IPv6

Opportunity for deployment of **privacy-enabled** mobile networks rel5.2

IPv6 Task Force Meeting,
14th January 2004, Brussels

Dr. Alberto Escudero-Pascual

Ass. Prof. Royal Institute of Technology (KTH)

S-16440 Sweden

it-universitetet KISTA

aep@kth.se ID: 721205-8376

IPv6: 3ffe:200:15:2:0:60:1dff:fef1:64d4

- Researcher at the Royal Institute of Technology (KTH) in the area of **security** and **privacy** in **mobile** Internet.

- Combining both **technical** and **legal** requirements from privacy.

IPv6: More f-or privacy

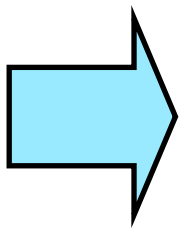
More addresses

More self-configuration

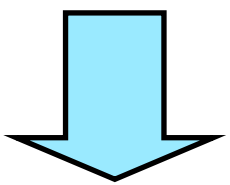
More mobility

More security

More QoS



More f-or privacy



More **tools** by default

Three schools of 'privacy'

US school (Alan Westin)

Ability to regulate information about ourselves

EU school

Expression of the individual's personhood. Capability to define his/her essence as a human being (thoughts, actions and decisions)

Eclectic school (Ken Gormley)

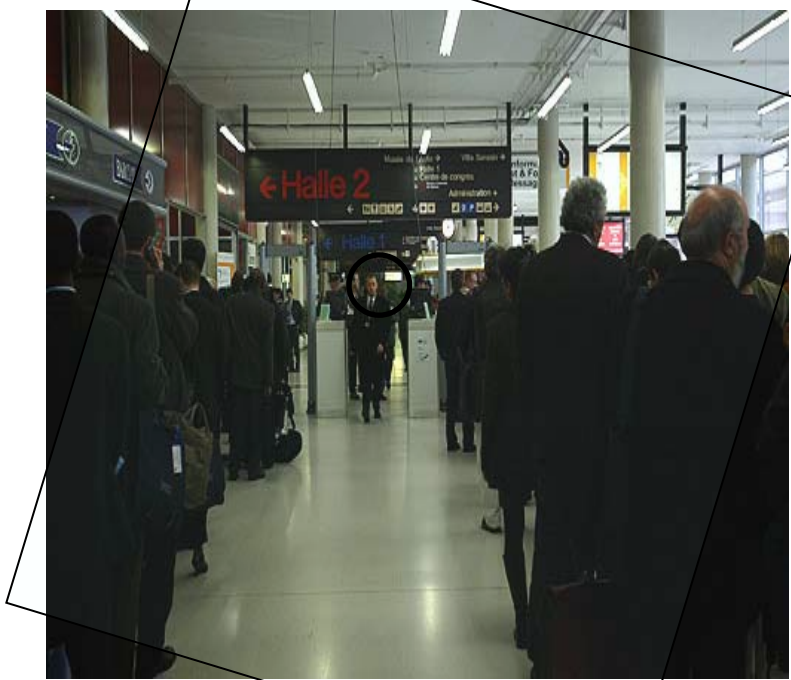
Distils privacy into three essential components.

Privacy Rights

1. The right to be **left alone**
2. The right to decide: when, how, and to what **extent information** about them is communicated to others.
3. The right to **secrecy, anonymity and solitude**.

Privacy in mobile Internet (1)

The capability of a **mobile node** to **conceal** the relation between **location** and **personal identifiable information** from third parties while the user is on the **move**.



Privacy in mobile Internet (2)

<I> am **<here>** to do **<this>, <now>**!

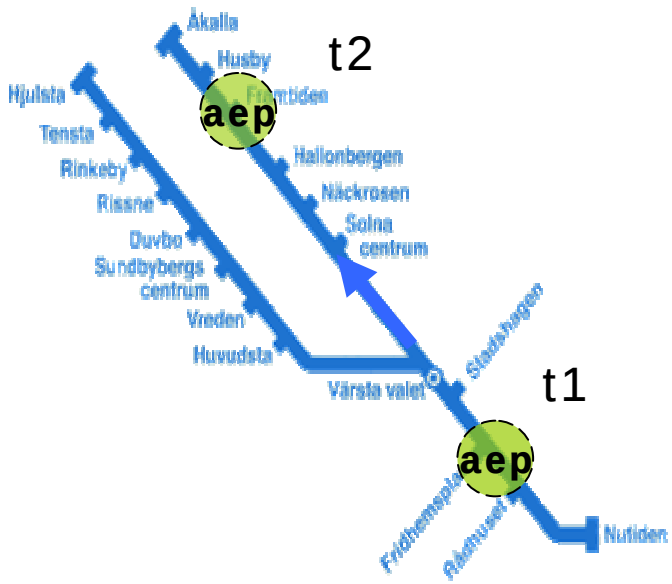
<identity $id_1, id_2, \ldots, id_n$>

<location $l_1, l_2, l_3 \ldots$>

<action $a_1, a_{11}, a_2, a_3, a_{31} \ldots$>

<time $t_1, t_2, t_3 \ldots$>

Privacy in mobile Internet (3)



1

Alberto is

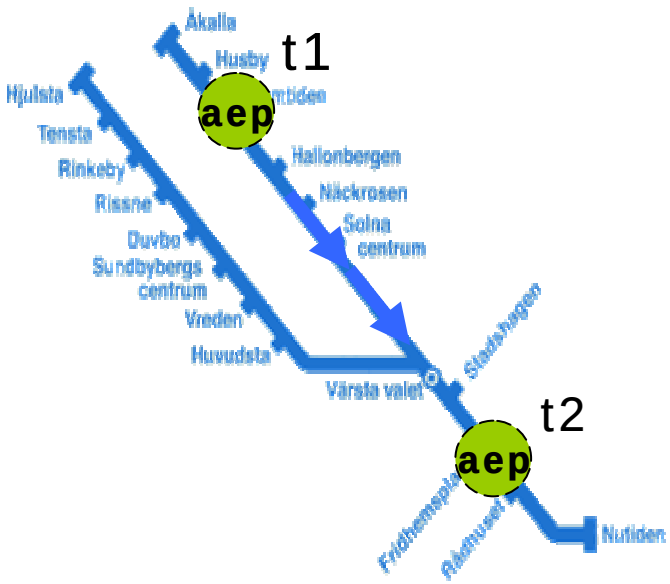
in the **<Metro>** 2

booking 3

two tickets to Venice! 4

5

‘Cryptacy’ in mobile Internet (4)



1 Crypt

Alberto is

2 Crypt

in the **<Metro>**

booking

3 Crypt

two tickets to

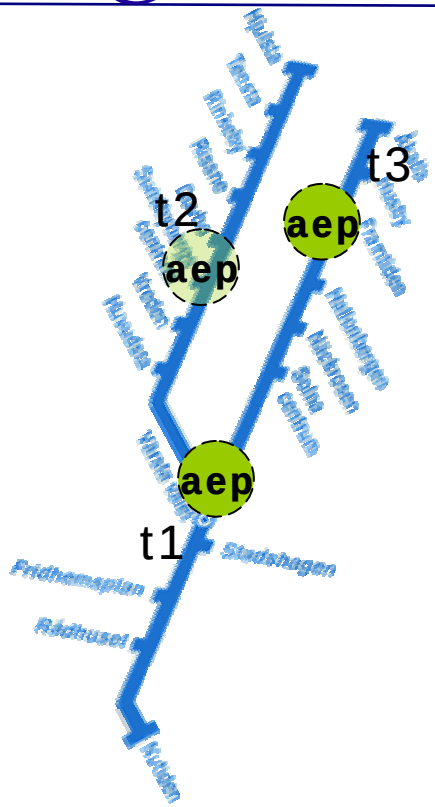
Venice!

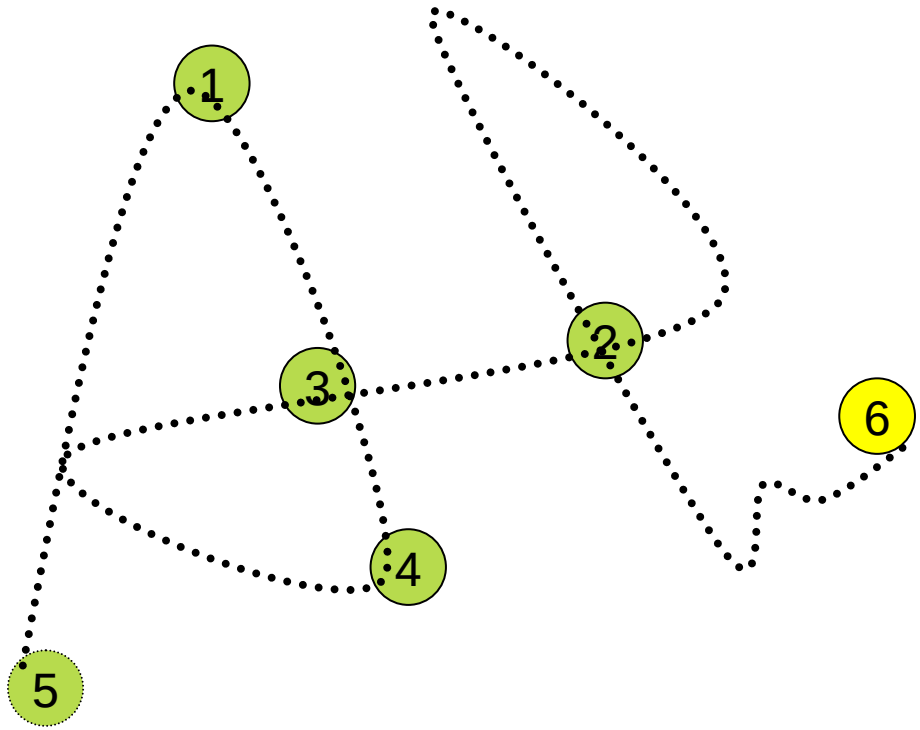
4 Crypt

5 Crypt

6 **For 14th February 2004**

‘Digital signature’ in mobile Internet (5)

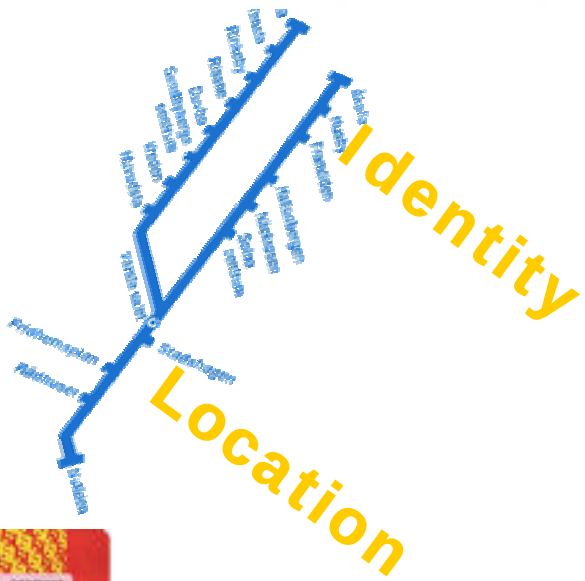


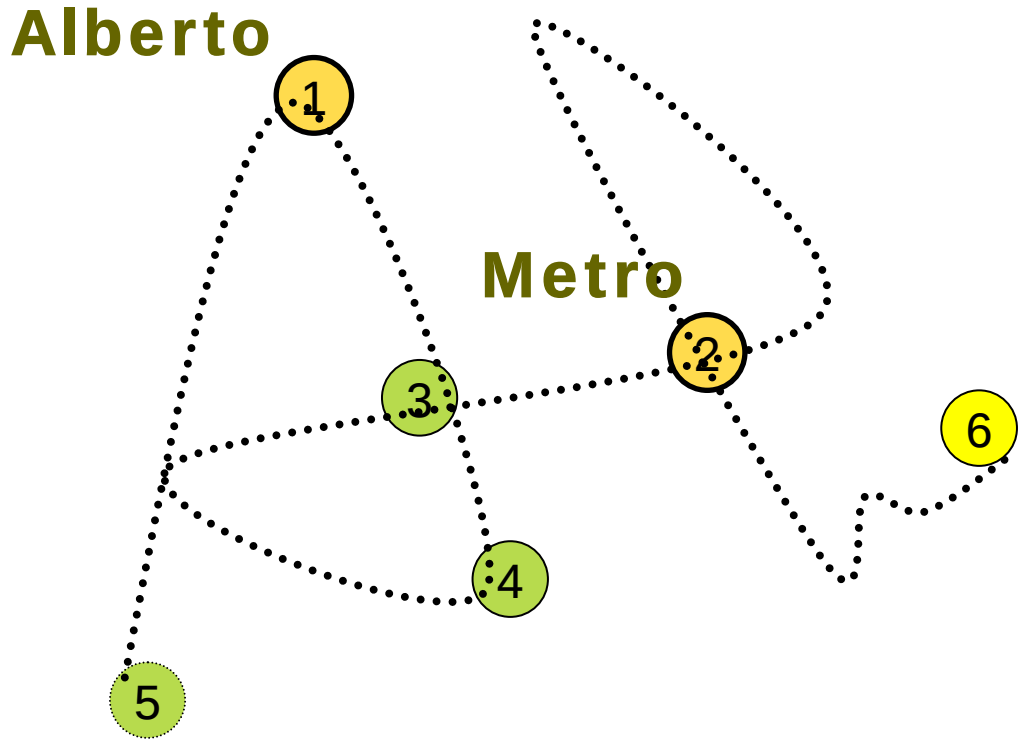


<identity id1,id2,…,idn>
<location l1,l2,l3…>
<action a1,a11,a2,a3,a31…>
<time t1,t2,t3…>

it-universitetet
KISTA

Privacy and Internet addressing

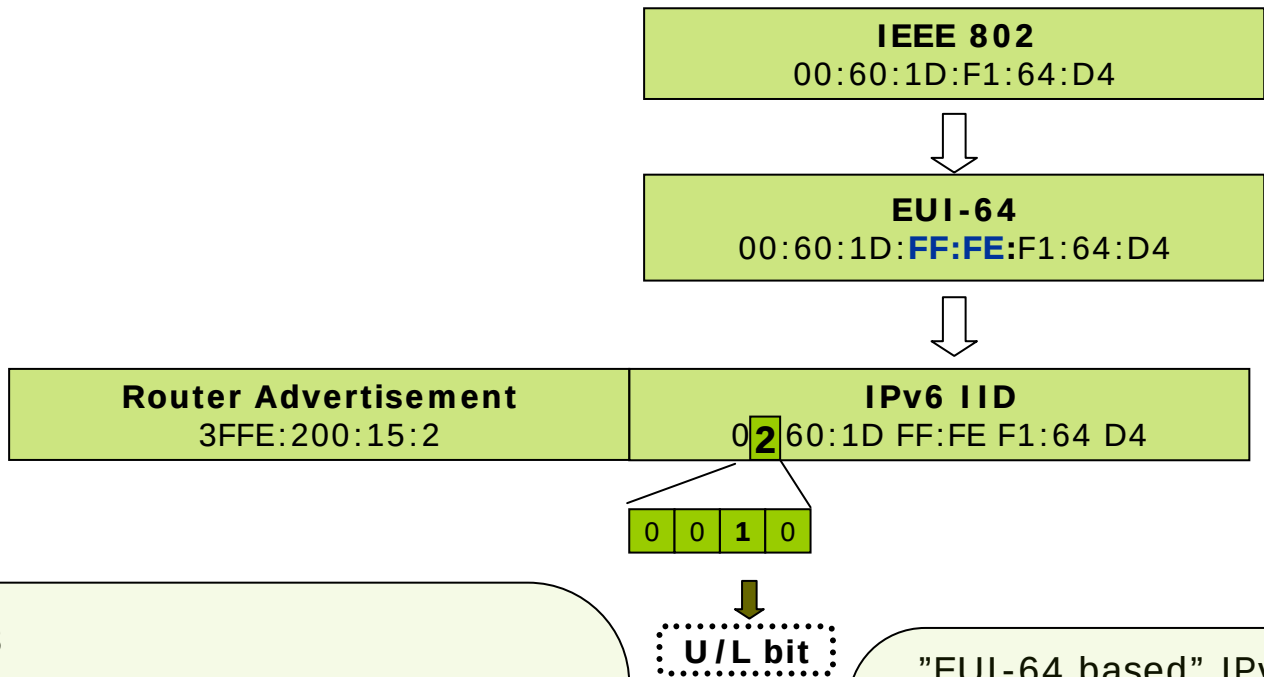




1

Identity & IPv6 Addressing

Identity and IPv6 Addressing (1)



RFC2373

- IPv6 addressing architecture

RFC2374

- IPv6 aggregatable global unicast address

RFC2462

- IPv6 address autoconfiguration

"EUI-64 based" IPv6 Interface Idenifier(IID) is a **unique identifer.**

64 right bits **remain contant**
U/L bit: CLAIM of uniqueness

Identity and IPv6 Addressing (2)

The problem

It is possible to track a **UNIQUE device** and the its related **<actions>**.

UNIQUE user =
= UNIQUE device =
= CONTENT (t)

Suggested solutions

1. Privacy extension for stateless address autoconfiguration **RFC3041** [Narten, Draves]

2. Use of **CGAs, SUCV, ABK** [Montenegro, Castelluccia, Kempf, O'Shea, Roe]

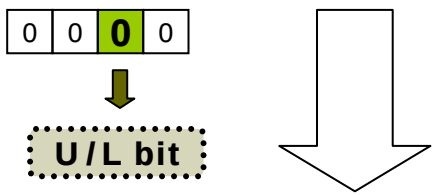
Opportunity!!

Escudero A. "Location Privacy in IPv6, tracking the binding updates", Tutorial at IDMS2001, Lancaster. UK, September 2001.

Analysis of RFC3041

RFC3041 ”privacy extension for address autoconfiguration”
Suggests:

1. to generate the IID randomly
2. change the u/l bit *u=0* to indicate not globaly unique



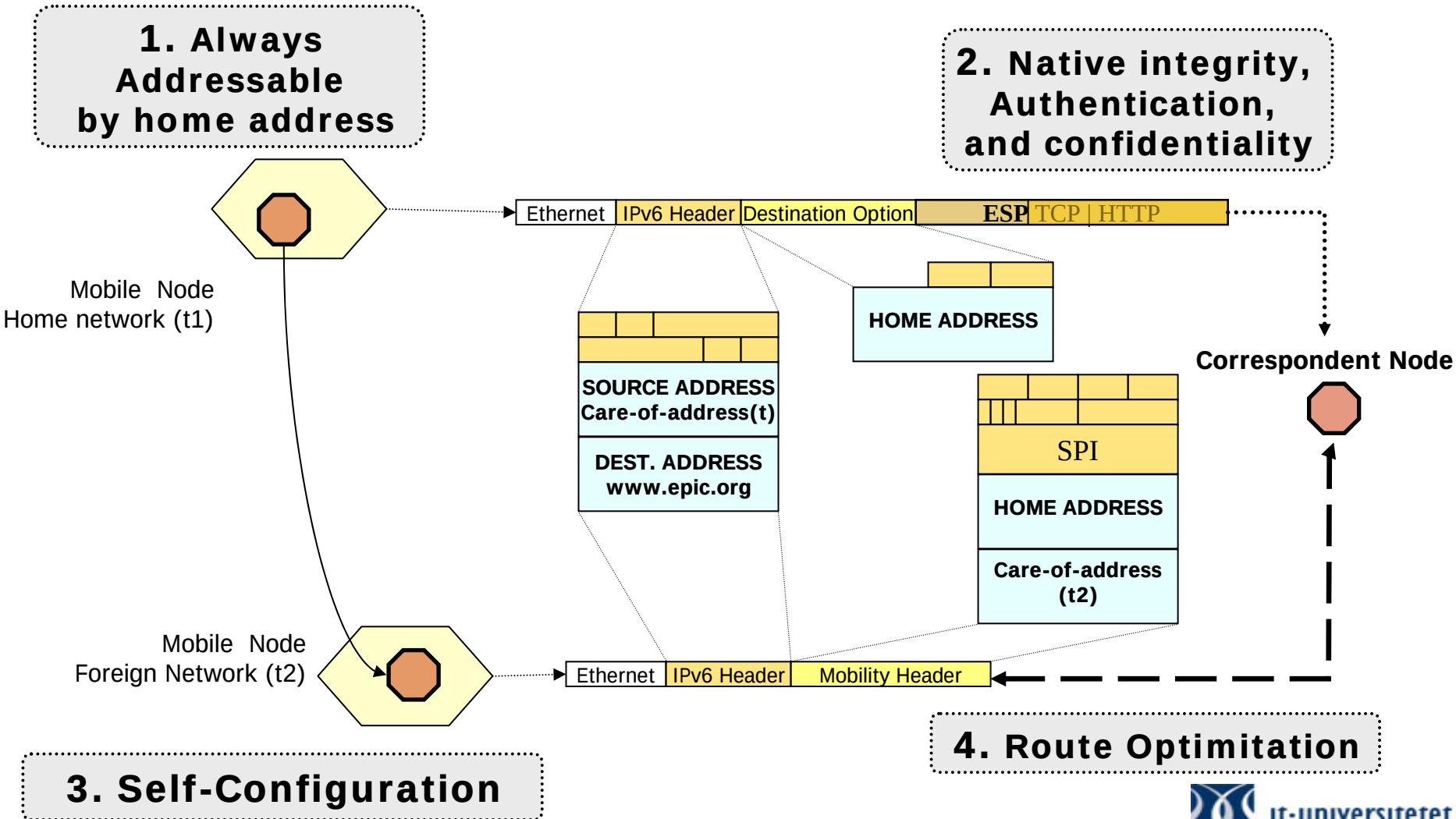
While the *u bit* indicates that the IID is not globaly unique, reveals under certain scenerios that an user wants to protect his/her privacy

Escudero A. ”Requirements for unobservability of privacy extension in IPv6”, Radio Vetenskap, Stockholm, Sweden. June 2002.

2

Location & Mobile IPv6 Addressing

Location and MobileIPv6 addressing (1)



Location and MobileIPv6 addressing (2)

The problem

It is possible to track the ***seamless mobility*** of **UNIQUE device** and the its related **<actions>**.

UNIQUE user =
= UNIQUE moving device =
= CONTENT (t)

Suggested solutions

1. **(IPv4, IPv6) No changes to IP routing**
   1. OnionRouting (US Navy),
   2. Freedom Network (ZKS),
   3. F-Freedom extensions (KTH)

2. **(IPv6) Changes to IP routing (inside of the AS)**
   1. …
   2. CPP forwarding (DoCoMo USA Labs)

Opportunity!!

Escudero A. ”Location Privacy in IPv6, tracking the binding updates”, Tutorial at IDMS2001, Lancaster. UK, September 2001.

P1

Location Privacy in IP

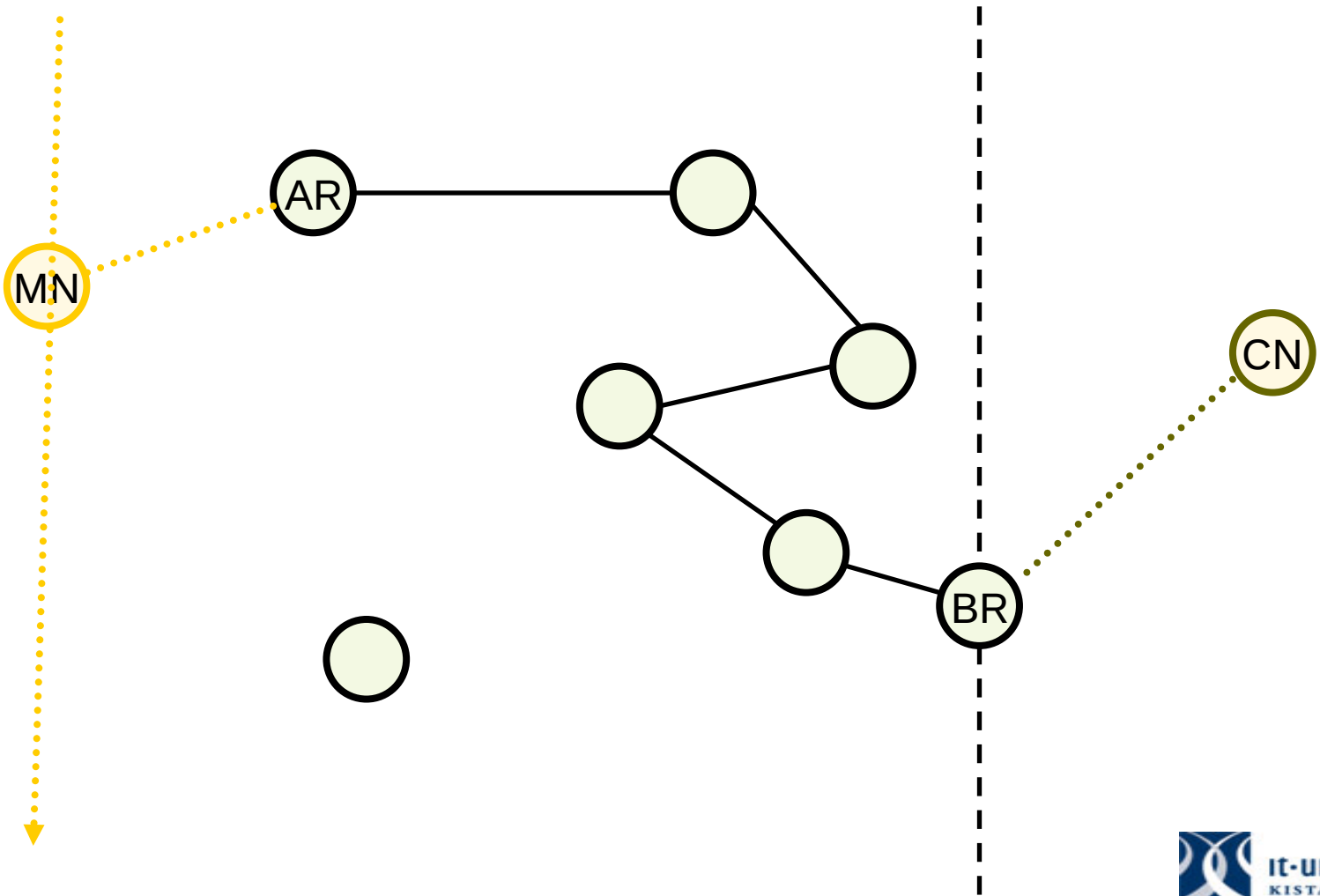
Previous work

Untraceable Mobility Support in the ZKS Freedom PIP network.

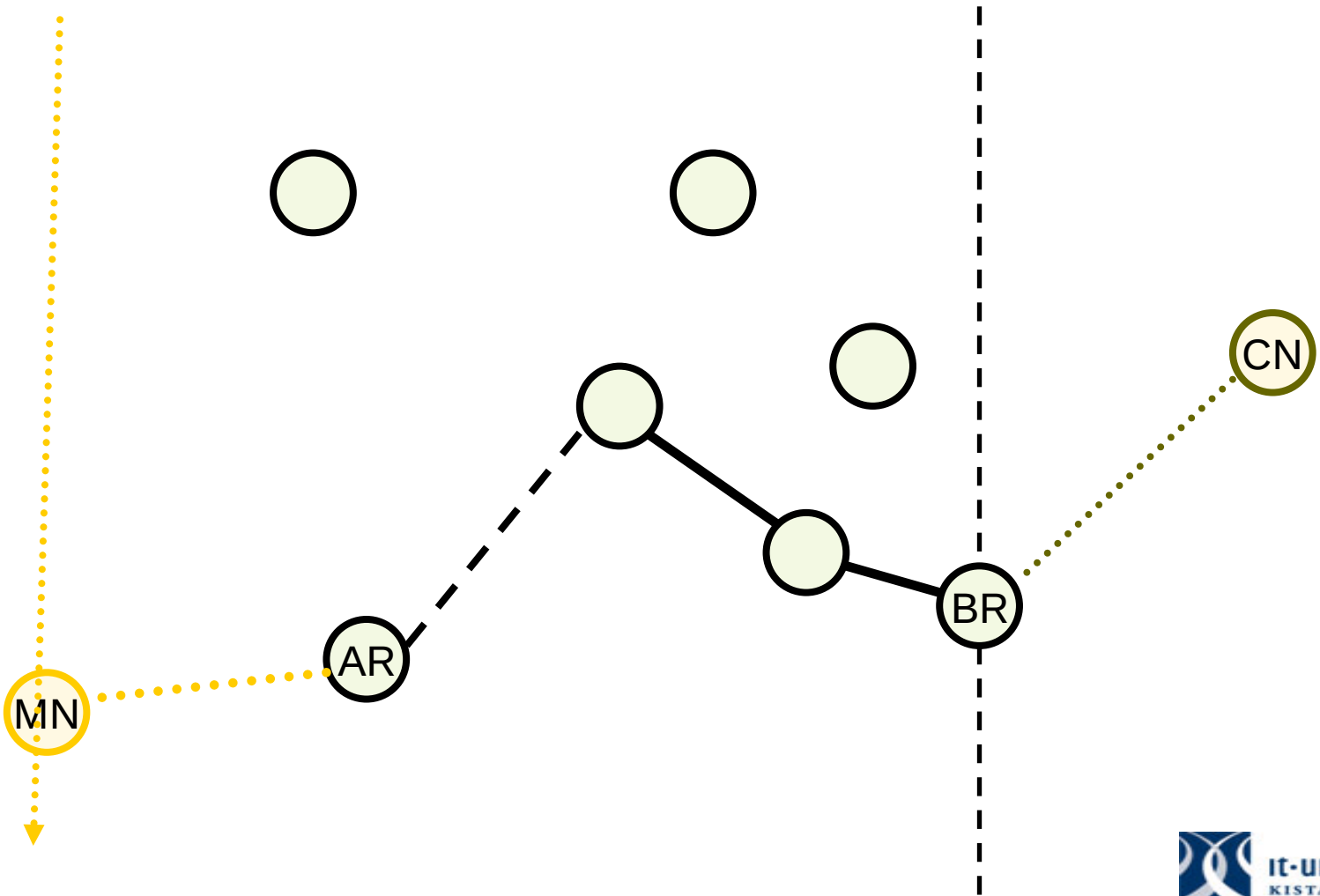
1. Proposal to extend the Zero Knowledge Systems' Freedom network to support mobility.
2. F-Fredom a Pseudonymous IP network
   - Mixes (Chaum)
   - Hierarchical MobileIP (Castellucia et al.)

P1 **Escudero A., Hedenfalk M. and, Heselius P.** "Location privacy in mobile internetworking. Protocol Extensions to the Freedom Netowork", INET2001, Stockholm. June 2001.

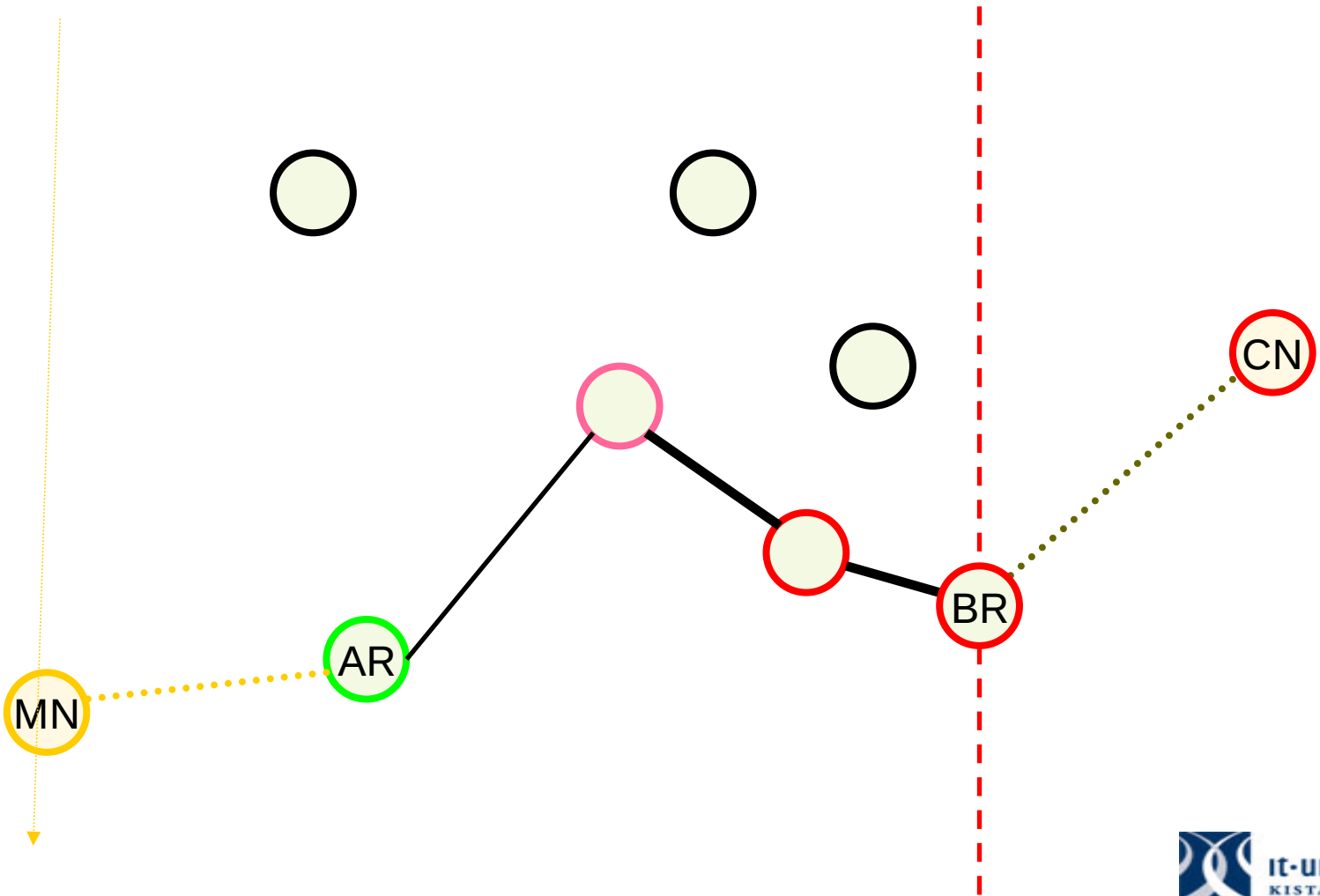
Core Concept: OR, MAP, AIP, …



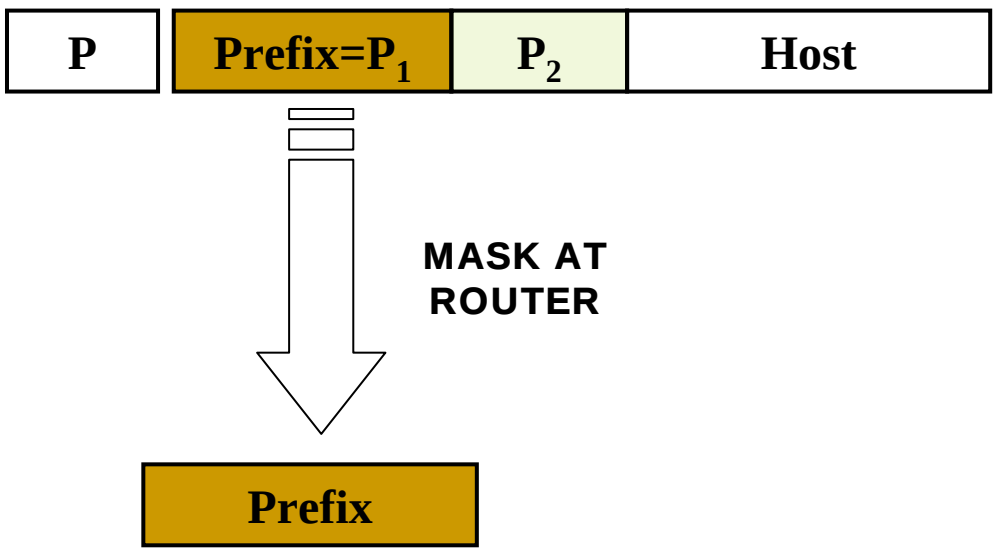
Core Concept: OR, MAP, AIP, …

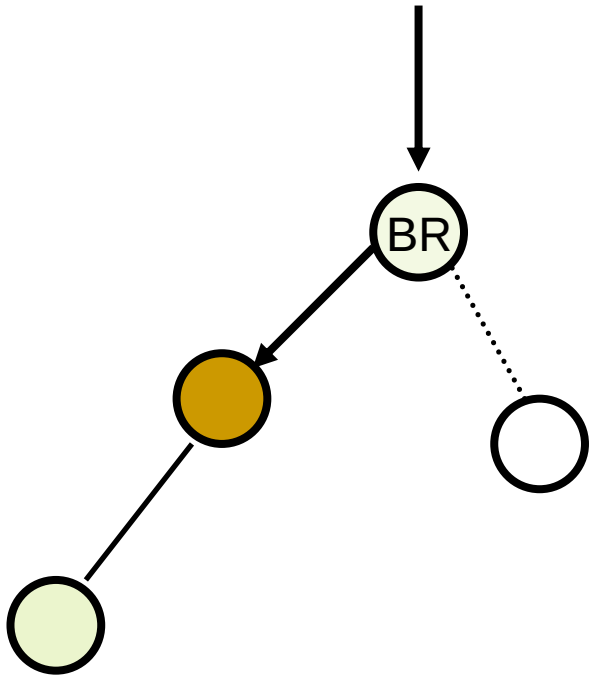


Core Concept: OR, MAP, AIP, …

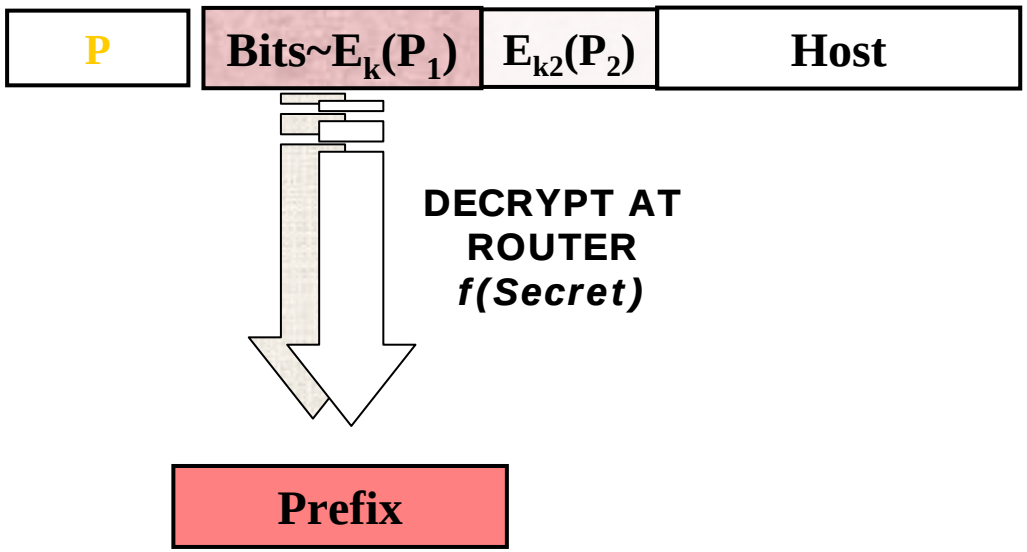


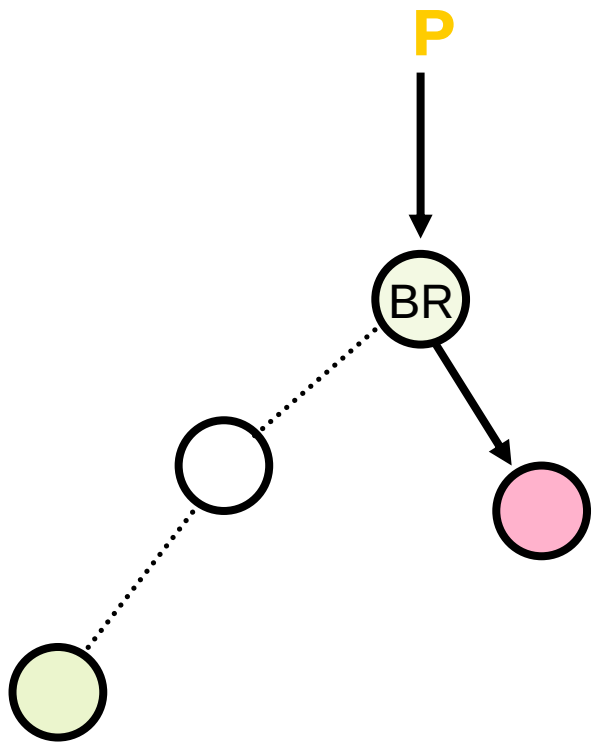
IPv6: Cryptographically Protected Routing Prefixes





IPv6: Cryptographically Protected Routing Prefixes





Conclusion

1. More tools, More possibilities

2. More opportunities for privacy

3. More work needs to be done in the area of Internet addressing and Identity and Location Privacy

IPv6 is ready for more privacy, are we?

it-universitetet KISTA