International Telecommunication Union

MAGNET identity management proposal for Personal Networks

Dimitris M. Kyriazanos

PhD Student – NTUA

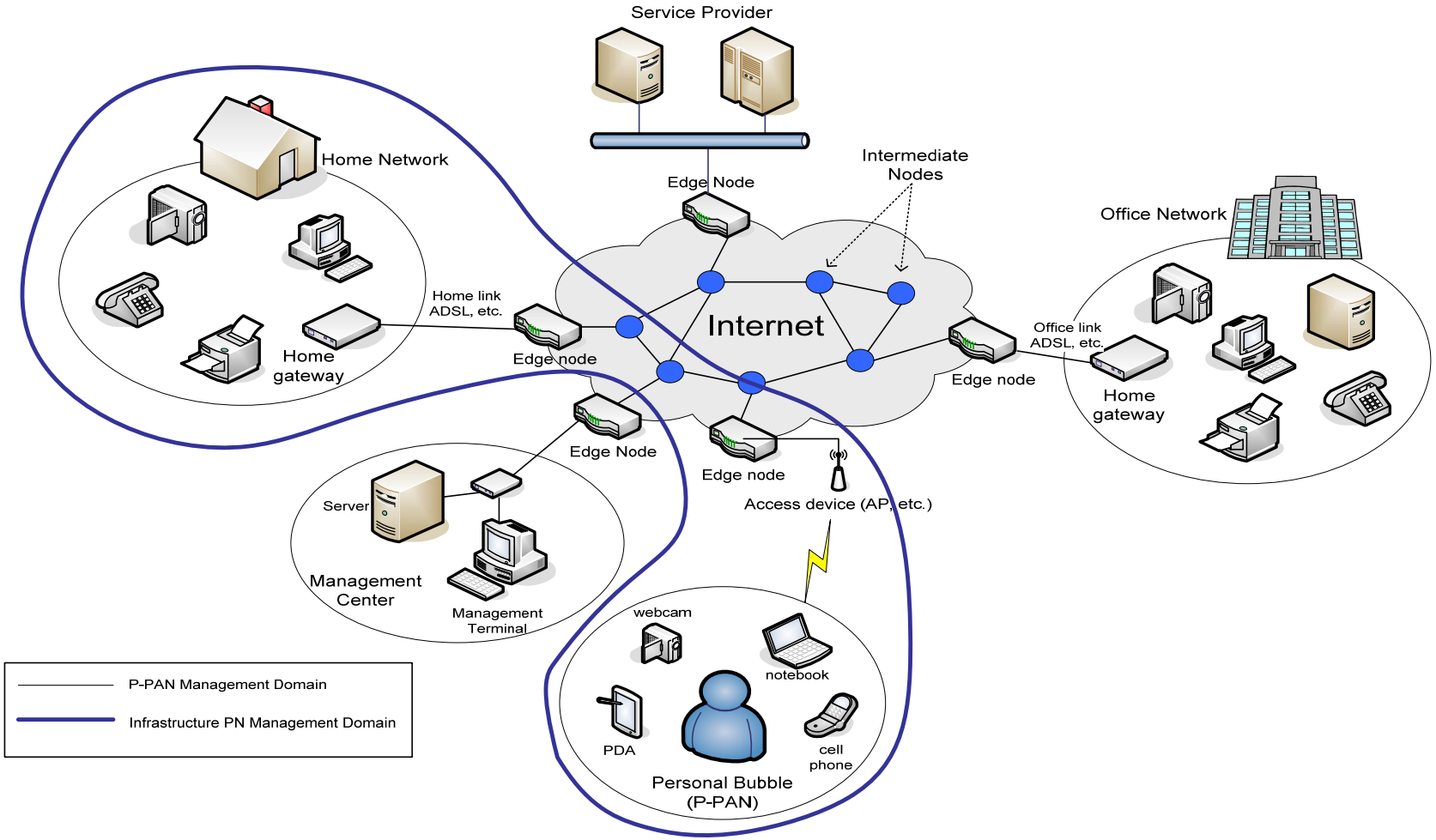
ITU-T Workshop on "Digital Identity for NGN"
Geneva, 5 December 2006

ITU-T

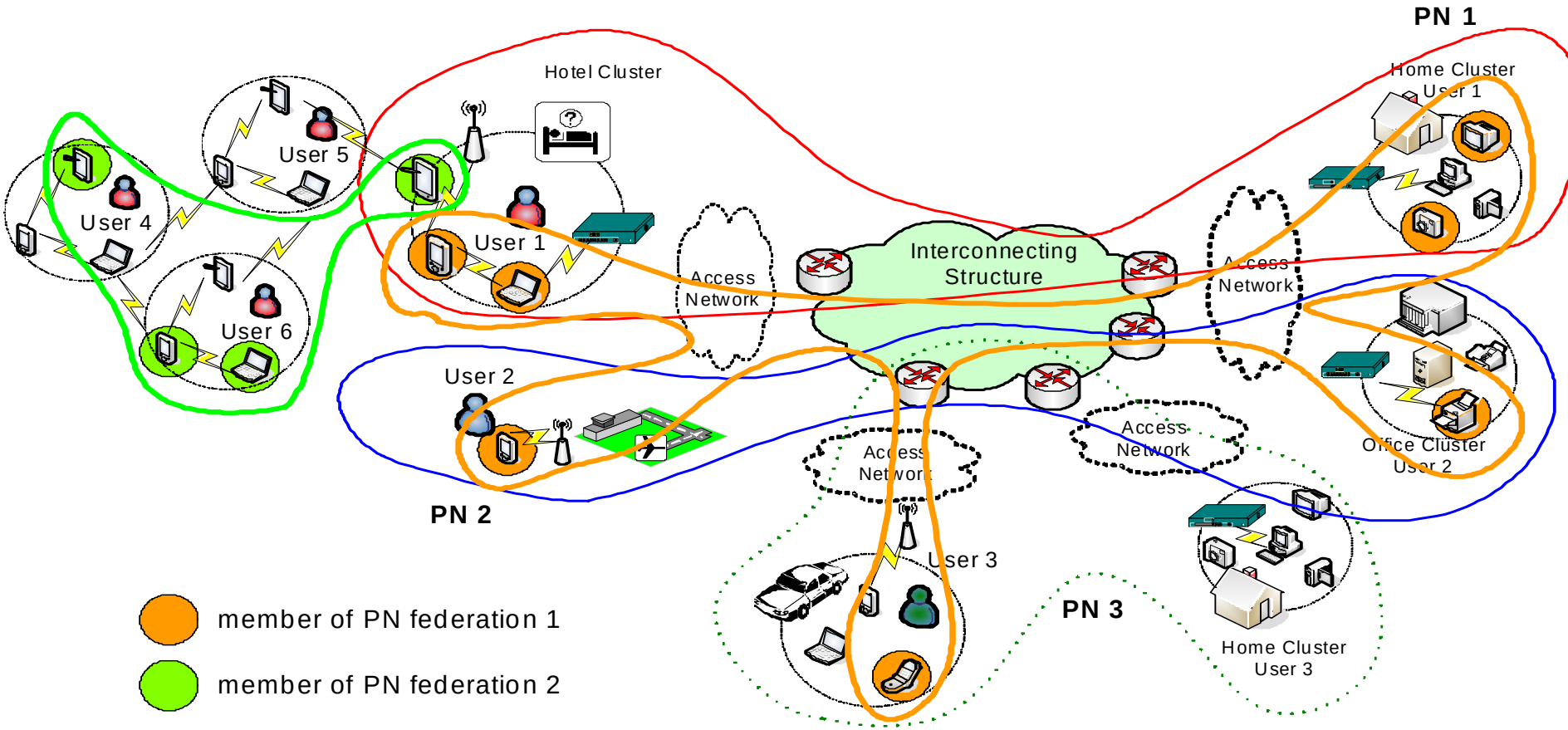
Personal Network - A Definition

- A Personal Network (PN) is the set of all networking-capable devices that someone uses for personal purposes including telecommunications, financial transactions, information, entertainment
- A PN may be geographically distributed (e.g. home cluster, car cluster, office cluster) – the clusters are interconnecting through VPNs forming an overlay network
- Despite its very dynamic nature, the security requirements of a PN are very strict, because the resources it interconnects contain a significant amount of personal information (like contact lists, bank accounts, passwords or various preferences)

From a PN…


Service Provider
Edge Node
Intermediate Nodes
Home Network
Home link ADSL, etc.
Home gateway
Edge node
Internet
Office Network
Office link ADSL, etc.
Edge node
Home gateway
Edge Node
Edge node
Access device (AP, etc.)
Server
Management Center
Management Terminal
webcam
notebook
PDA
cell phone
Personal Bubble (P-PAN)
P-PAN Management Domain
Infrastructure PN Management Domain

...to a PN Federation



ITU-T

Some definitions

- *Identifier*. An identifier distinguishes a distinct entity within the context of a specific namespace.
- *Attribute*. An attribute is a characteristic associated with an entity, such as an individual.
- *Identity/ Profile*. In an identity management system, identity is that set of permanent or long-lived temporal attributes associated with an entity.
- *Identity management*. Identity management is the process that ensures secure creation, storage, exchange and update of digital identity.

ITU-T

Identity management: what for?

1. A support to security schemes.
2. A support for mobility and pervasiveness
3. Protection of users' privacy
4. More usable and ergonomically-designed IT systems

ITU-T

Identity management: what for?

1. A support to security schemes.
2. A support for mobility and pervasiveness
3. Protection of users' privacy
4. More usable and ergonomically-designed IT systems

ITU-T

How to support security?

- An entity in the cyberspace owns many identifiers: IP addresses, MAC addresses, URLs, email address, UUID …
- → Opens door to identity usurpation, forgery

- An entity has to manage credentials/keys for each communication layer, application or radio technology.
- → need for a unique, primary address that vouches for all the others and bound to security credentials

ITU-T

How to support mobility?

- In most cases (layer 3 and above) mobility = an address change
- → primary address remains unchanged, while other addresses act as locators (a HIP-like approach). No need for re-authentication.

- -Same reasoning applies also for vertical handover (Wi-Fi to BT for instance)

ITU-T

Step 1: make it secure

- Idea: link an identifier to cryptographic material

1. key = *f* (identifier)
- → identity-based cryptography

2. Identifier = *f* (key)
- → cryptographically-generated addresses
- What we chose in MAGNET: Identifier= hash (public key)

ITU-T

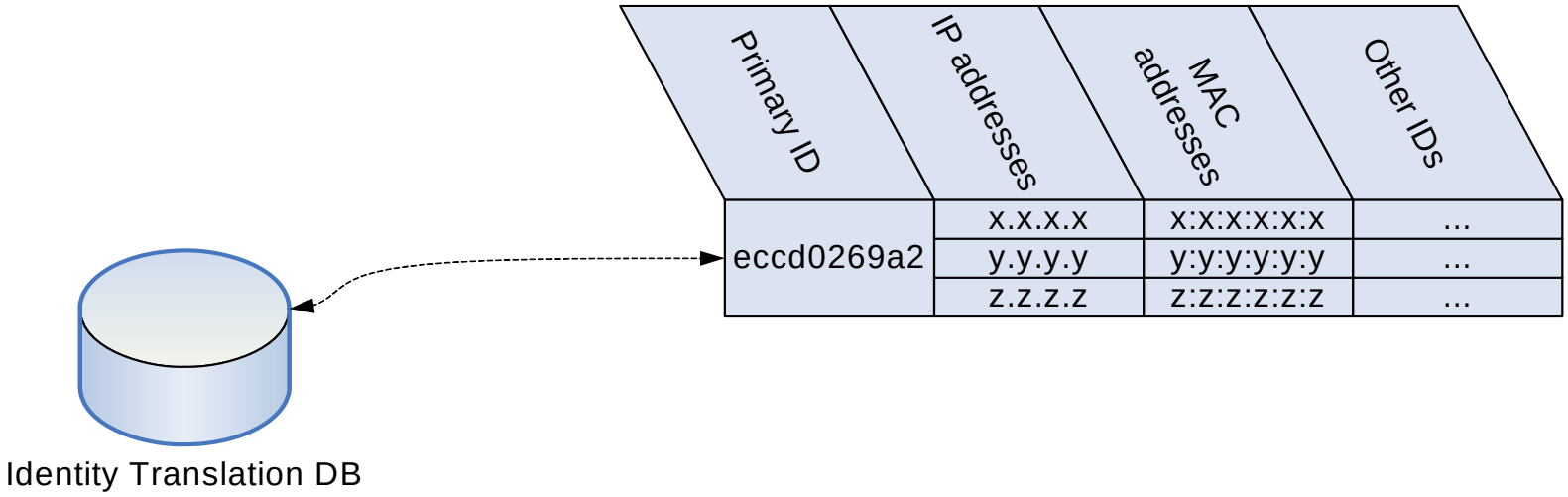
Step 2: design a namespace

- We associate a unique ID to PN federations and PNs computed as *CBIDgroup=hash(PKgroup)* derived by the group generator. We also propose the following structure for MAGNET namespace:
- $CBID_{PN\text{-}F}||CBID_{PN}||CBID_{Entity}||$validity/access control
- The name is certified or used with identity-based cryptography, which brings group membership proof and address ownership proof.

ITU-T

Step 3: link to other addresses

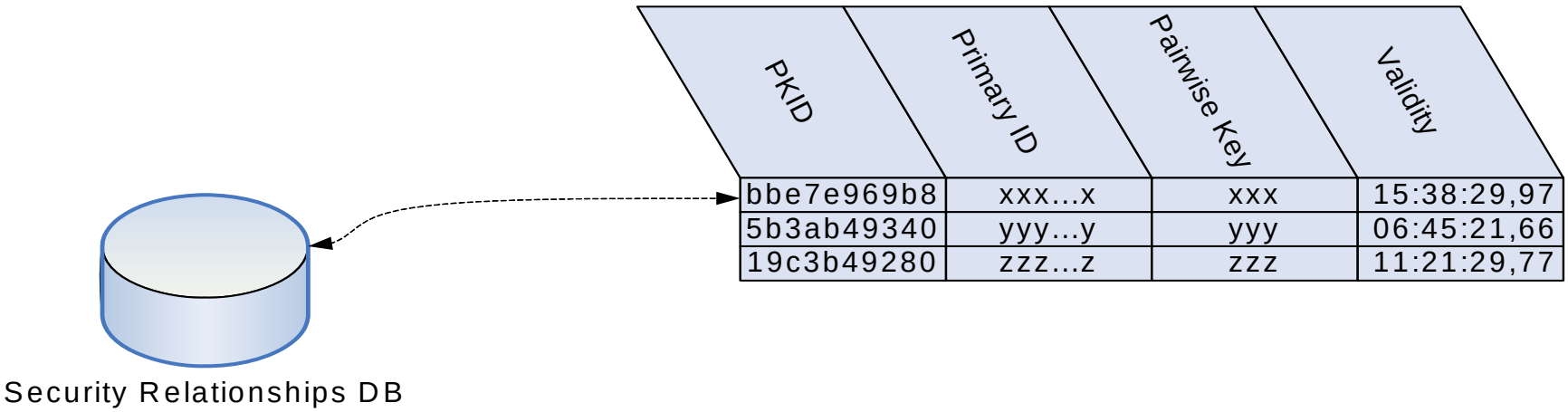
- Identity Translation database (ITD)is used to map the unique MAGNET ID into the usual ones.



ITU-T

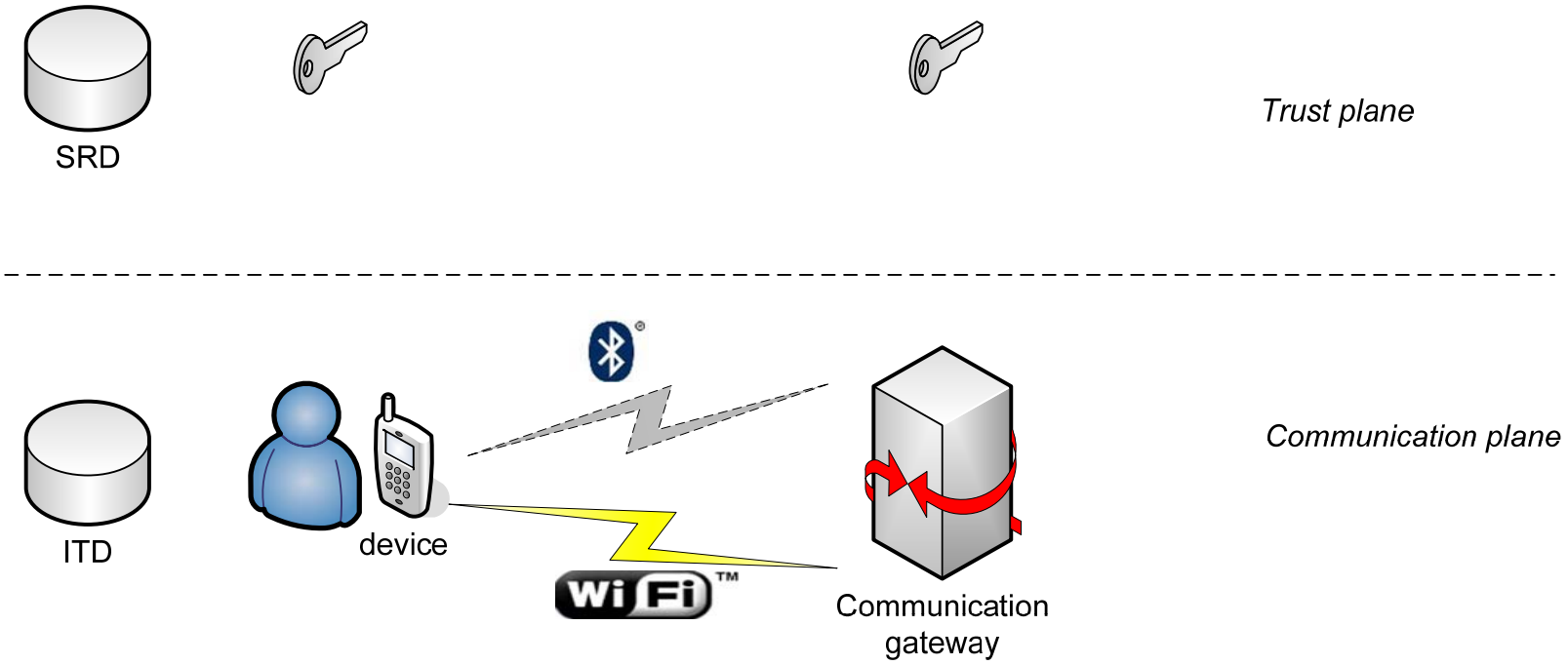
Step 4: link to security associations

- The Security Relationships Database (SRD) is used to store the pairwise keys, referenced by the unique ID of the corresponding devices.



ITU-T

o A practical use case: fast vertical HO



ITU-T

Identity Management I: Security Profiles

- The Profiles provide structured information about all PN elements and conceptual entities
- User information: the identity, organization, role, group membership, areas of interest and preferences of the user.
- The pair-wise long term keys
- Group information
- Service information
- Trust level
- Reputation
- Policies:
- PN-Federation credentials, timestamps and related information.
- User Role associations

ITU-T

Identity Management II: Profile Management

- Profiles will definitely not remain static.
  - Mobility of users & Portability of devices.
  - Time-limited memberships and rights.
  - Security crisis (e.g. theft or loss of device)
- Any changes on the profiles are supposed to be passed on to any related policy management and security applications throughout the PN overlay network dynamically, without requiring offline time and (re-)programming efforts.
- The administrator should be allowed to dynamically issue new policies and change existing ones, while being sure that these new policies are spread and stored securely to any involved devices throughout the PN .

ITU-T

Identity Management II: Profile Management

- Profile Management Modules and Profile Repositories:
  - **Distributed** into specific cluster administrative devices, promoting scalability for the PN.
  - In each "master" device a policy management module is present, enabling:
    - the master device to act as a "policy officer" for the devices in his jurisdiction.
    - user policy administration **over the entire PN**.
- Policy registration occurs either:
  - Transparently along with Service, Device or other Entity registration (interoperation with SD platform and device registration platform), performing Policy registration.
  - User-driven, offering policy management capabilities to the administrator (via XML-driven GUI)
- Secure operation:
  - Encryption of Security Profiles.
  - Integrity check upon decryption.

ITU-T

Last but most Important: Privacy!

- Four basic guidelines:
  - Notice: The individual should have clear notice of the type of information collected, its use, and an indication of third parties other than the original collector who will have access to the data.
  - Choice: The ability to choose not to have data collected.
  - Access: The ability for the data subject to see what personal information is held about him/her, to correct errors, and to delete the information if desired.
  - Security: Reasonable measure taken to secure (both technically and operational) the data from unauthorized access.

ITU-T

Thank you!

- For more information about MAGNET Beyond project please visit: www.ist-magnet.org
- Or contact:
- Dimitris Kyriazanos: dkyri@telecom.ntua.gr
- Khaled Masmoudi: Khaled.Masmoudi@int-evry.fr