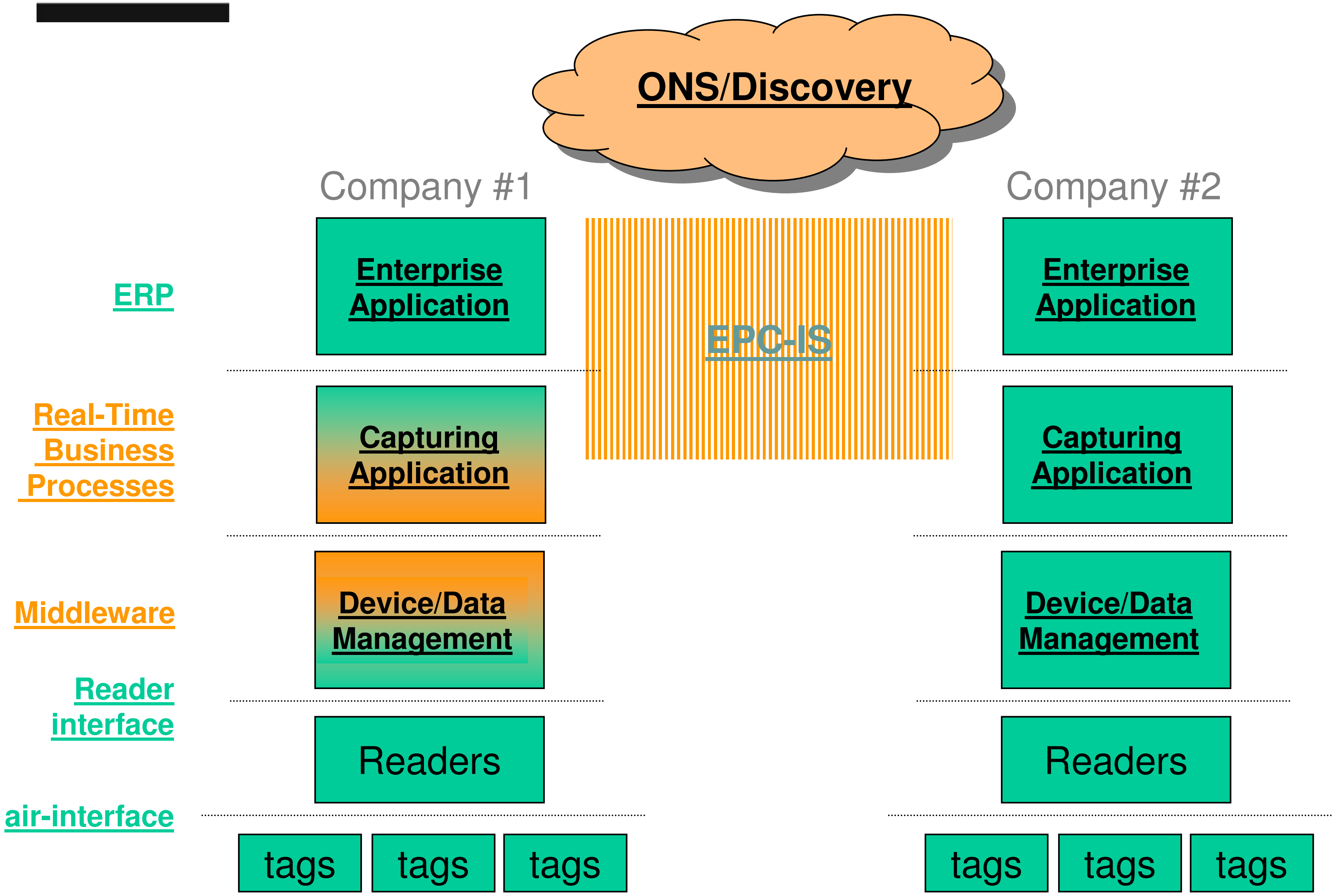
RFID: Today and the Future

Sanjay Sarma, MIT

AUTO-ID LABS

The Functional Stack Today



ONS/Discovery

Company #1

Company #2

ERP

Enterprise Application

EPC-IS

Enterprise Application

Real-Time Business Processes

Capturing Application

Capturing Application

Middleware

Device/Data Management

Device/Data Management

Reader interface

Readers

Readers

air-interface

tags

tags

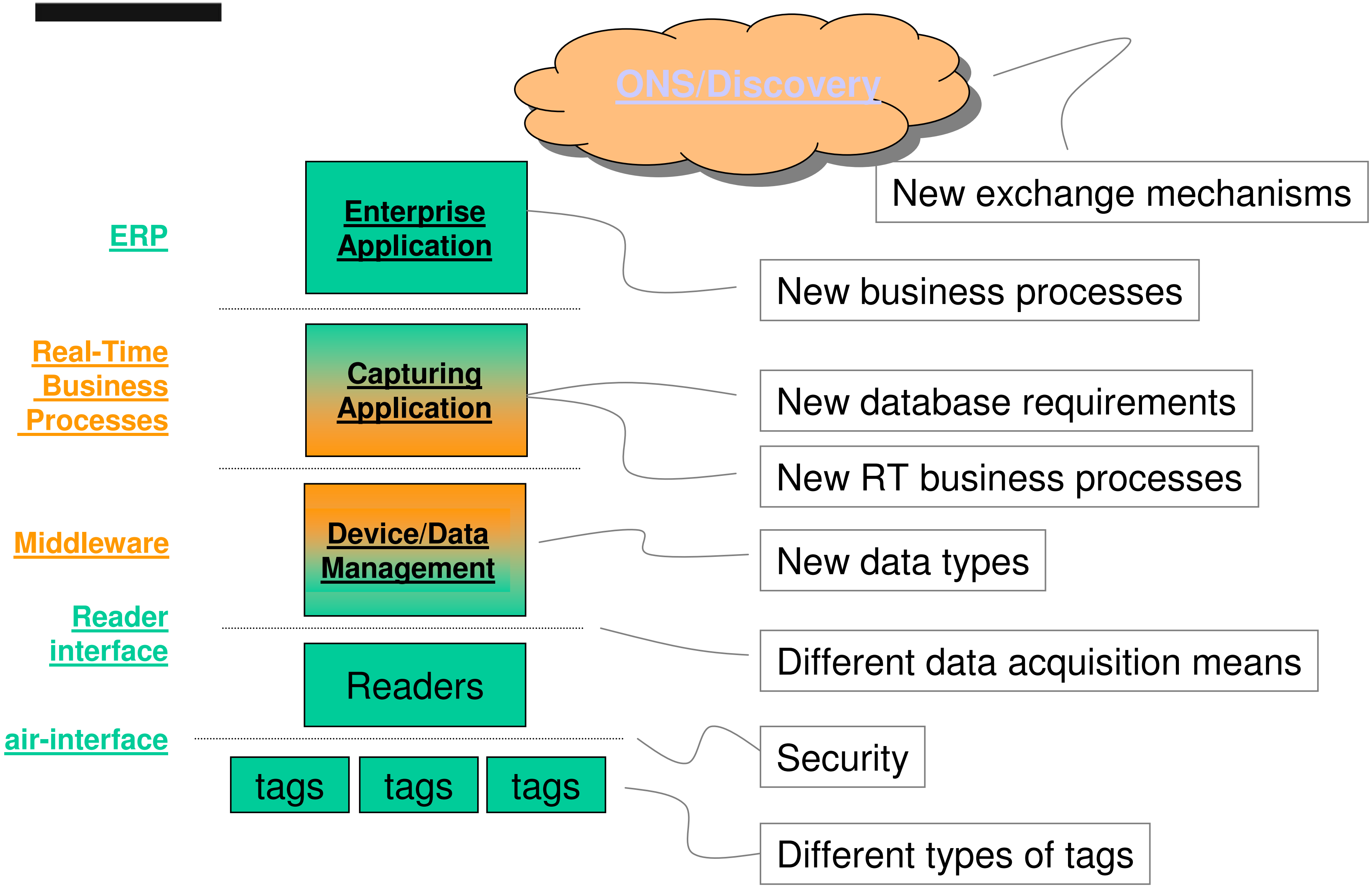
tags

tags

tags

tags

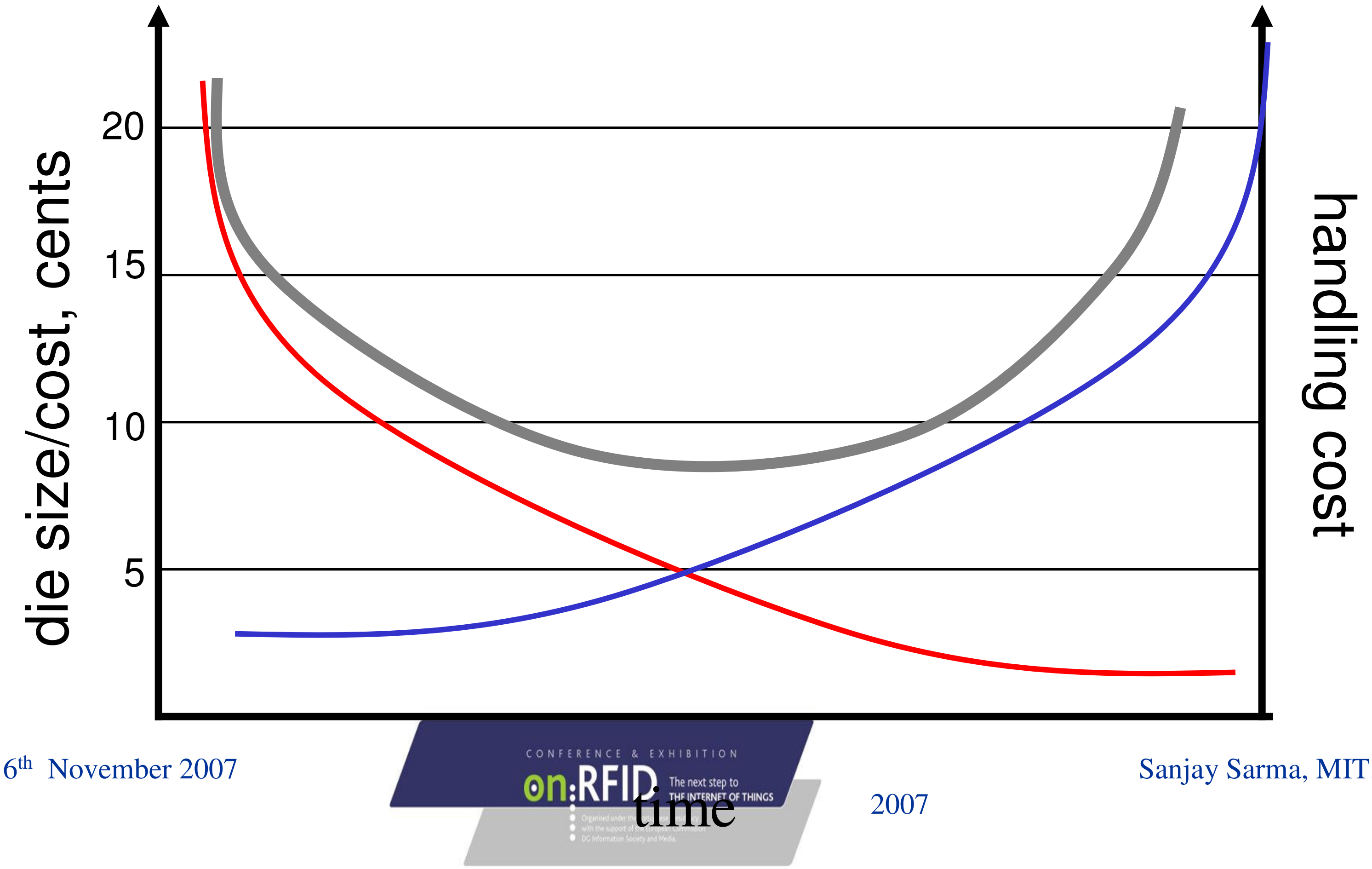
Preparing for Tomorrow



Tag Innovations

Low-cost RFID

Silicon: 4c/mm^2



Passive Tags

Constant struggle:

- Cost
- Range
- Functionality

New functionality:

- Security
- Extra memory
- Sensors

Security in Passive RFID Tags

Goals:

- Tag authentication (fighting counterfeits)
- Reader authentication
- Protection from Eavesdropping

Need encryption!

Sarma, S. E., Weis, S. A. and Engels, D. W., "RFID Systems and Security and Privacy Implications," Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), San Francisco, CA, August 12-15, 2002.

Encryption

- Tag has a one-way formula with a secret key
- Secret known by "authority" and tag
- Reader asks tag a question
  - If tag gives right answer, then good
  - If tag gives wrong answer, then bad
- Needs AES/DES type encryption

DES/AES

- “New Light-Weight Crypto Algorithms for RFID,” Axel Poschmann, Gregor Leander, Kai Schramm, Christof Paar, ISCAS 2007: 1843-1846.
- “AES Implementation on a Grain of Sand,” M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, *Information Security, IEE Proceedings*, vol. 152, no. 1, pp. 13–20, 2005.
- AES uses interleaving.
- DES promising, not shown yet.
- Expensive.

The challenge with encryption

- Expensive, though recent advances make it feasible
- Consumes power, so read-rate/range will diminish
- Slow, so performance will diminish
- Give it a few more years

New class of technologies

- Digital fingerprint of IC on tag
- Read/create that fingerprint at manufacturing
- Verify it on demand
  - Tag is un-clonable

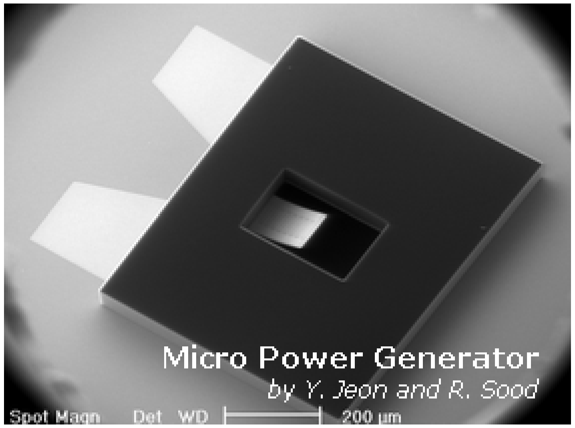
"Physical unclonable functions for device authentication and secret key generation" Edward Suh & Srinivas Devadas, Proceedings of the 44th annual conference on Design automation, 2007.

Tag Innovations: Memory

- Today, EPC has 96-bit ID though Gen 2 has more space
- Space for growth
- Extra memory can be expensive, slow, impact range
- Vendors working on up to 64KB tags

Tag Innovations: Sensors

- Sensors need power
  - Passive tags don’t have remote power
  - If reader present, reader can sense!
- Battery-assisted, or semi-passive tags
- Scavenged power (Professor Kim, MIT)
- Sensor transduction
- Data compression



Tag Innovations: Metal Performance

- Metamaterials
  - Split-ring resonators
  - Artificially “create space” between tag and metal

- “Miniaturized UHF tags based o metamaterials geometries”, Javier Dacuña, Rafael Pous. Bridge Project.
- “Some novel design for RFID antennas and their performance enhancement with metamaterials”, M. Stupf, R. Mittra, J. Yeo , J. R. Mosig, Microwave and Optical Technology Letters. 2007. Volume 49, Issue 4, Pages 858 – 867.

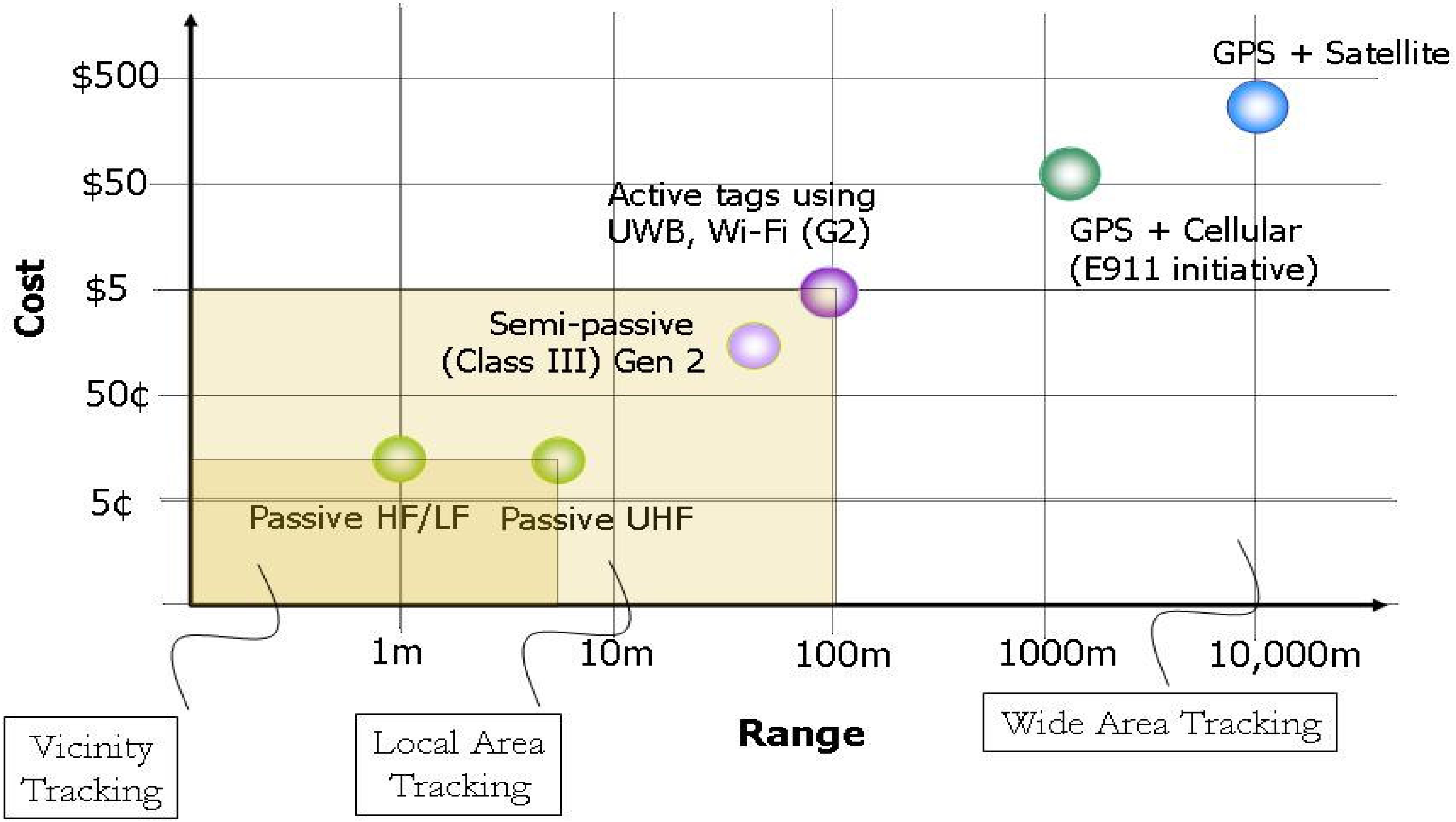
Tag Innovations: Actuators

- Imagine if you could write to a tag

  …. And turn on a switch!
- RFID can be transport-layer for many remote communications devices.
  - Electrical
  - Home entertainment
  - Power-meters, water-meters
  - Etc.
- Needs power and security

Beyond Passive RFID

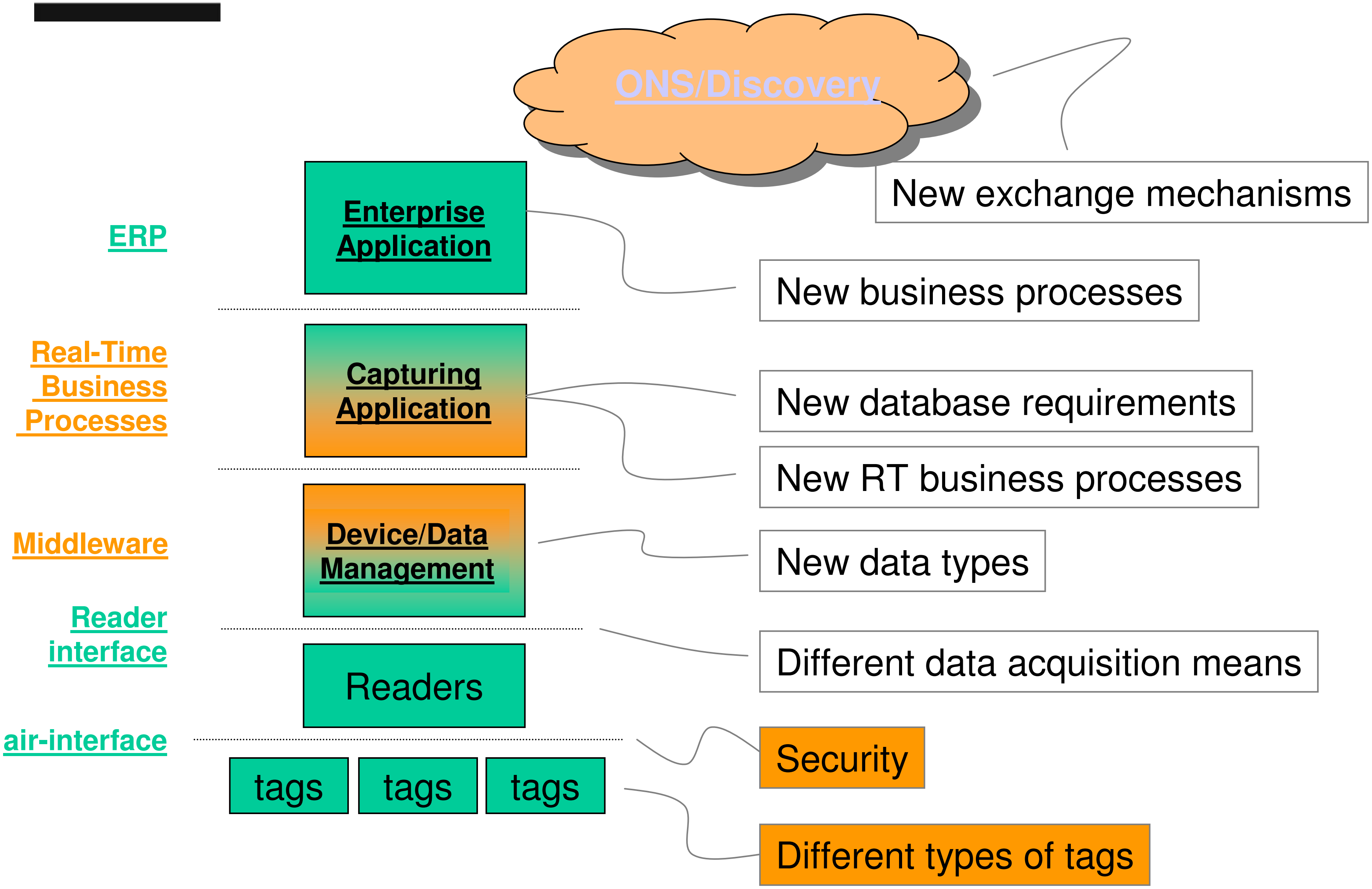
Mapping the Space



Active Tags

- WiFi
  - Low-power WiFi
  - WiFi with Real-Time Location Systems
  - Low-power Wifi with sensors
- Cellular
  - E911 in the US
  - Cell-phones with GPS and GPRS/3G backhaul
- WiMax?

Preparing for Tomorrow

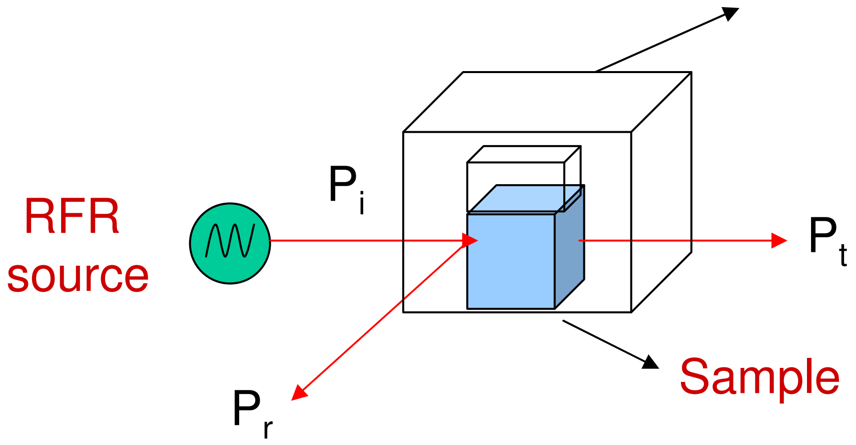


Reading

- Passive RFID readers
  - Application specific readers (ASR’s)
    - Focused functionality
    - Integrated backhaul
  - Distributed readers
  - Smart readers
  - Handhelds
- New read-attributes
  - Security
  - Signal strength
  - Angle-of-arrival
  - Phased-array radar
- WiFi Access Points
  - The router reports presence
  - RTLS Location servers (Cisco 2700 for example)
  - Location logic
- WAN
  - Interpreting GPS
  - Interpreting E911
  - Using NFC communication trail

Reader Influence

- RF frequencies: 125 KHz, 13.6 MHz, 915 MHz, 2.45 GHz.
- RF power – that which causes no significant thermal effect.
- Experimental setup:



Temperature controlled TEM cell

Sample

P_i, Incident power

P_r, Reflected power

P_t, Transmitted power

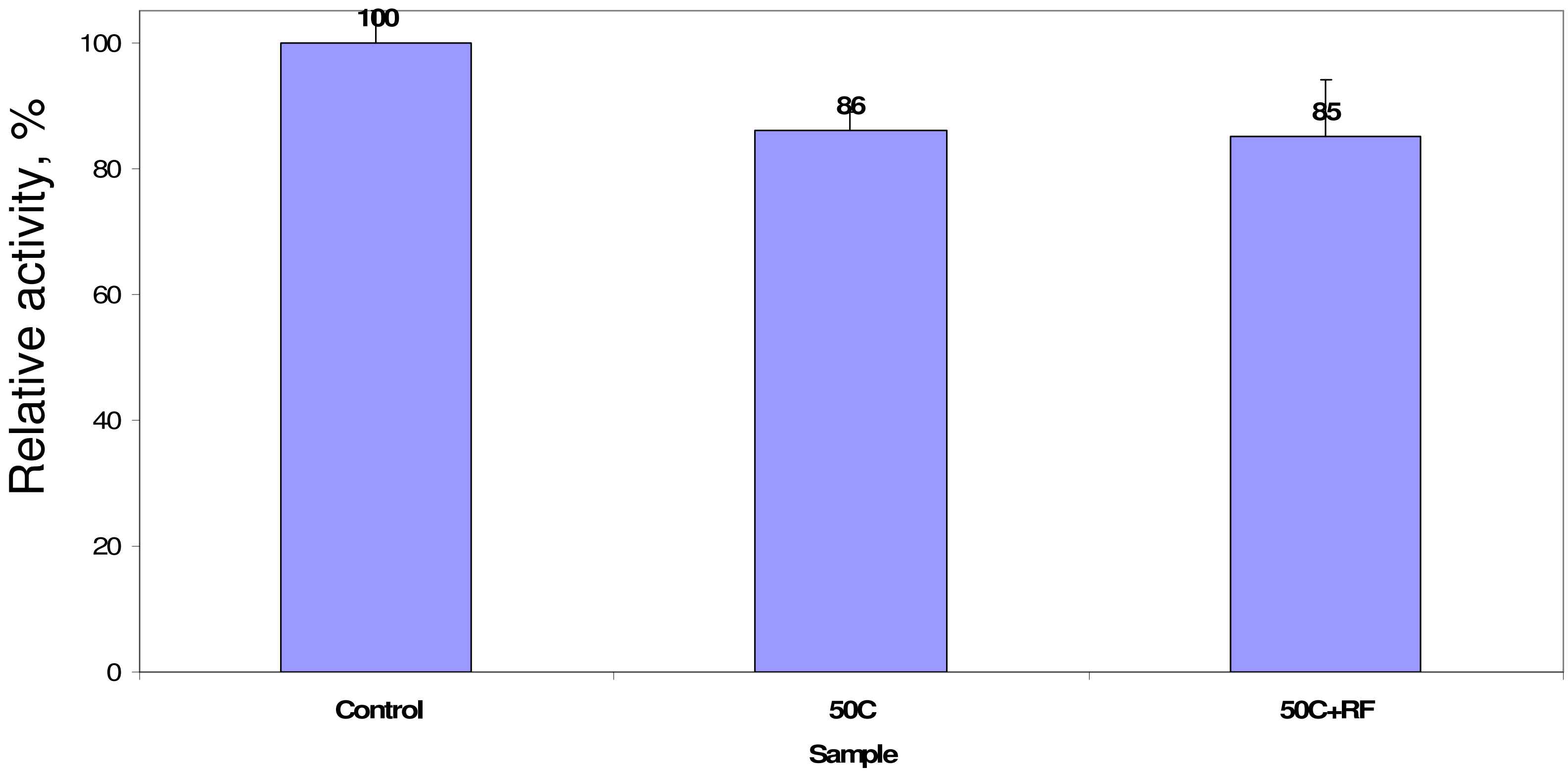
- Amount of RF power absorbed, P_a, will be measured.
  - $P_a = P_i - (P_r + P_t)$

- Temperature will be controlled.

Courtesv: Jennifer Schefiliti & Professor Klibanov. MIT

Preliminary Results

HRP enzymatic activity following exposure to RF (2.45GHz, 21W) at 50℃ for 24 hours

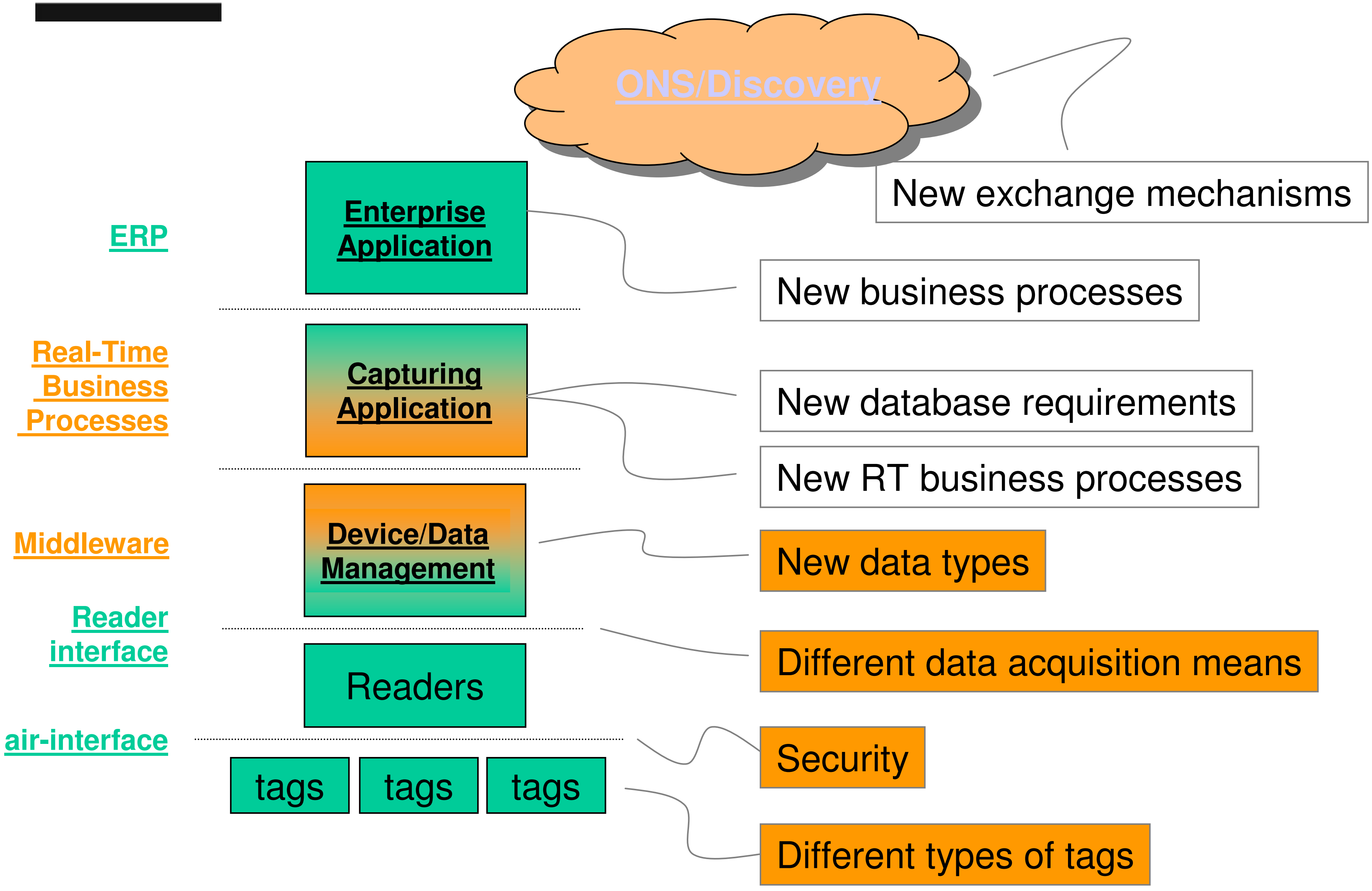


NO EFFECT SEEN ! ! !

Courtesy: Jennifer Schefiliti & Professor Klibanov, MIT

AUTO-ID LABS

Preparing for Tomorrow



ONS/Discovery

New exchange mechanisms

ERP

Enterprise Application

New business processes

Real-Time Business Processes

Capturing Application

New database requirements

New RT business processes

Middleware

Device/Data Management

New data types

Reader interface

Readers

Different data acquisition means

air-interface

tags

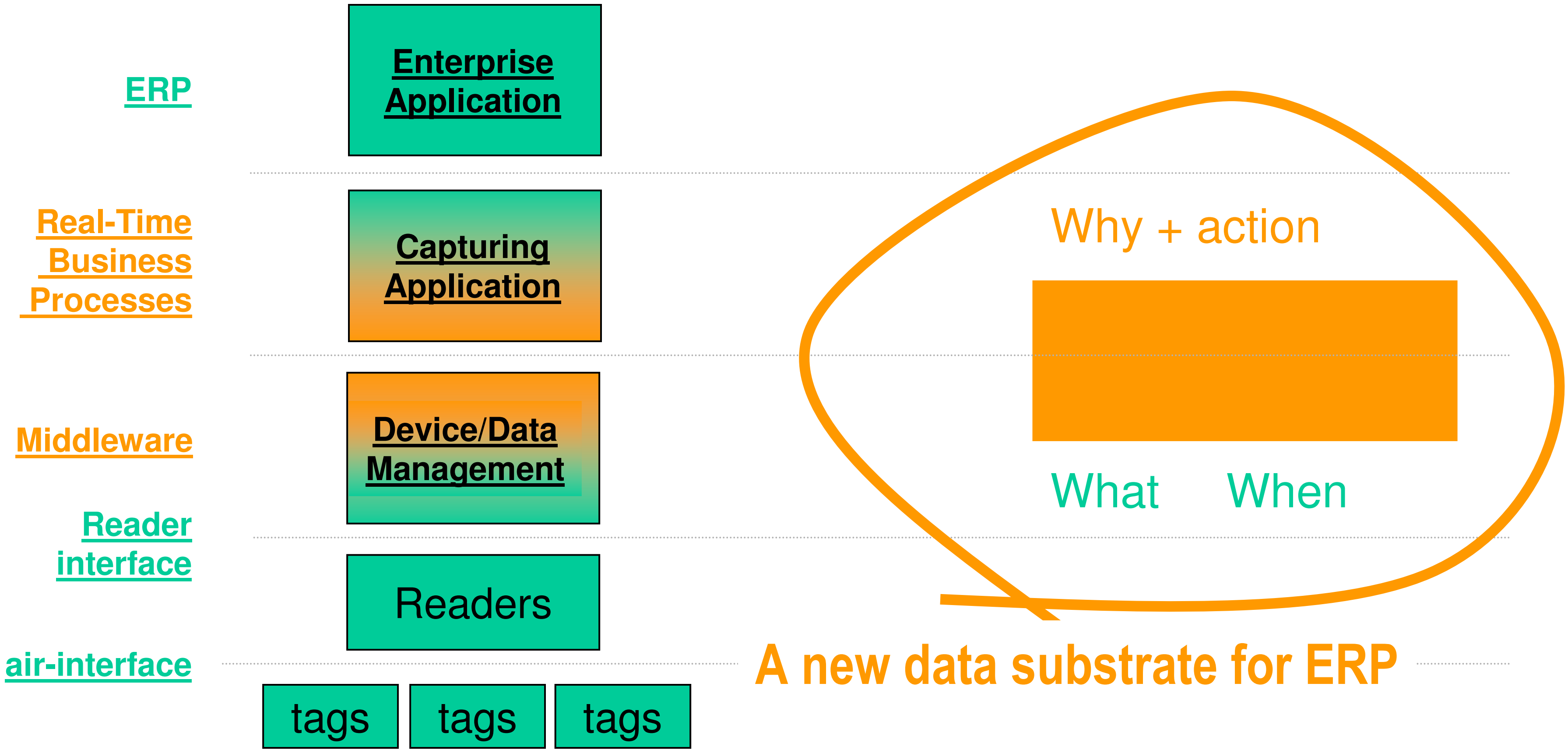
tags

tags

Security

Different types of tags

Real-time Business Processes



ERP

Enterprise Application

Real-Time Business Processes

Capturing Application

Middleware

Device/Data Management

Reader interface

Readers

air-interface

tags

tags

tags

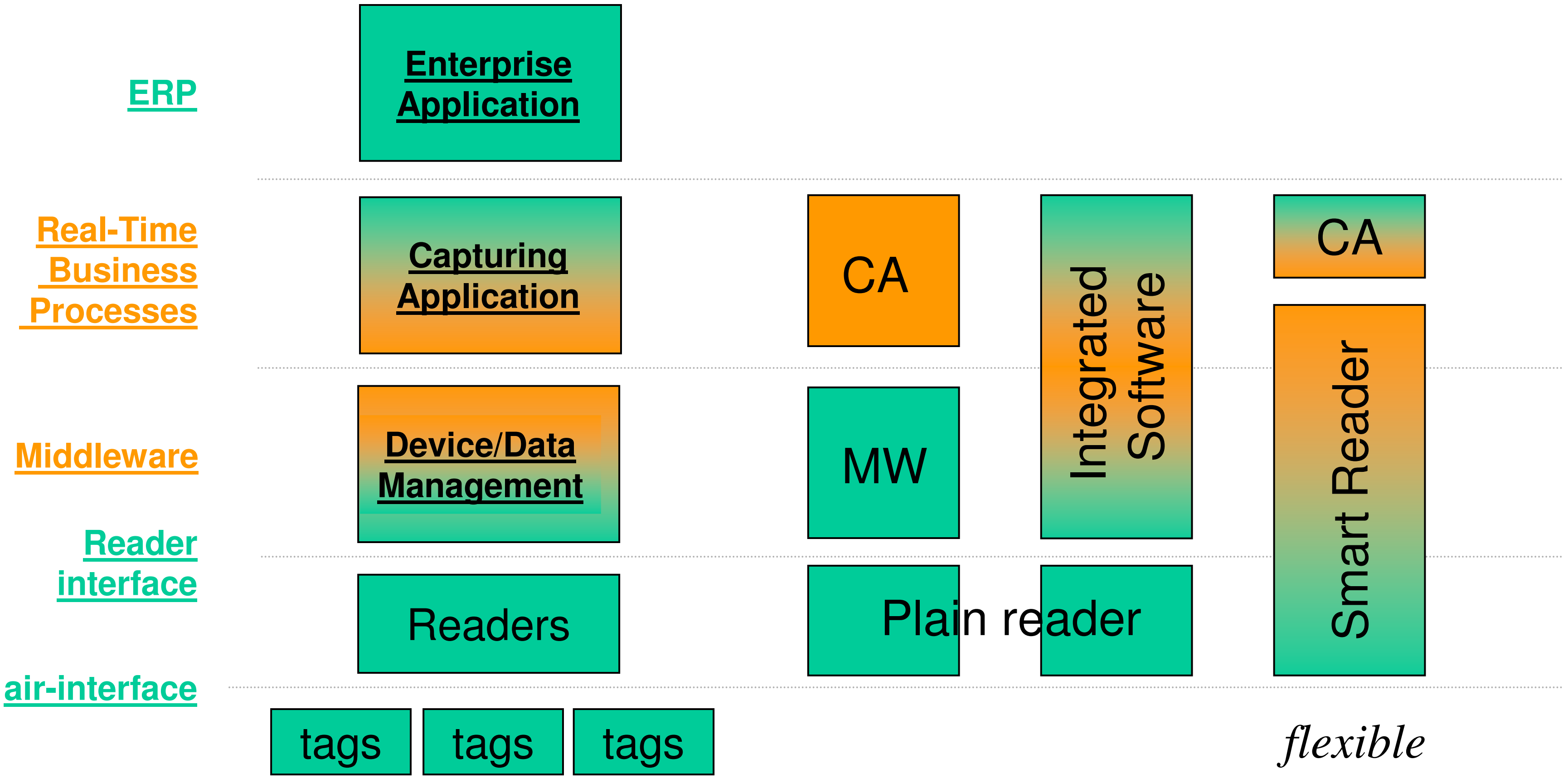
Why + action

What

When

A new data substrate for ERP

Different Modalities



ERP

Enterprise Application

Real-Time Business Processes

Capturing Application

CA

Integrated Software

CA

Middleware

Device/Data Management

MW

Smart Reader

Reader interface

Readers

Plain reader

air-interface

tags

tags

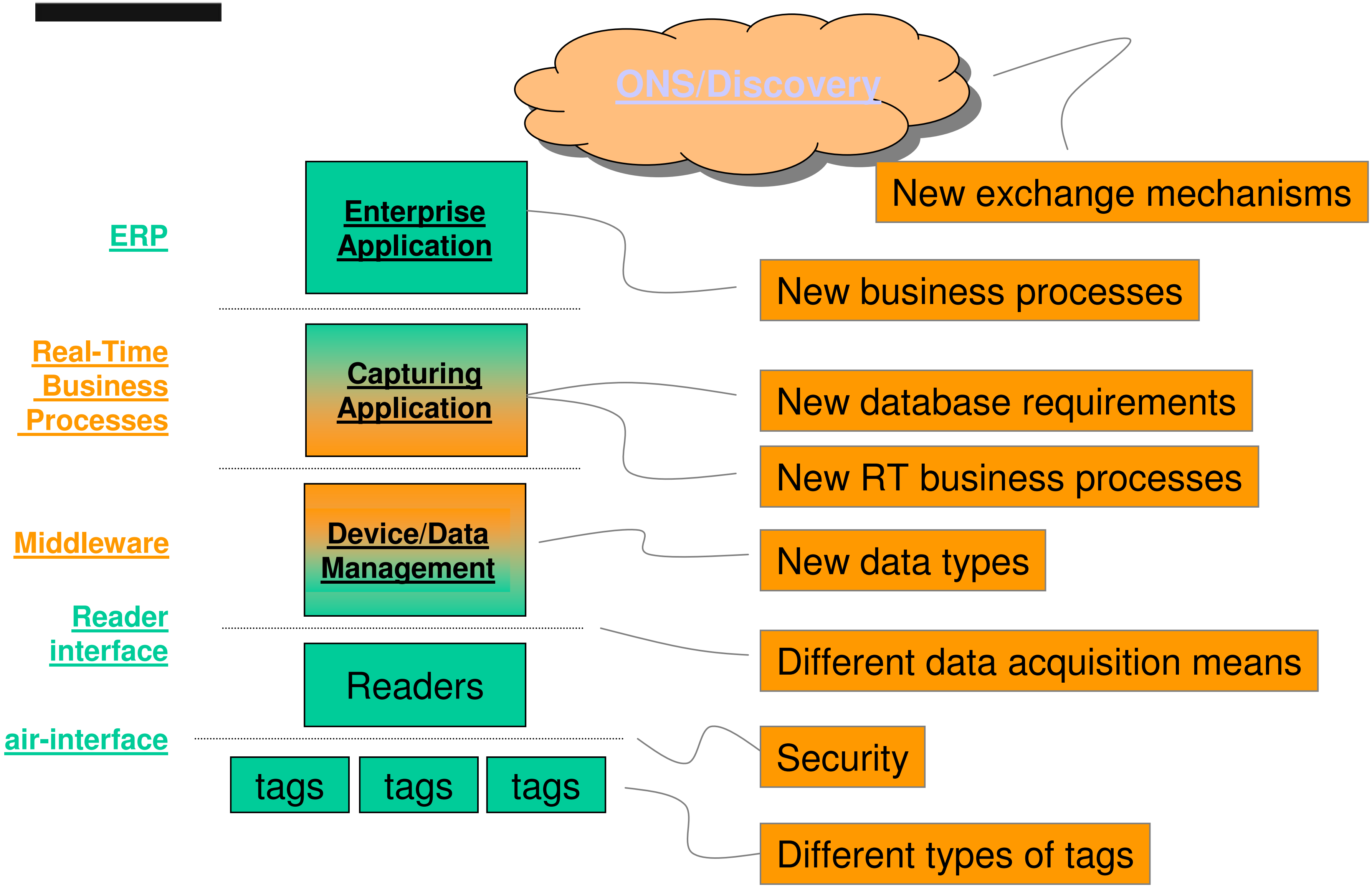
tags

flexible

New DB requirements

- Event-oriented
  - Close to, but not exactly, Complex Event Processing
- Self-healing
  - Missed reads
  - Spurious reads
  - Broken readers
  - Fail-safe inferencing
- Learning, data-mining software

Preparing for Tomorrow



ONS/Discovery

ERP

Real-Time Business Processes

Middleware

Reader interface

air-interface

Enterprise Application

Capturing Application

Device/Data Management

Readers

tags

tags

tags

New exchange mechanisms

New business processes

New database requirements

New RT business processes

New data types

Different data acquisition means

Security

Different types of tags

RFID will enable new business processes

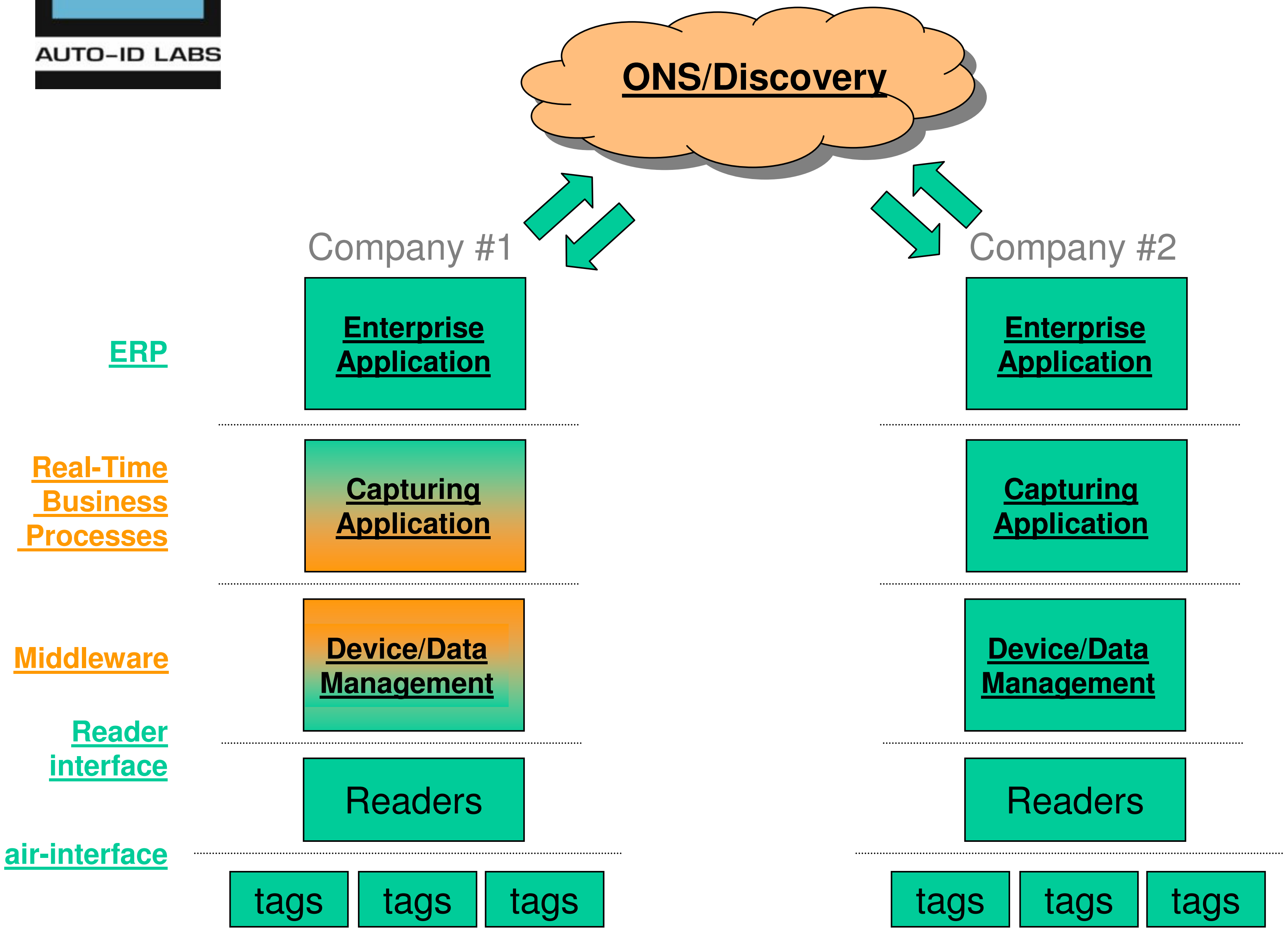
Of course it will help existing processes

- But it is important that the tail not wag the dog
- We are entering a newer, more chaotic world
- RFID will enable dynamic, real-time, reactive, jut-in-time processes.

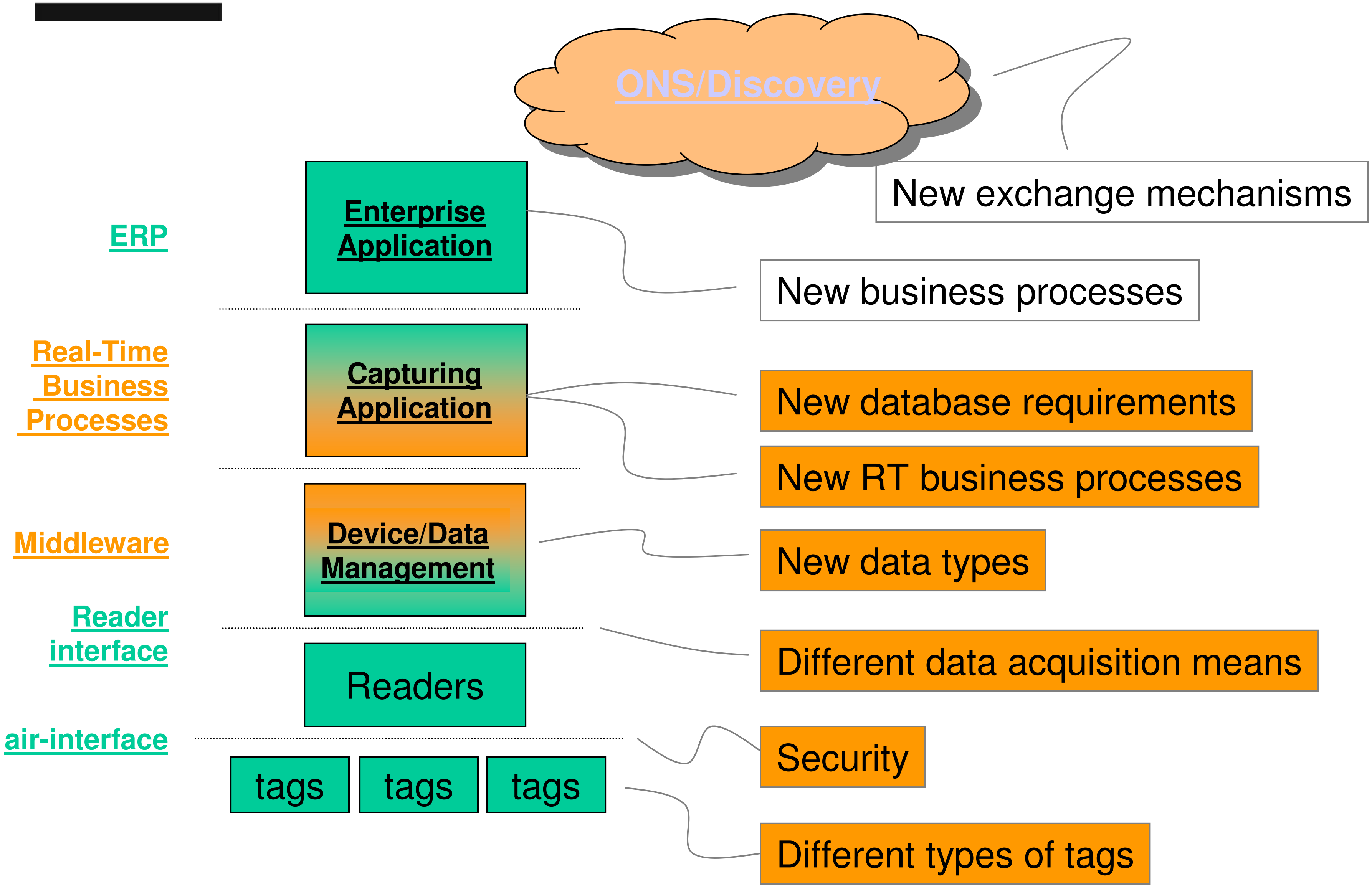
Discovery

	Past	Future
Retrieve	The initiator could ask where has this EPC has been.	The initiator could place standing request for information about an EPC in the future.
Post	The initiator could post information about an EPC for concerned parties most likely to possess an EPC now.	The initiator could post information about an EPC for the consideration of concerned parties in the future.

Discovery


ONS/Discovery
Company #1
Company #2
ERP
Real-Time Business Processes
Middleware
Reader interface
air-interface
Enterprise Application
Capturing Application
Device/Data Management
Readers
tags
tags
tags
Enterprise Application
Capturing Application
Device/Data Management
Readers
tags
tags
tags

Preparing for Tomorrow



ONS/Discovery

New exchange mechanisms

ERP

Enterprise Application

New business processes

Real-Time Business Processes

Capturing Application

New database requirements

New RT business processes

Middleware

Device/Data Management

New data types

Reader interface

Readers

Different data acquisition means

air-interface

tags

tags

tags

Security

Different types of tags

Conclusions

- RFID will cause a lot of change
  - Passive RFID has matured, will continue to improve
  - The landscape will expand
  - And enable new processes
- Do not paint yourself into a corner
- A great deal of creativity waits to be unleashed
- Think Internet 1995

Thank You

sesarma@mit.edu