Resource Record (RFC 2915)
- Designed for Dynamic Delegation Discovery System (DDDS) applications (RFC 3401, 3401, 3403, 3404)
  - Lazy binding of strings to data
  - Supports dynamically configured delegation
- Uses regular expressions to specify a delegation point within some other namespace
- e.g. used to locate SIP users

```
$ORIGIN 3.8.0.0.6.9.2.3.6.1.4.4.e164.arpa.
    NAPTR 10 100 "u" "E2U+sip" "!^.*$!sip:info@example.com!" .
```

ONS Result Set

- NAPTR fields:
  - **Order** And **Pref** show priority of this result within the set
  - **Flags** when set to “u” means regular expression containing URI
  - **Service** designates different types of services. The format of this field is EPC+service_name where service_name can be pml, html, xmlrpc, and ws
  - **Regexp** specifies a URI for the service being described (for ONS currently it is hostname and additional path information)
  - **Replacement** specifies the replacement portion of the rewrite expression (not used in ONS)

ONS Result Set Example



Orders	Pref	Flags	Service	Regexp	Replacement
0	0	u	EPC+pml	!^.*$!http://www.epc.dcs.bbk.ac.uk/cgi-bin/epcpml.php!	.
0	0	u	EPC+html	!^.*$!http://www.epc.dcs.bbk.ac.uk/epcpml.jsp!	.
0	0	u	EPC+xmlrpc	!^.*$!http://www.epc.dcs.bbk.ac.uk/exist/epc!	.
0	0	u	EPC+epcis	!^.*$!http://www.epc.dcs.bbk.ac.uk/epc!	.
0	0	u	EPC+ws	!^.*$!http://www.epc.dcs.bbk.ac.uk/ws/epc.wsdl!	.

Service codes:

EPC+pml: Product Markup Language document

EPC+html: Web page description

EPC+xmlrpc: XML Remote Procedure Call interface

EPC+ws: Web Service interface (WSDL)

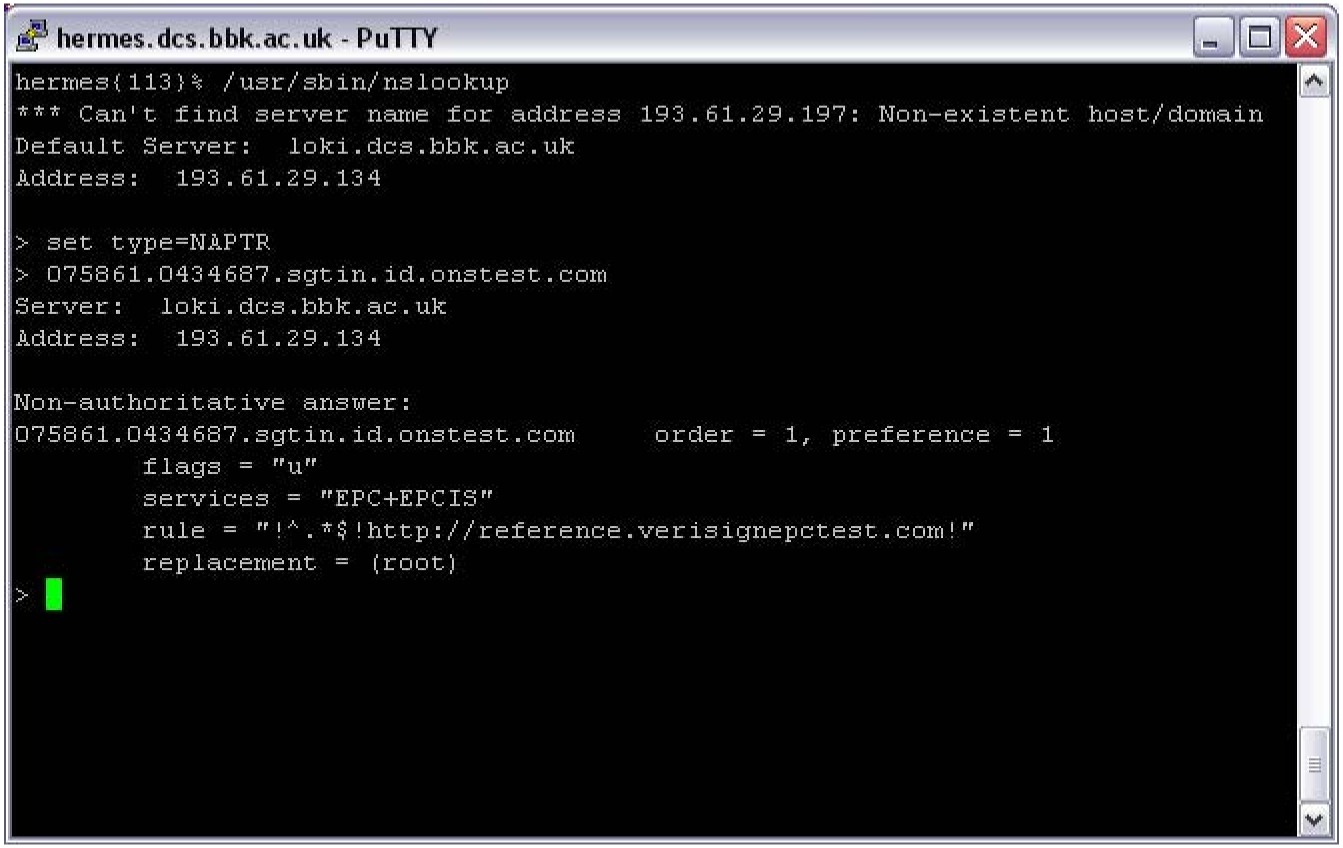
EPC+epcis: Authoritative EPC IS server

Example

Solaris 10 nslookup

Set DNS record type to NAPTR

ONS reply



```
hermes(113)% /usr/sbin/nslookup
*** Can't find server name for address 193.61.29.197: Non-existent host/domain
Default Server:  loki.dcs.bbk.ac.uk
Address:  193.61.29.134

> set type=NAPTR
> 075861.0434687.sgtin.id.onstest.com
Server:  loki.dcs.bbk.ac.uk
Address:  193.61.29.134

Non-authoritative answer:
075861.0434687.sgtin.id.onstest.com     order = 1, preference = 1
        flags = "u"
        services = "EPC+EPCIS"
        rule = "!^.*$!http://reference.verisignepctest.com!"
        replacement = (root)
>
```

Try test ONS server at epc.dcs.bbk.ac.uk