

Security & Privacy on EPC Networks

2nd Canada-France Workshop on Foundations & Practice of Security

Joaquin Garcia-Alfaro
Carleton University

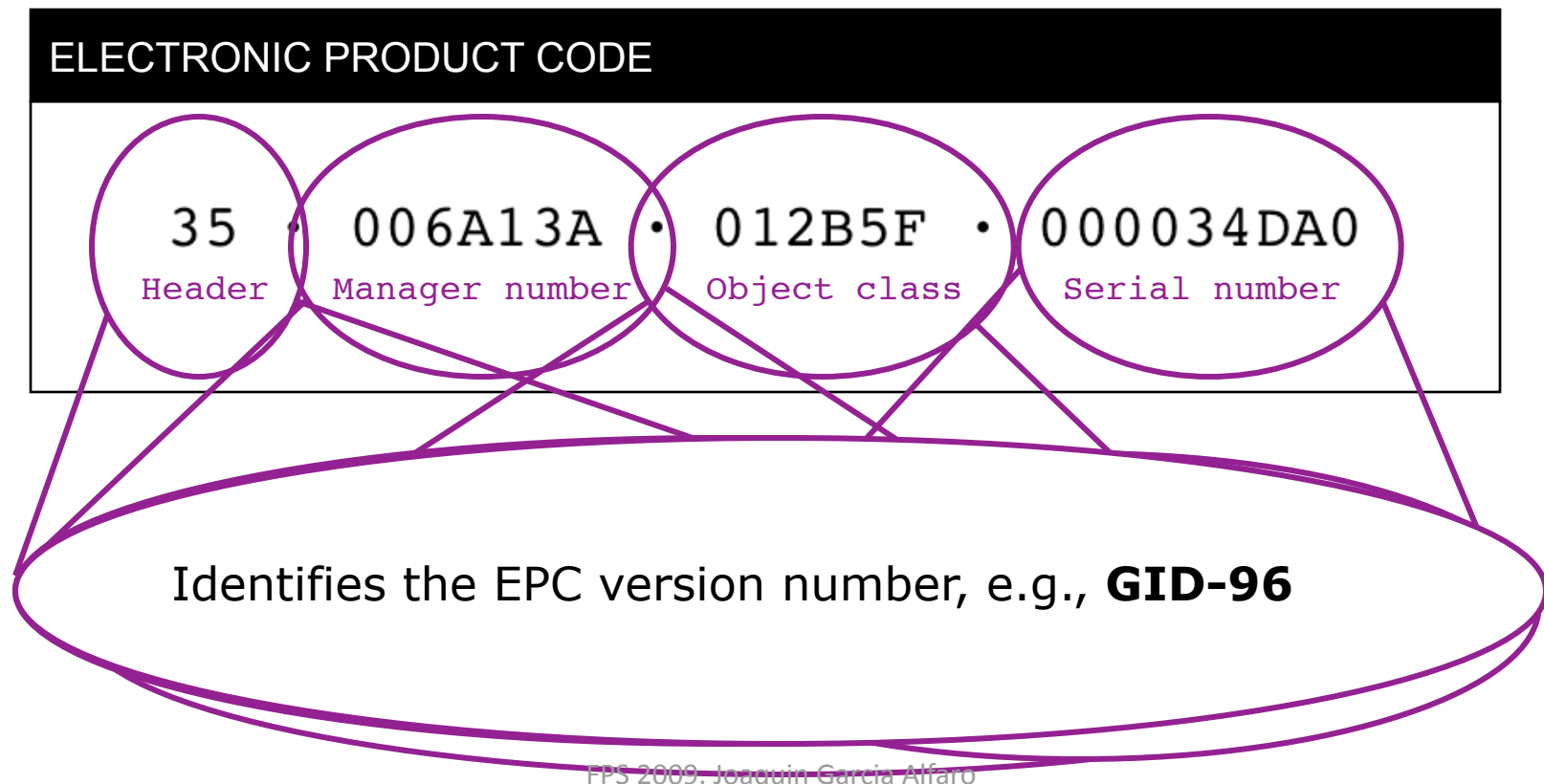
Joint work with
Michel Barbeau and Evangelos Kranakis

EPCGlobal Network

- Distributed infrastructure that enables physical objects to be connected to the Internet by using RFID technologies
- EPC: Electronic Product Code
 - Family of coding schemes to uniquely identify physical objects
- ONS: Object Name Service
 - Directory service that maps EPCs to Internet services

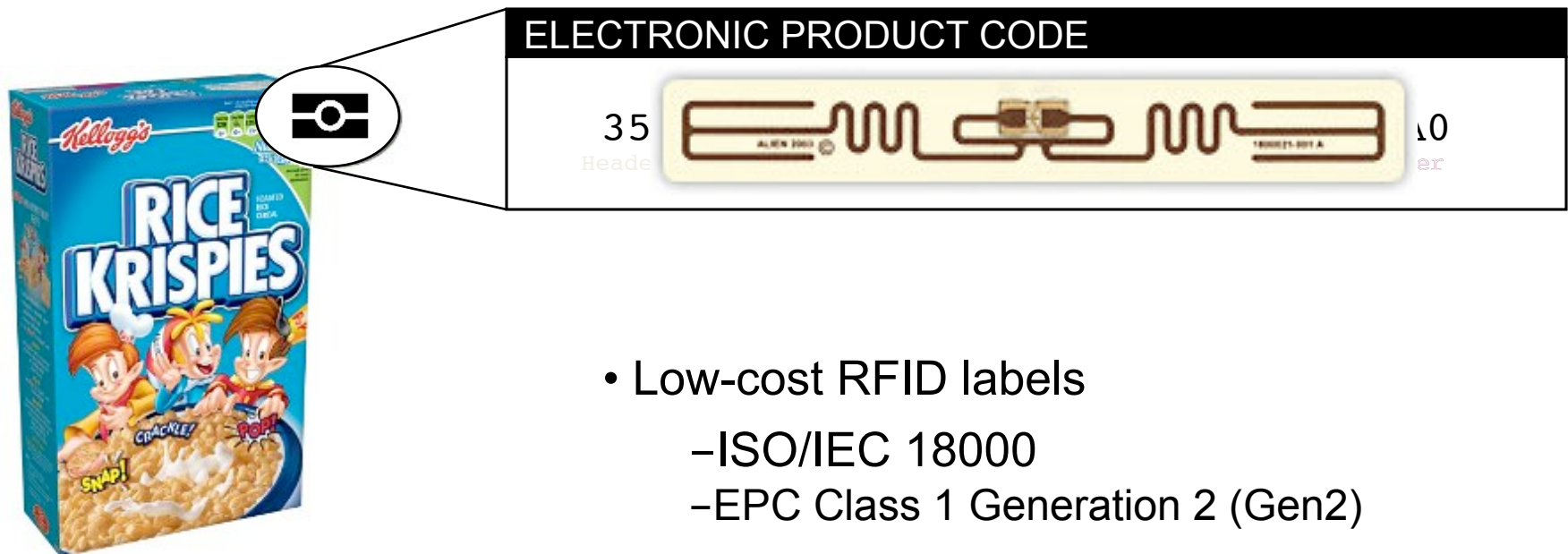
Electronic Product Code

- Successor of optical barcodes
- Sample representation of the EPC GID-96:



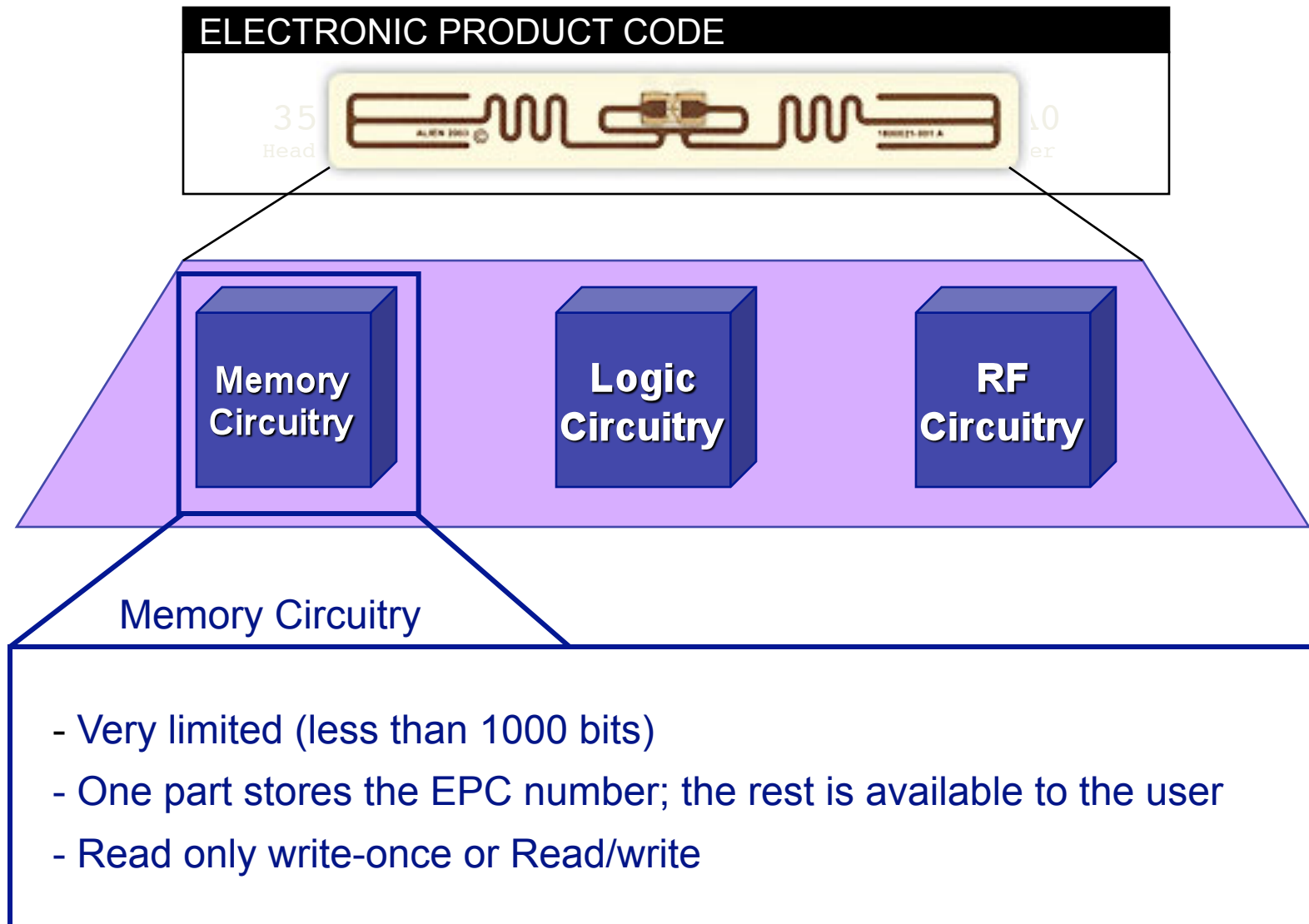
Electronic Product Code

- The EPC number is stored in an electronic label
- Using Radio Frequency technology, it “communicates” the code

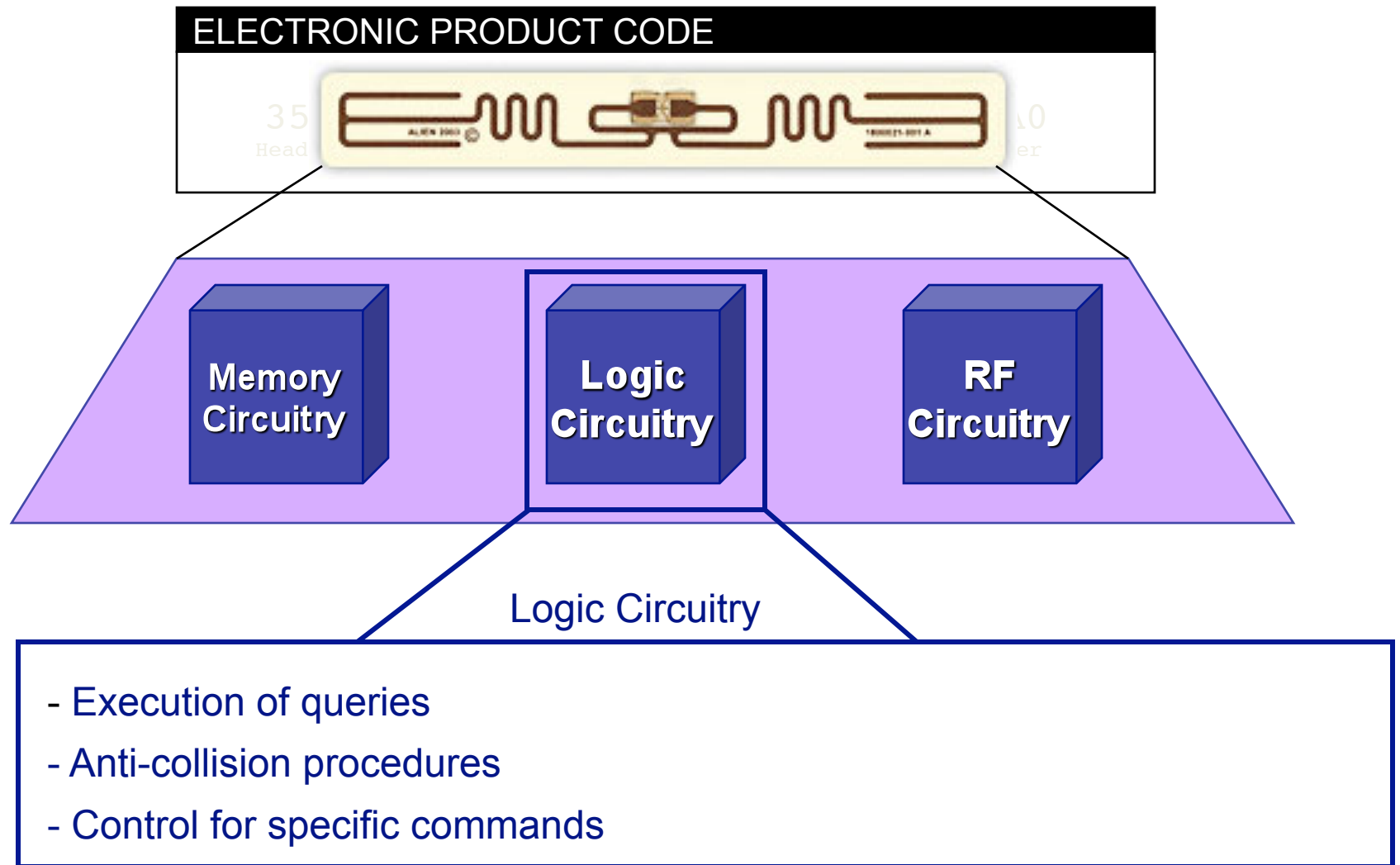


- Low-cost RFID labels
 - ISO/IEC 18000
 - EPC Class 1 Generation 2 (Gen2)

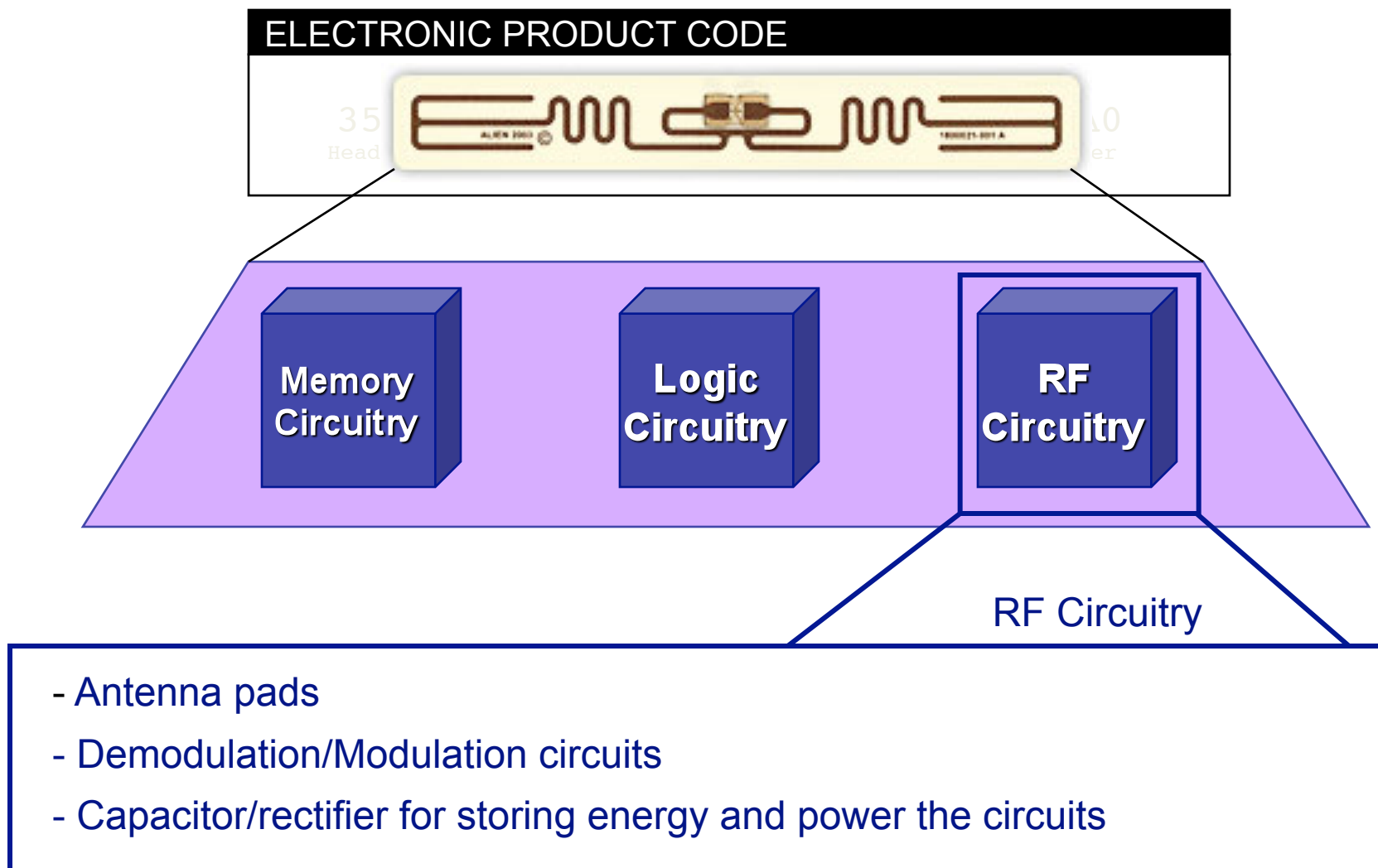
EPC Gen2 tags



EPC Gen2 tags



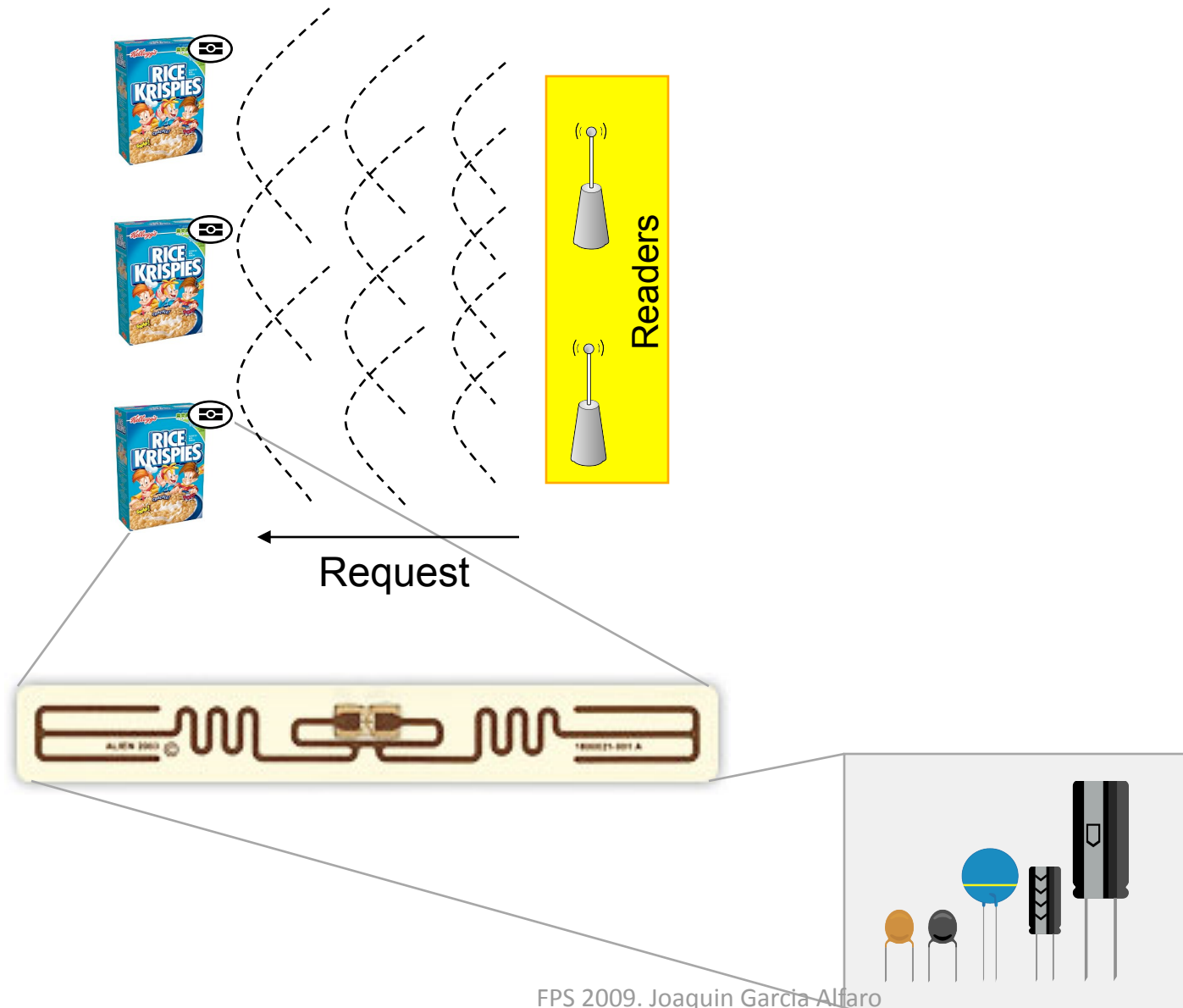
EPC Gen2 tags



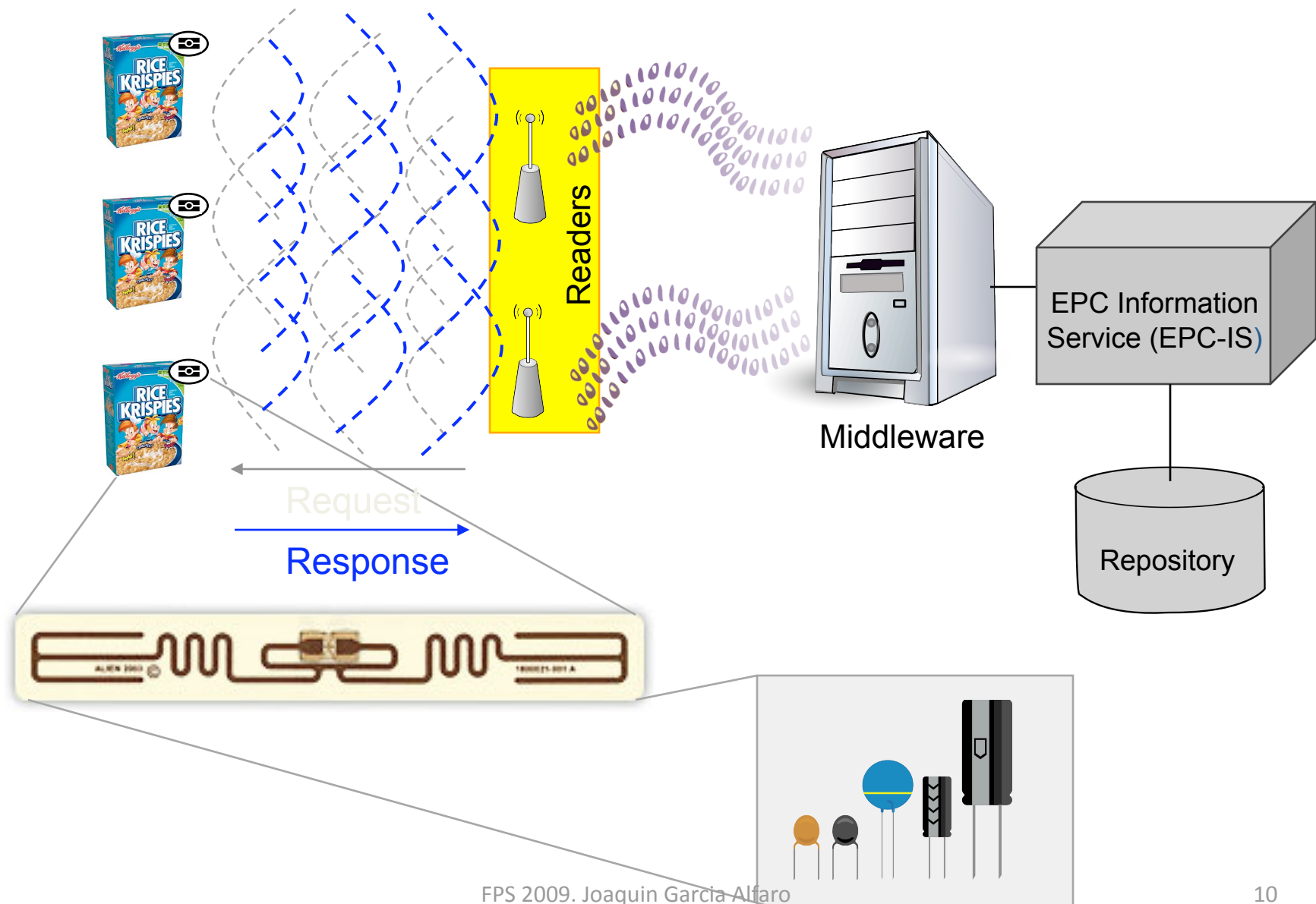
Tags & readers



Sample EPC network

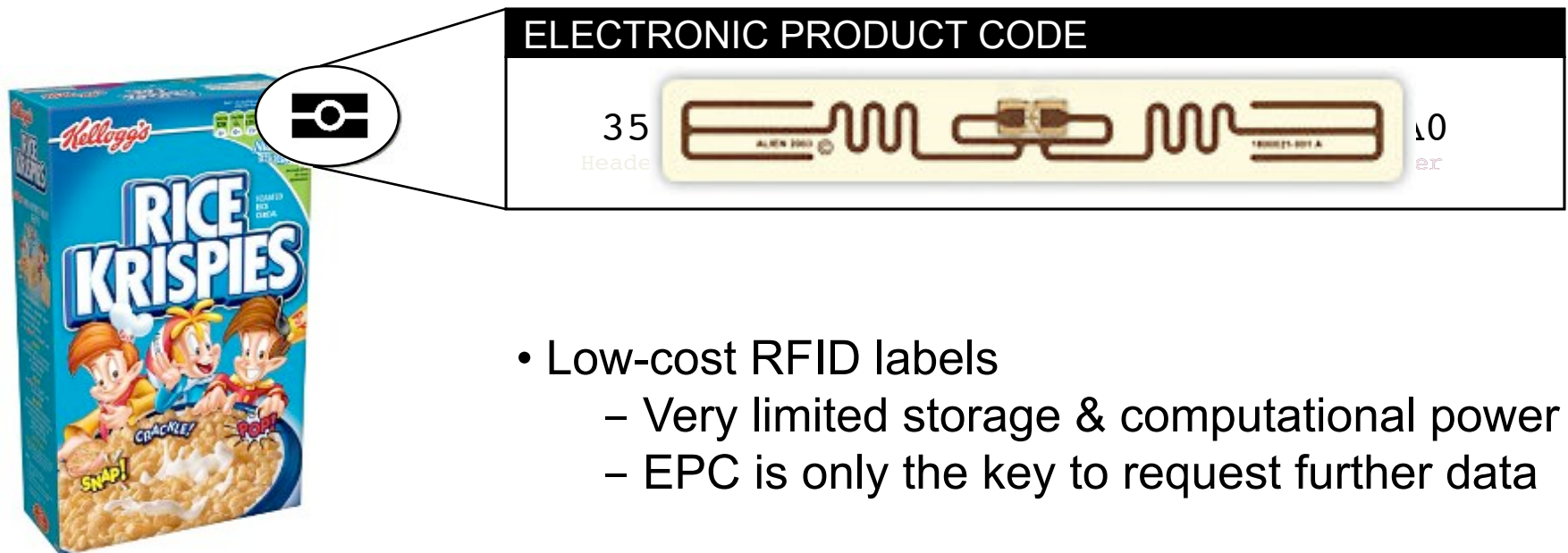


Sample EPC network



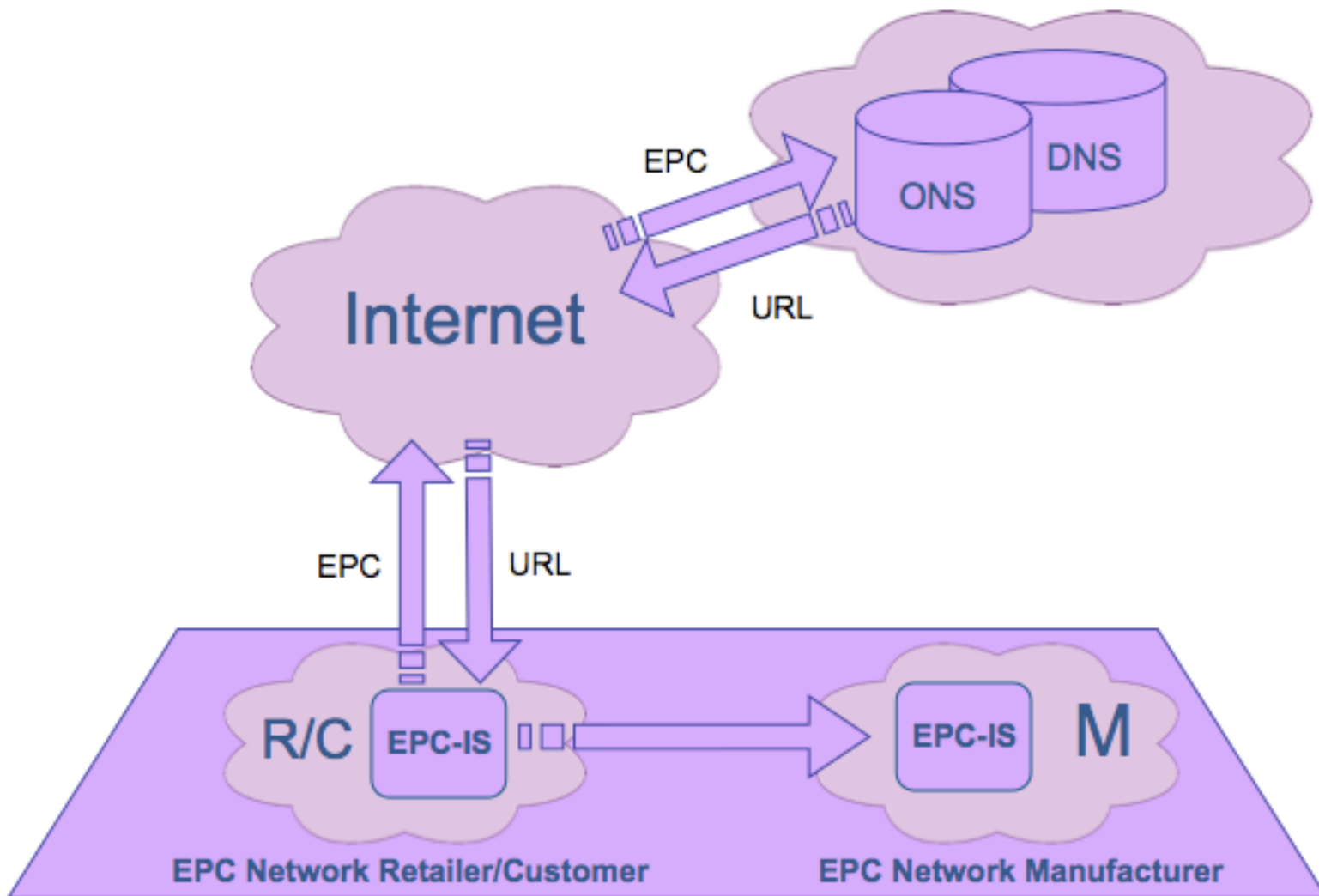
Electronic Product Code

- The EPC number is stored in an electronic label
- Using Radio Frequency technology, it “communicates” the code



- Low-cost RFID labels
 - Very limited storage & computational power
 - EPC is only the key to request further data

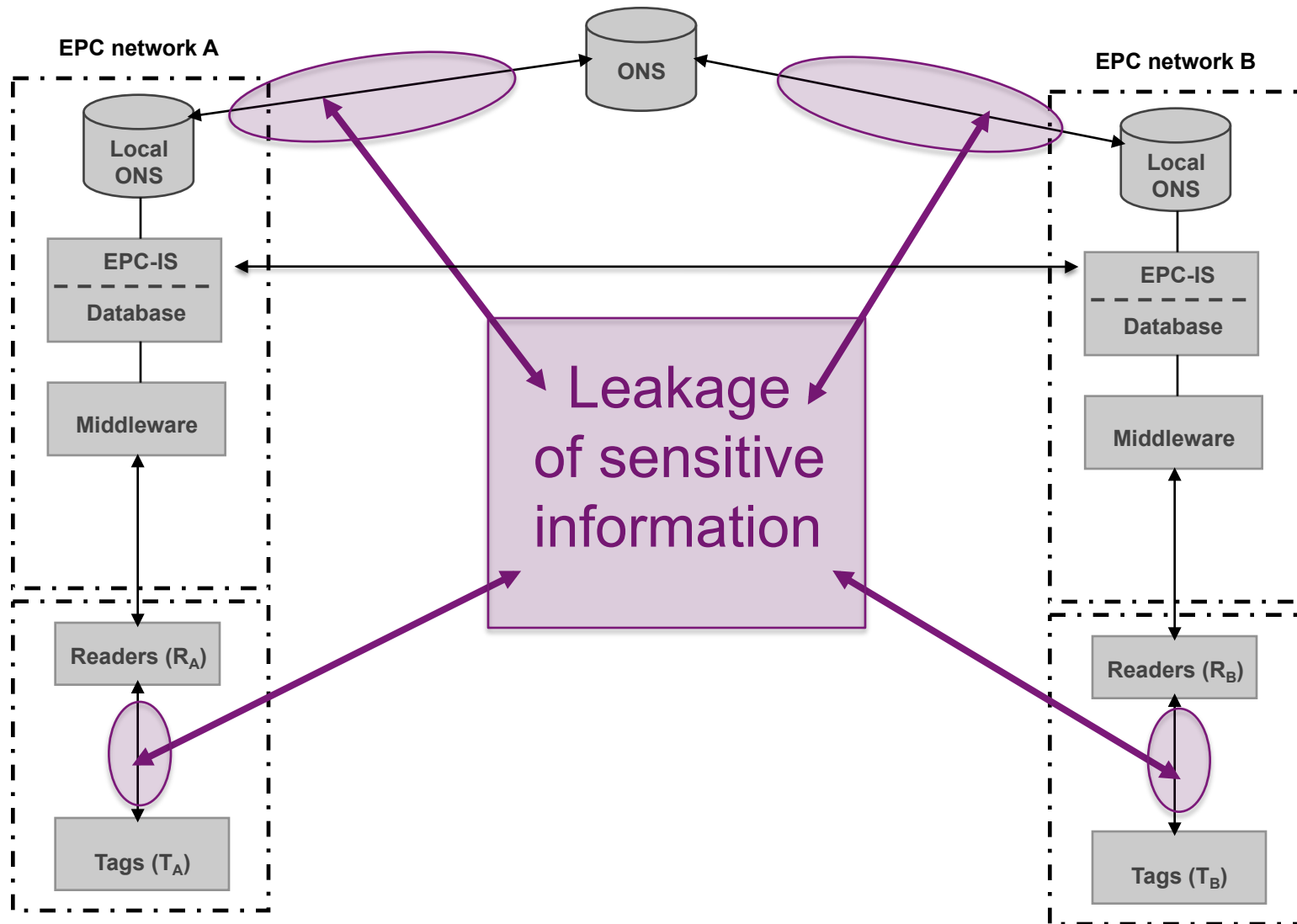
Interoperability between EPC Networks



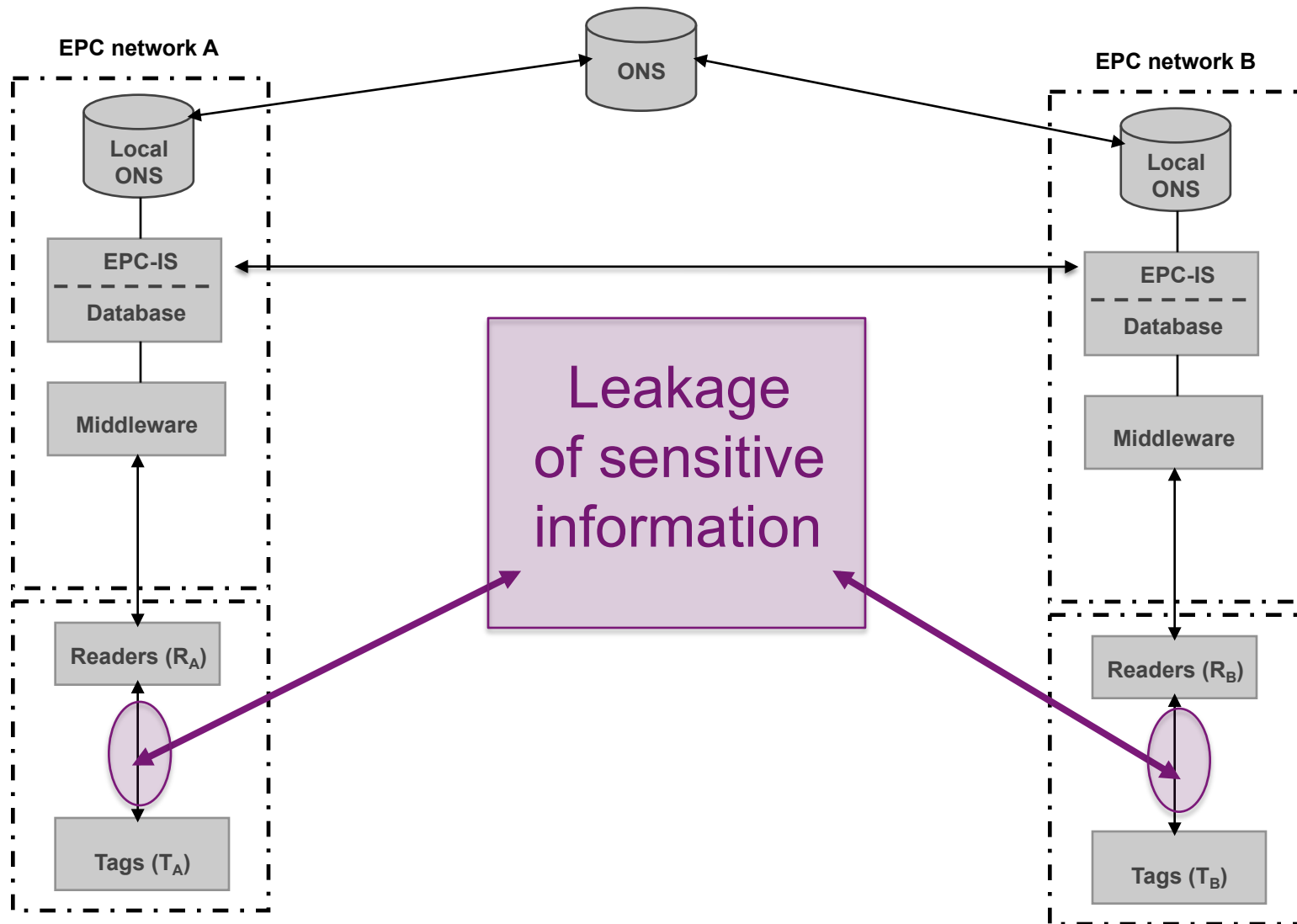
Threats to EPC networks

- Can target the different components of the infrastructure
- We focus on threats targeting the wireless channel between readers and tags & the ID resolution on the Internet

Threats to EPC networks



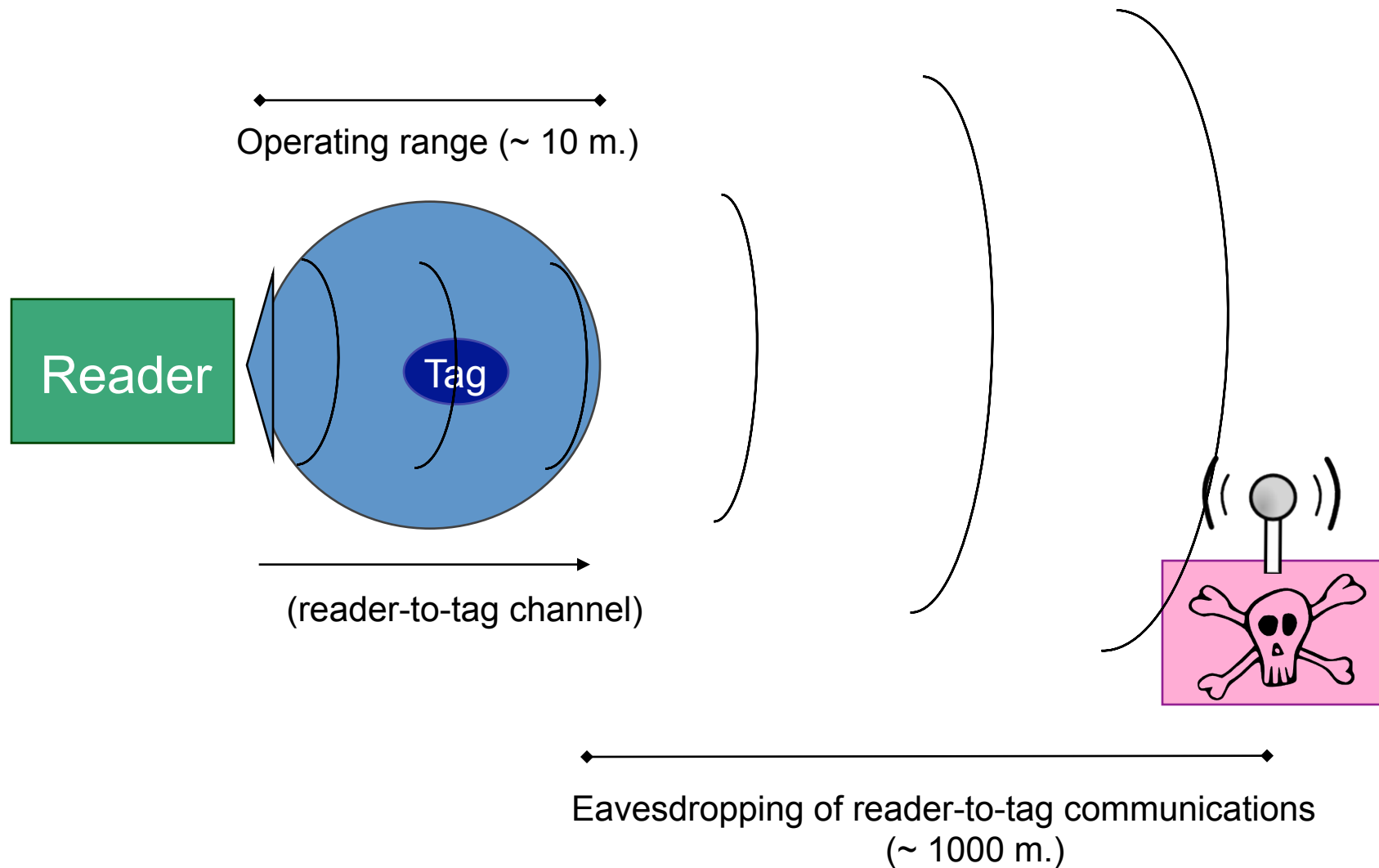
Threats to EPC networks



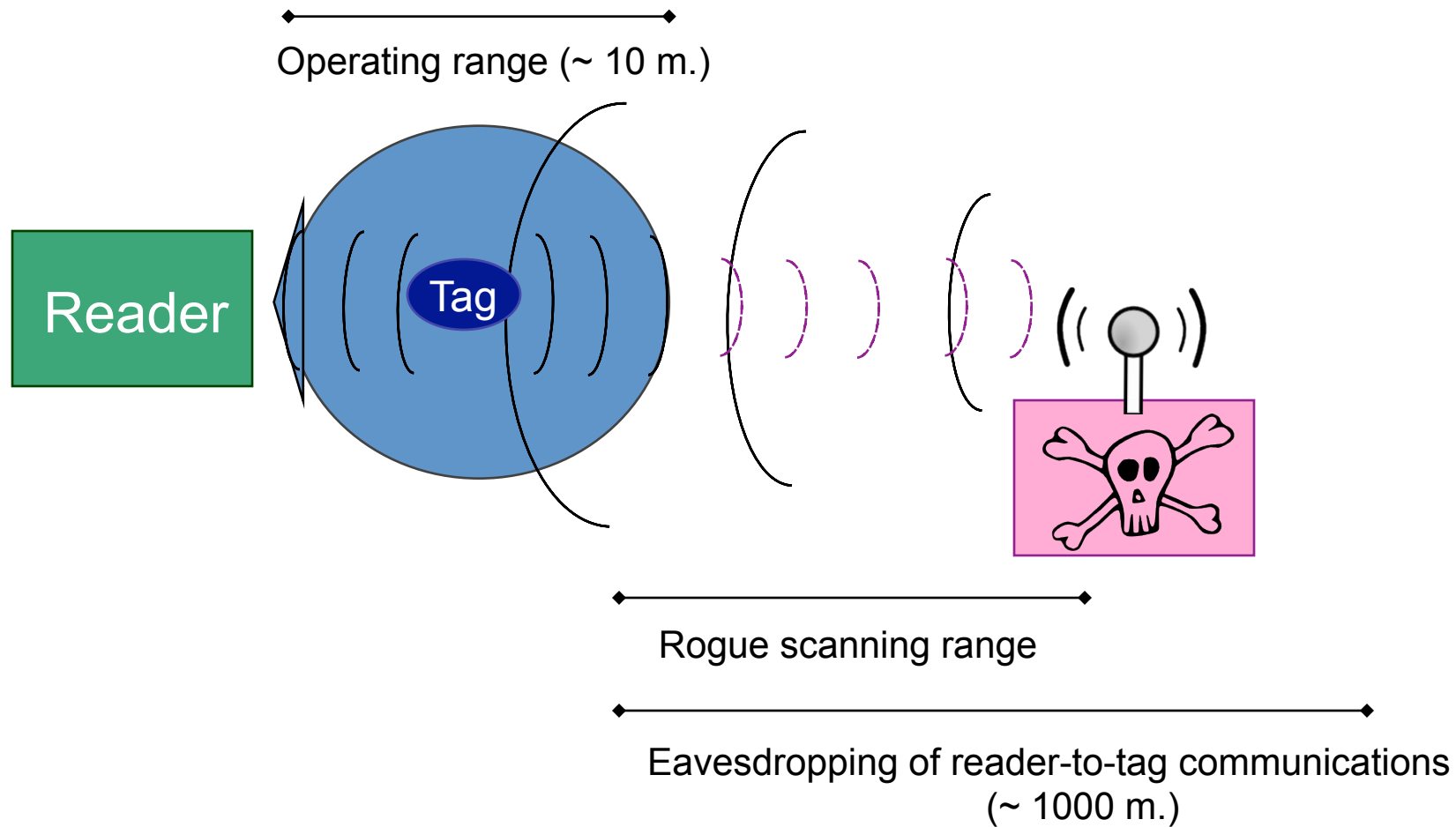
Threats targeting the wireless channel

- Security features on EPC are minimalist
 - Kill & Access command
- Communication over insecure channel
 - Lack of authentication & confidentiality
- Read-range distances sufficient to allow eavesdropping ...
 - ... if we consider a dishonest third party using highly sensitive receivers, special antenna, etc.

Eavesdropping reader channel

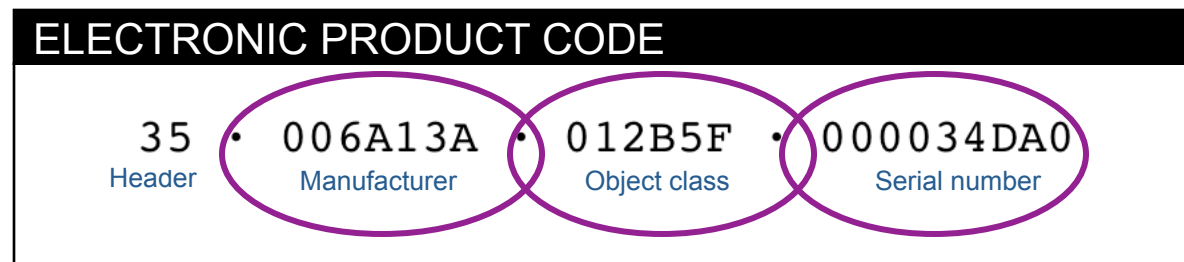


Rogue scanning



Disclosure of information

- Which information can be disclosed? the EPC number associated to a tagged object

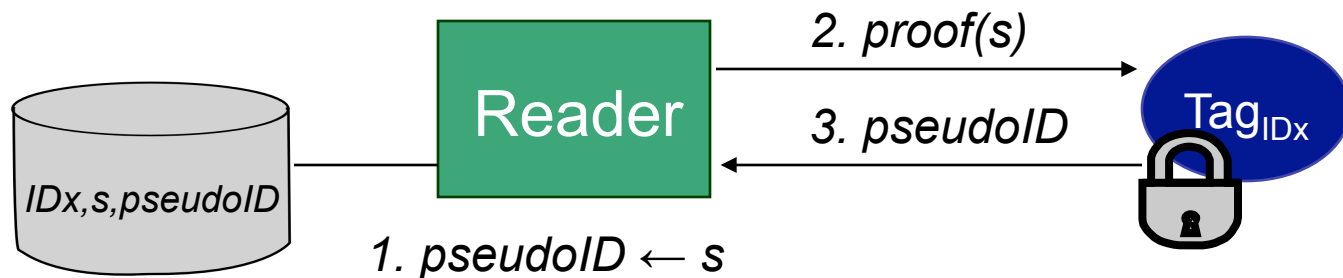


- Can lead to clandestine inventory, tracking, profiling, ...
 - For retailers, impact might be rated as medium
 - For holders of objects on health care or military scenarios, impact can be rated as high

How to deal with these threats ?

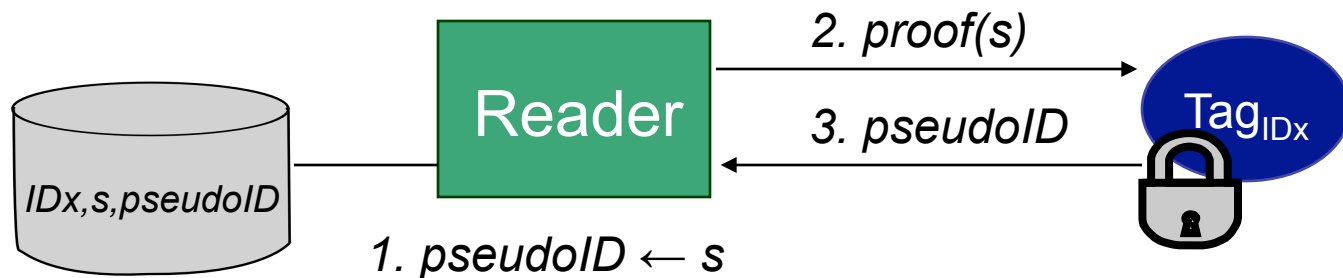
- Shielding, jamming, blockers, guardians, ...
 - It may work on some RFID applications
 - Requires the management of new components
- Use of low-overhead and lightweight authentication
 - Pseudo-randomness and XOR masking

Lock-based Access Control



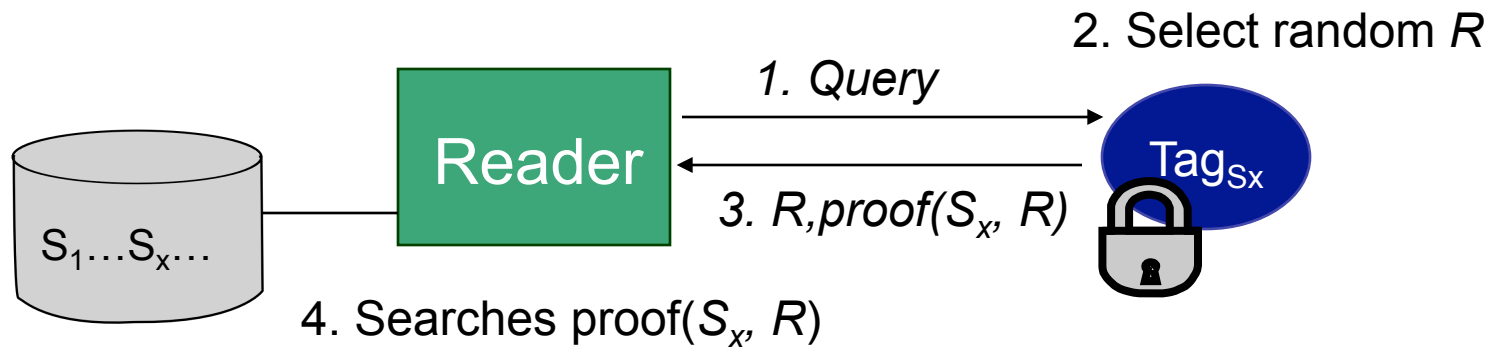
- Readers and tags share a common secret (s)
- When tag receives a proof of this secret, it locks itself
→ when interrogated, it only responds with a pseudonym
- Tag unlocks itself when it receives again a proof of secret

Lock-based Access Control



- It may handle eavesdropping and rogue scanning, but still allows location & tracking
- Adversaries should not be able to get useful information about the item for tracking or discovering tag identity !

Randomized Lock-based Access Control



[Garcia-Alfaro, Barbeau, Kranakis, 2009] *A Proactive Threshold Secret Sharing Scheme Handling Gen2 Privacy Threats*, March 2009.

Proof-of-concept



ELECTRONIC PRODUCT CODE

35
Head



10
er

EPC C1G2 Reader

S=Proj(Pool(1:18,1:10)) mod 31:

23	20	24	16	01	19	26	03	28	26	30	18	01	19	29	04	26	18
20	29	13	07	11	08	22	07	08	00	18	26	23	24	12	00	12	13
24	13	02	00	03	20	17	03	20	29	06	08	08	24	16	02	00	26
16	07	00	12	23	28	02	07	20	17	20	09	08	16	19	21	11	00
01	11	03	23	14	04	17	26	23	20	24	09	04	26	10	30	03	25
19	08	20	28	04	07	12	18	20	14	27	01	07	20	13	20	18	23
26	22	17	02	17	12	11	24	11	27	29	28	23	02	28	13	30	10
03	07	03	07	26	18	24	14	21	01	30	08	26	05	15	20	15	06
28	08	20	20	23	20	11	21	17	09	18	23	21	15	26	28	22	12
26	00	29	17	20	14	27	01	09	18	22	03	27	04	16	05	06	14
30	18	06	20	24	27	29	30	18	22	03	22	19	29	27	13	29	13
18	26	08	09	09	01	28	08	23	03	22	08	16	10	08	09	23	08
01	23	08	08	04	07	23	26	21	27	19	16	28	15	08	04	14	22
19	24	24	16	26	20	02	05	15	04	29	10	15	09	18	23	25	11
29	12	16	19	10	13	28	15	26	16	27	08	08	18	12	23	30	24
04	00	02	21	30	20	13	20	28	05	13	09	04	23	23	29	01	26
26	12	00	11	03	18	30	15	22	06	29	23	14	25	30	01	02	30
18	13	26	00	25	23	10	06	12	14	13	08	22	11	24	26	30	20

Pool of shares:

13	27	14	11	15	27	26	28	01	05	26	18	03	10	02			
05	01	04	10	06	17	01	14	28	16	19	06	15	03	29			
11	18	25	12	29	02	03	03	15	02	07	28	11	22	16			
07	26	29	25	11	12	28	20	22	04	21	24	05	15	30			
19	19	08	02	19	07	02	10	10	29	15	16	24	06	18			
20	16	15	18	04	14	10	26	06	19	24	27	23	29	06			
03	25	21	21	01	05	04	24	19	21	04	14	16	23	03			
27	14	30	05	25	18	15	12	16	27	16	08	08	16	10			
02	30	22	09	05	10	13	23	26	17	03	30	25	02	13			
25	02	02	30	30	30	12	15	03	08	14	05	20	26	20			
10	15	26	08	09	29	20	07	02	07	27	22	17	08	26			
16	11	12	14	03	16	16	30	25	15	30	11	10	07	04			
21	13	19	16	24	24	14	19	08	13	11	01	29	19	09			
08	17	18	19	20	20	11	25	12	20	01	13	28	20	14			
22	03	01	06	10	19	08	04	27	18	17	23	30	18	01			
15	07	11	29	22	08	05	27	04	01	05	19	19	21	27			
28	12	23	26	16	11	23	29	09	30	12	21	02	25	22			
26	10	09	17	28	22	07	17	11	23	23	02	14	01	25			
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18

Info about last item:

Bin:0111011101001010101101101101001010011000001000110010011000101000 (90 bits)

Hex:0E1D06151B161AA09180510081C13110414 (18 elements)

Vec[14;29;06;21;27;22;26;10;09;24;05;16;08;28;19;17;04;20] (18 elements)

Already in pool.

(linearly dependent with respect to share Pool[14])

Info about last item

ONS lookup

10-18 sim.

02-03 sim.

+1

Clear

Reset

EPC C1G2 Reader

S=Proj(Pool(1:18,1:10)) mod 31:

Pool of shares:

13 27
05 01
11 18
07 26
19 19
20 16
03 25
27 14
02 30
25 02
10 15
16 11
21 13
08 17
22 03
15 07
28 12
26 10
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18

Info about last item:
Bin:0111011101001101010111011101101001001001110000010110000010001110010011100010010010100 (90 bits)
Hex:0x0E1D06151B161A0A09180510081C13110414 (18 elements)
Vec:[14;29;06;21;27;22;26;10;09;24;05;16;08;28;19;17;04;20] (18 elements)
Already in pool.
(linearly dependent with respect to share Pool[14])

Info about last item

ONS lookup

10-18 sim.

02-03 sim.

+1

Clear

Reset

S=Proj(Pool(1:18,1:10)) mod 31:

23 20 24 16 01 19 26 03 28 26 30 18 01 19 29 04 26 18
 20 29 13 07 11 08 22 07 08 00 18 26 23 24 12 00 12 13
 24 13 02 00 03 20 17 03 20 29 06 08 08 24 16 02 00 26
 16 07 00 12 23 28 02 07 20 17 20 09 08 16 19 21 11 00
 01 11 03 23 14 04 17 26 23 20 24 09 04 26 10 30 03 25
 19 08 20 28 04 07 12 18 20 14 27 01 07 20 13 20 18 23
 26 22 17 02 17 12 11 24 11 27 29 28 23 02 28 13 30 10
 03 07 03 07 26 18 24 14 21 01 30 08 26 05 15 20 15 06
 28 08 20 20 23 20 11 21 17 09 18 23 21 15 26 28 22 12
 26 00 29 17 20 14 27 01 09 18 22 03 27 04 16 05 06 14
 30 18 06 20 24 27 29 30 18 22 03 22 19 29 27 13 29 13
 18 26 08 09 09 01 28 08 23 03 22 08 16 10 08 09 23 08
 01 23 08 08 04 07 23 26 21 27 19 16 28 15 08 04 14 22
 19 24 24 16 26 20 02 05 15 04 29 10 15 09 18 23 25 11
 29 12 16 19 10 13 28 15 26 16 27 08 08 18 12 23 30 24
 04 00 02 21 30 20 13 20 28 05 13 09 04 23 23 29 01 26
 26 12 00 11 03 18 30 15 22 06 29 23 14 25 30 01 02 30
 18 13 26 00 25 23 10 06 12 14 13 08 22 11 24 26 30 20

Pool of shares:

13 27 14 11 15 27 26 28 01 05 26 18 03 10 02
 05 01 04 10 06 17 01 14 28 16 19 06 15 03 29
 11 18 25 12 29 02 03 03 15 02 07 28 11 22 16
 07 26 29 25 11 12 28 20 22 04 21 24 05 15 30
 19 19 08 02 19 07 02 10 10 29 15 16 24 06 18
 20 16 15 18 04 14 10 26 06 19 24 27 23 29 06
 03 25 21 21 01 05 04 24 19 21 04 14 16 23 03
 27 14 30 05 25 18 15 12 16 27 16 08 08 16 10
 02 30 22 09 05 10 13 23 26 17 03 30 25 02 13
 25 02 02 30 30 30 12 15 03 08 14 05 20 26 20
 10 15 26 08 09 29 20 07 02 07 27 22 17 08 26
 16 11 12 14 03 16 16 30 25 15 30 11 10 07 04
 21 13 19 16 24 24 14 19 08 13 11 01 29 19 09
 08 17 18 19 20 20 11 25 12 20 01 13 28 20 14
 22 03 01 06 10 19 08 04 27 18 17 23 30 18 01
 15 07 11 29 22 08 05 27 04 01 05 19 19 21 27
 28 12 23 26 16 11 23 29 09 30 12 21 02 25 22
 26 10 09 17 28 22 07 17 11 23 23 02 14 01 25
 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18

Info about last item:

Bin:01110111010011010101110110110100101001001110000010110000010001110010011100010010010100 (90 bits)

Hex:0x0E1D06151B161A0A09180510081C13110414 (18 elements)

Vec:[14;29;06;21;27;22;26;10;09;24;05;16;08;28;19;17;04;20] (18 elements)

Already in pool.

(linearly dependent with respect to share Pool[14])

Info about last item

ONS lookup

10-18 sim.

02-03 sim.

+1

Clear

Reset

Contributions of our Proposal

- **Compact:** shares fit into the memory of EPC tags (90 to 270 bits)
- **Proactive:** tags can renew their shares without changing the initial secret
- **Robust:** our scheme guarantees strong security
- **Anonymous:** process does not require tag identities

[Garcia-Alfaro, Barbeau, Kranakis, 2009] *A Proactive Threshold Secret Sharing Scheme Handling Gen2 Privacy Threats*, March 2009.

Conclusions

- Evolution of optical barcodes
- May lead to privacy violations
- Threats to wireless channel between readers and tags
- Countermeasures to increase technical difficulties