ENABLING EFFICIENT AND OPERATIONAL MOBILITY IN LARGE HETEROGENEOUS IP NETWORKS

Enabling Efficient and Operational Mobility in Large Heterogeneous IP Networks

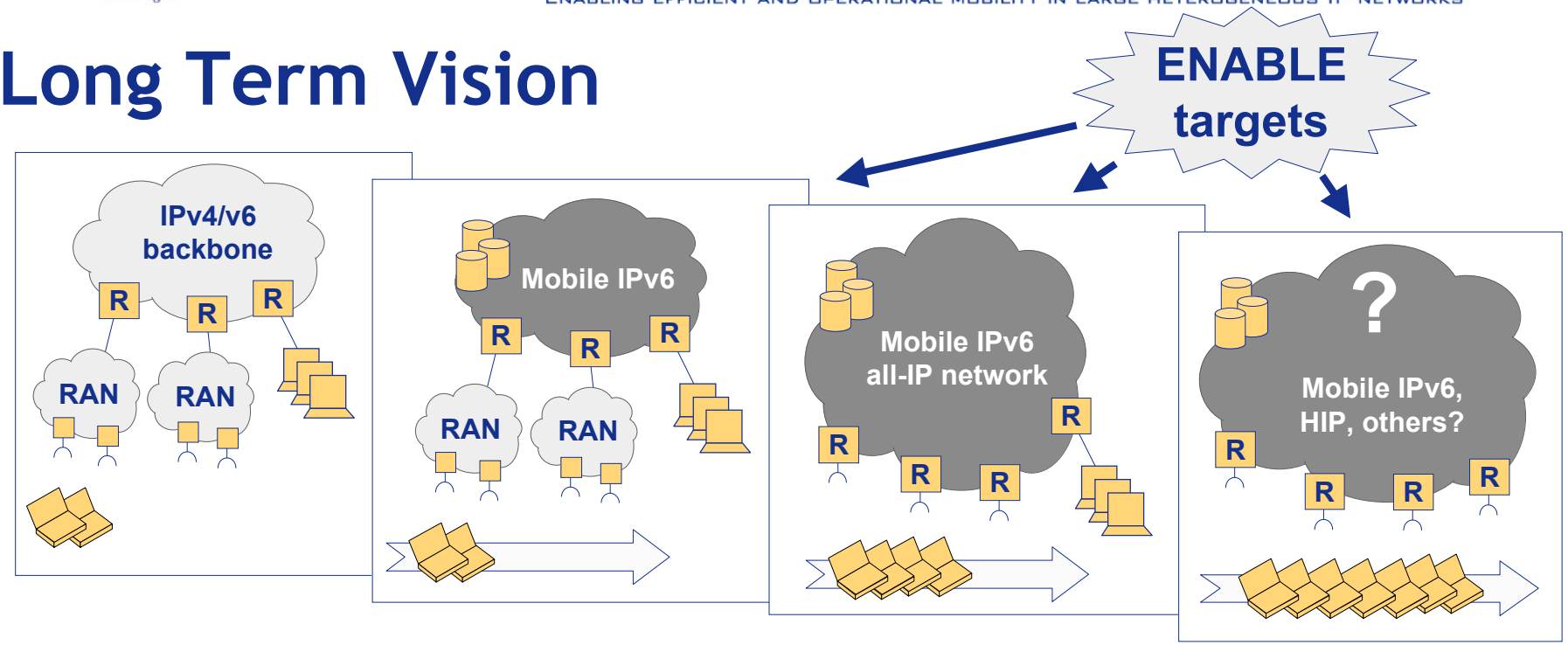
Jordi Palet, Consulintel
(jordi.palet@consulintel.es)

Information Society Technologies

Project Goal

- Enable deployment of efficient and operational mobility as a service in large scale IPv6 network environments, taking into account also the transition from IPv4
  - Research and contribution to standardization fora (IETF, 3GPP, etc.)
  - Validation through laboratory experiments (prototypes, testing, etc.)
- Main areas of work
  - Enhancement of Mobile IPv6 to enable **transparent mobility** in **large operational networks** with **multiple administrative domains**, **heterogeneous accesses** and a rapidly **growing number of users**
  - Enrichment of the basic mobility service provided by Mobile IPv6 with a set of **"premium" features** (fast handover, QoS, etc.)
  - Analysis of goals and design principles for the **evolution beyond Mobile IPv6 in the long term**

Long Term Vision



Today

Dedicated RANs optimized for specific services

- cellular (2.5-3G)
- Wireless LAN
- WMAN (WiMAX)

Step 1

Integration of heterogeneous RANs to offer efficient and cost-effective ubiquitous mobility

- MIPv6 is the key

Step 2

Smooth migration to an all-IP network architecture

- all services over IP
- MIPv6 with fast handover support

Step 3

Fully mobile Internet

- tremendous growth in the number of terminals
- MIPv6 might suffer its age

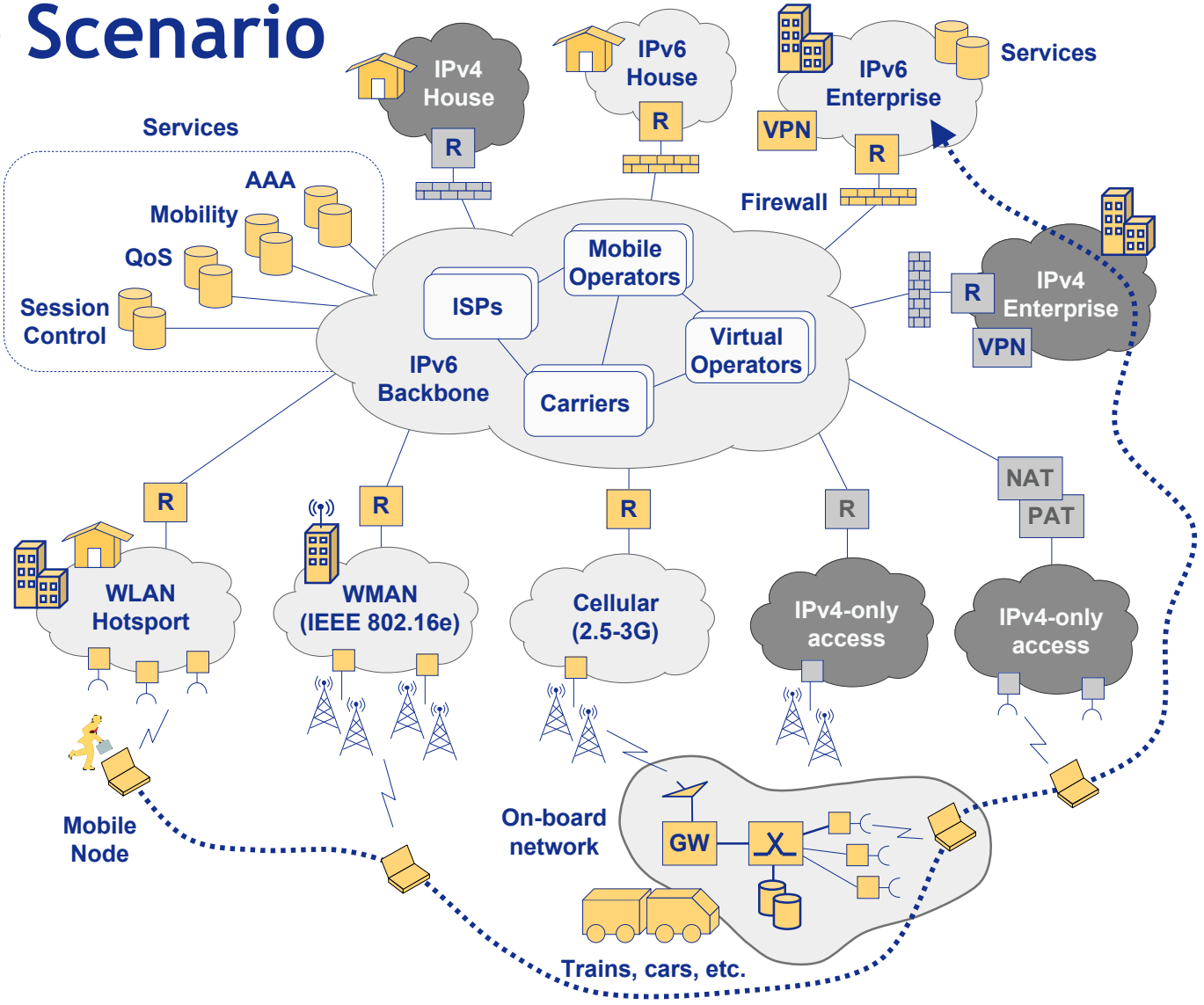
Key Research Objectives (I)

- Improvement of Mobile IPv6 scalability
  - **Dynamic provisioning** of configuration data on terminals and HAs
  - **Load-sharing** across HAs
- Improvement of reliability
  - Solutions for **HA failover** (no single point of failure)
- Control of mobility service
  - **Service authorization** based on a AAA infrastructure
- Enable offering of “premium” network features
  - **On-demand and secure activation** of fast handovers, QoS, etc.
- Integration of Mobile IPv6 in real-life environments
  - Coexistence with **middle-boxes** (firewalls, VPN concentrators, etc.)
  - Deployment of **Mobile IPv6 in IPv4-only accesses**

Key Research Objectives (II)

- Analysis of protocols and architectures for long-term network evolution
  - **Scalability** to an incredibly high number of terminals
  - Optimized support for **terminals with very limited processing and storage capabilities** (e.g. sensors)
  - Deploying **Mobile IPv6 may not be enough in this scenario** and therefore possible long-term alternatives/enhancements must be carefully evaluated
    - ❑ **Host Identity Protocol (HIP)**
    - ❑ **IKEv2 Mobility and Multihoming (MOBIKE)**
    - ❑ **NETwork based Localized Mobility Management (NETLMM)**
    - ❑ **Others**

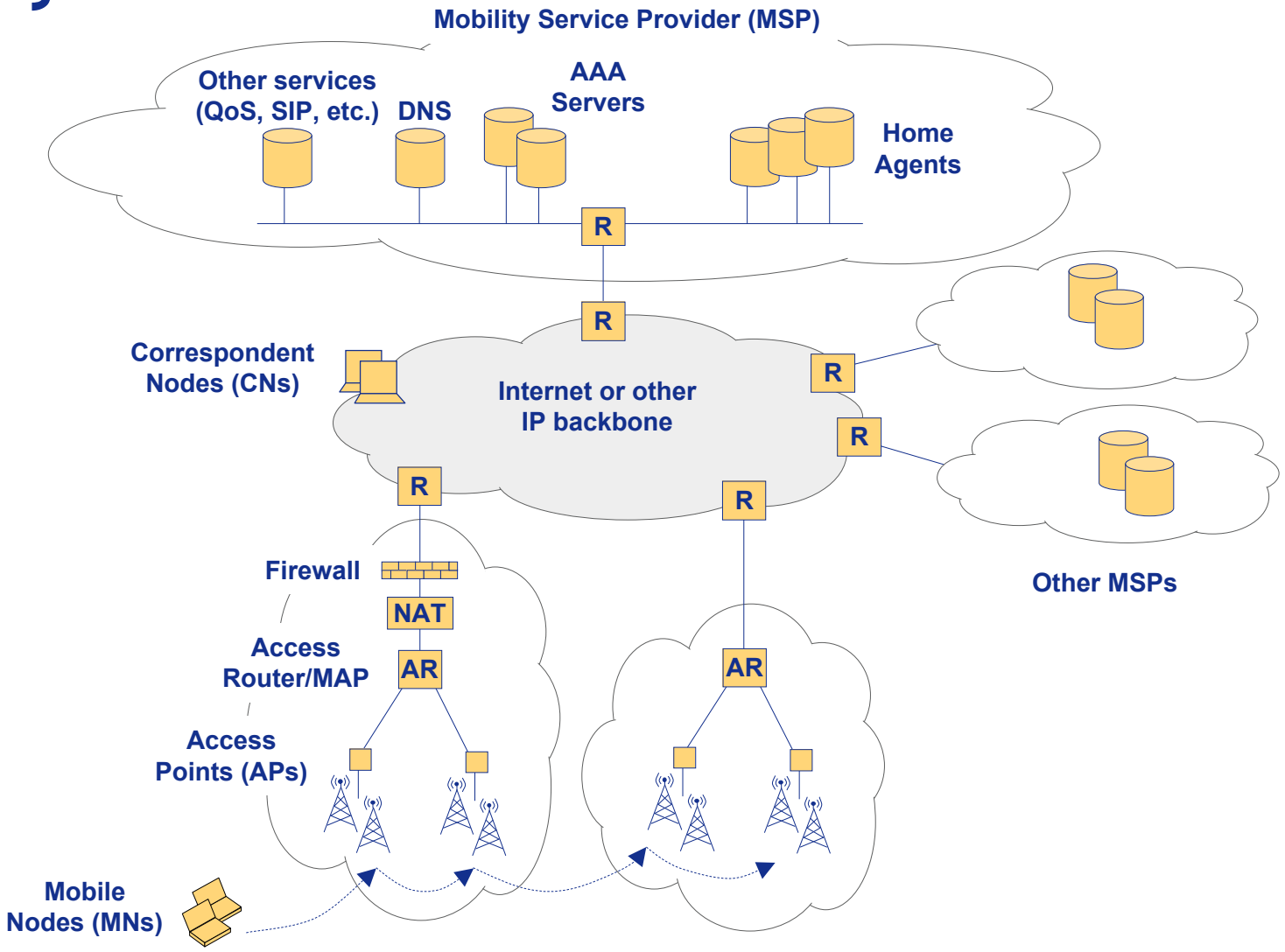
Reference Scenario



Expected Impact

- Mobile IPv6 as it is today is not suitable to implement the ENABLE Reference Scenario
- ENABLE will fill the gaps working in close relation with the IETF, to ensure that the solutions developed by the project are in line with the architectural principles devised by the Internet community and can get possibly standardized
- The research in ENABLE will increase the ability to deploy a future-proof mobility infrastructure for the usage of demanding, future applications like pervasive peer-to-peer, audio/video conferencing over IP, emergency services, etc.
- ENABLE will also contribute to the development of a long-term vision towards the future fully mobile Internet, investigating on possible transition paths towards novel, and not yet fully understood, technologies

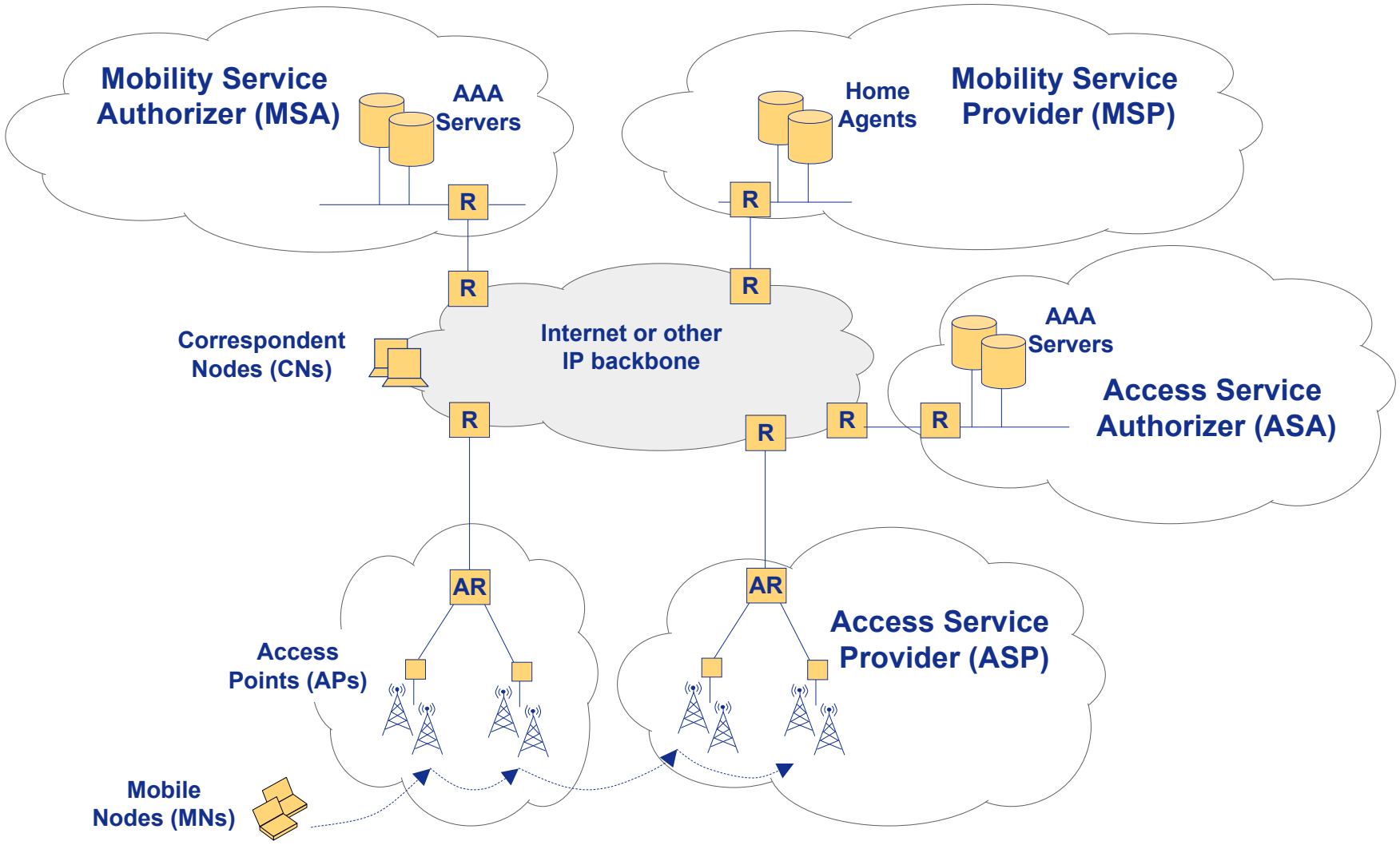
ENABLE System Architecture



Bootstrapping

- Goal
  - Addressing the operational requirement for dynamic provisioning of configuration data on terminals and HAs and MIPv6 service authorization
- Configuration data
  - HA address
    - Required on MN
    - Used for registering Binding Updates with HA
  - MN‘s Home Address
    - Required on MN
    - Used for communication with other nodes
    - Could change if home network will be renumbered
  - Keying Material
    - Required on MN and HA
    - Used to set up a security association (IPsec) between MN and HA

Service Entities Involved in Bootstrapping



Bootstrapping Architectures Investigated by IETF

- Split scenario
  - Mobility Service Authorizer (MSA) is different from Access Service Authorizer (ASA)
  - Assignment of Home Agent done using DNS
- Integrated scenario
  - Mobility Service Authorizer (MSA) is the same as Access Service Authorizer (ASA)
  - Assignment of Home Agent done using DHCPv6

Steps of the Split Scenario

- Getting network access
  - Using DHCPv6 or IPv6 stateless address autoconfiguration
- Home Agent assignment done by DNS request from MN
  - Requesting for a FQDN of a HA (e.g. ha.service-provider.com)
  - Requesting for a MIPv6 service (e.g. mip6.ipv6.service-provider.com)
- Setting up an IPsec security association between HA and MN
  - Use of Internet Key Exchange version2 (IKEv2) for this purpose
  - For this purpose the HA may contact a PKI or AAA for MN authentication and service authorization
- Assignment of a Home Address to MN
  - Done within the IKEv2 exchange
  - MN could propose a Home Address
- Update of the MNs DNS entry with the new Home Address
  - Triggering of DNS update within Binding Update from MN to HA
  - HA updates DNS directly or further delegates this to AAA

Steps of the Integrated Scenario

- Getting network access
  - Using DHCPv6 or IPv6 stateless address autoconfiguration
- Home Agent assignment done by DHCPv6 request from MN
  - HA is provided by the Mobility Service Provider
    - ❑ AAA of Mobility Service Provider provides HA to DHCPv6
    - ❑ DHCPv6 finally assigns HA to MN
  - HA is provided by Access Service Provider
    - ❑ Direct assignment of HA to MN by DHCPv6
- Remaining steps identical to split scenario
  - Setting up an IPsec security association between HA and MN
  - Assignment of a Home Address to MN
  - Update of the MNs DNS entry with the new Home Address

Handover Problem

- Authentication in wireless networks is usually based on EAP
- Cryptographic material derived by EAP methods is used to establish SAs between the MN and the access network
- Drawbacks
  - EAP authentication is usually a time-consuming process and it is expected to be performed each time the MN moves to a new EAP authenticator, even when it has been authenticated recently and owns unexpired keying material
  - The home domain is contacted each time the MN must be authenticated, introducing additional delay when the home domain is far away
- Both drawbacks produce undesirable delays during the handover process

Possible Solutions

- Context transfer
  - Transmission of the cryptographic keys from the current gateway to candidate ones
  - Widely criticized from the security standpoint
- Pre-authentication
  - The MN authenticates itself with candidate access devices (APs or ARs) before attaching to them
- Fast re-authentication
  - Different approaches
    - Avoid running a full EAP authentication exchange
    - Support efficient re-authentication for the EAP peer locally within the visited domain
    - Use GSABA (Generic Service Authorization Architecture) proxy as a Key Distribution Center (KDC) to push keying material to the network access equipment (without re-running EAP)

Contacting ENABLE

- Project web site:
  - http://www.ist-enable.org
- Project Coordinator:
  - Ivano Guardini (ivano.guardini@telecomitalia.it)
- Dissemination, Liaison and Standardization:
  - Jordi Palet (jordi.palet@consulintel.es)