AUTOMOTIVE | INFOCOM | TRANSPORT & ENVIRONMENT | AERONAUTICS | SPACE | DEFENCE & SECURITY

Secure IPv6 deployment

IPv6 conference, 14.12.2010, Ghent

Wolfgang Fritsche, IABG

Agenda

Scope and objectives of the project

Example user scenarios

- **E-government**
- **Mobile user**

Further general aspects for secure IPv6 deployment

Conclusion

Scope and objectives of project

Scope and objectives of the project (1/3)

EC contracted project on “IPv6 security models and dual-stack (IPv6/IPv4) implications”

- Project started October 2009 and last until July 2010
- Contract assigned to IABG and EADS

Main objective

- Contribute to the secure deployment of IPv6
- Focus on existing and emerging private and business user scenarios

Scope and objectives of the project (2/3)

- Analysis and evaluation of emerging and existing private and business user scenarios regarding:
  - New security models and architectures possible by using IPv6
  - Benefits and shortcomings of IPv6 security models and architectures compared to IPv4 security models and architectures
  - Benefits and shortcomings introduced by IPv6 and IPv4 coexistence
- Recommendation for further action
  - Fixing vulnerabilities
  - Identifying missing research and developing work
  - Outlining open standardization issues
  - ...
- Stakeholders and experts from respective areas are involved in the study via direct contacts and 2 workshops
  - 1st workshop held on 23rd February in Brussels
  - 2nd workshop held on 25th June at German IPv6 summit

Scope and objectives of the project (3/3)

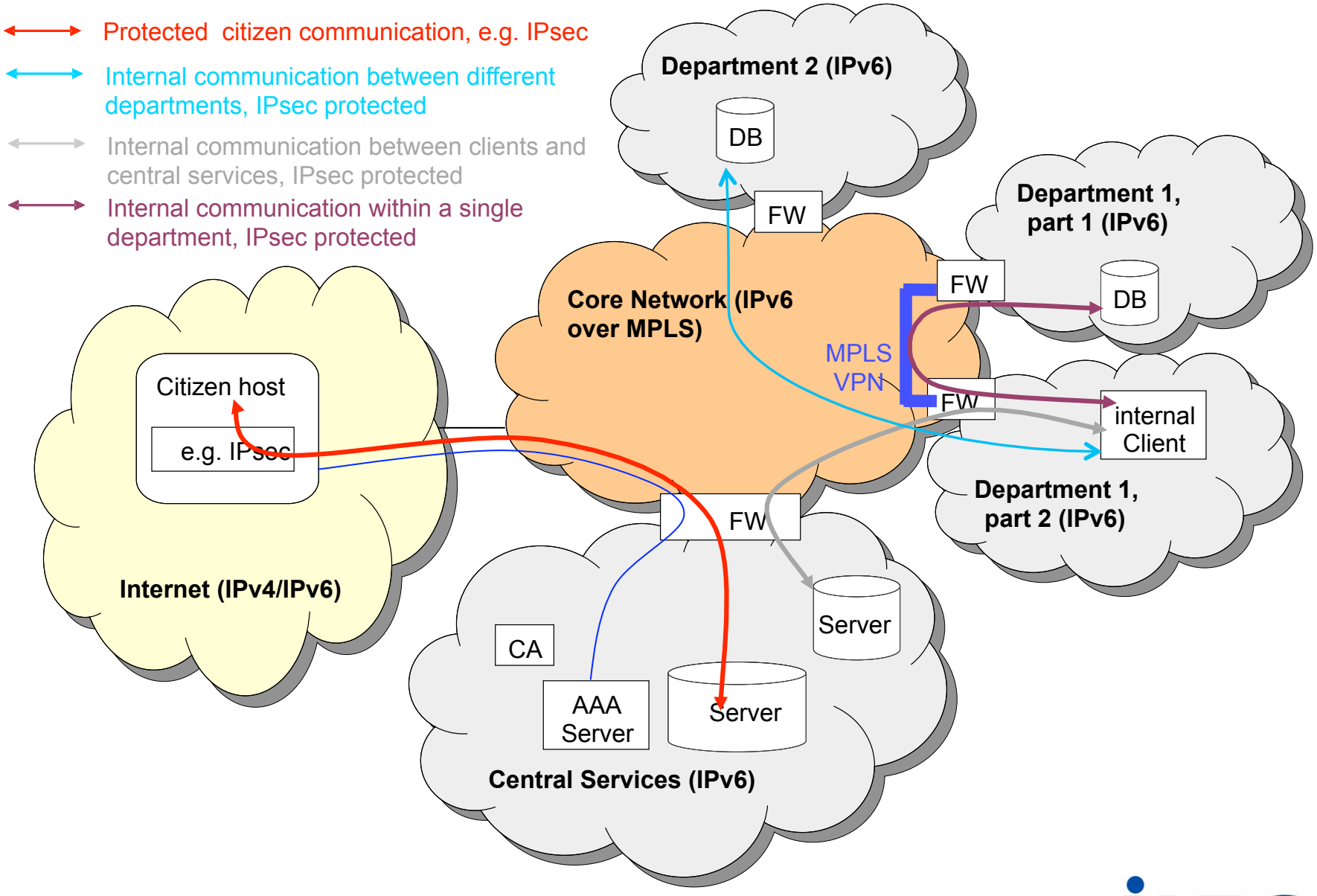
- Project started with following scenarios
  - E-government
  - Mobile user
  - Public safety
  - Direct secure end-to-end communication
  - Corporate networks
  - Personal Area Network (PAN)
  - Access security
  - Car-to-car communication
  - Home network connectivity and networked gaming
  - Collective transports
- Part of these have been investigated in more detail in 2nd phase of project
  - Including analysis of IPv6-IPv4 coexistence

Example scenarios

E-Government: Overview

- Scenario:
  - Government network comprises:
    - Interconnections of different departments (e.g. ministries) and central services networks
    - Protected connection of citizens to e-government services
  - E-government services for citizens:
    - Voting, tax declaration, car registration, …
    - Centralization of transactions and processes saves administrative effort and costs
- IPv6 relevance:
  - Government network administrators suffer from multiple NAT levels
    - High effort for management
    - Difficult to introduce new services like VoIP
    - Restricted flexibility to reorganize network after election
  - Governments are now planning the migration to IPv6, e.g. the German DOI network

E-Government: Security architecture



E-government: Key IPv6 security advantages and challenges

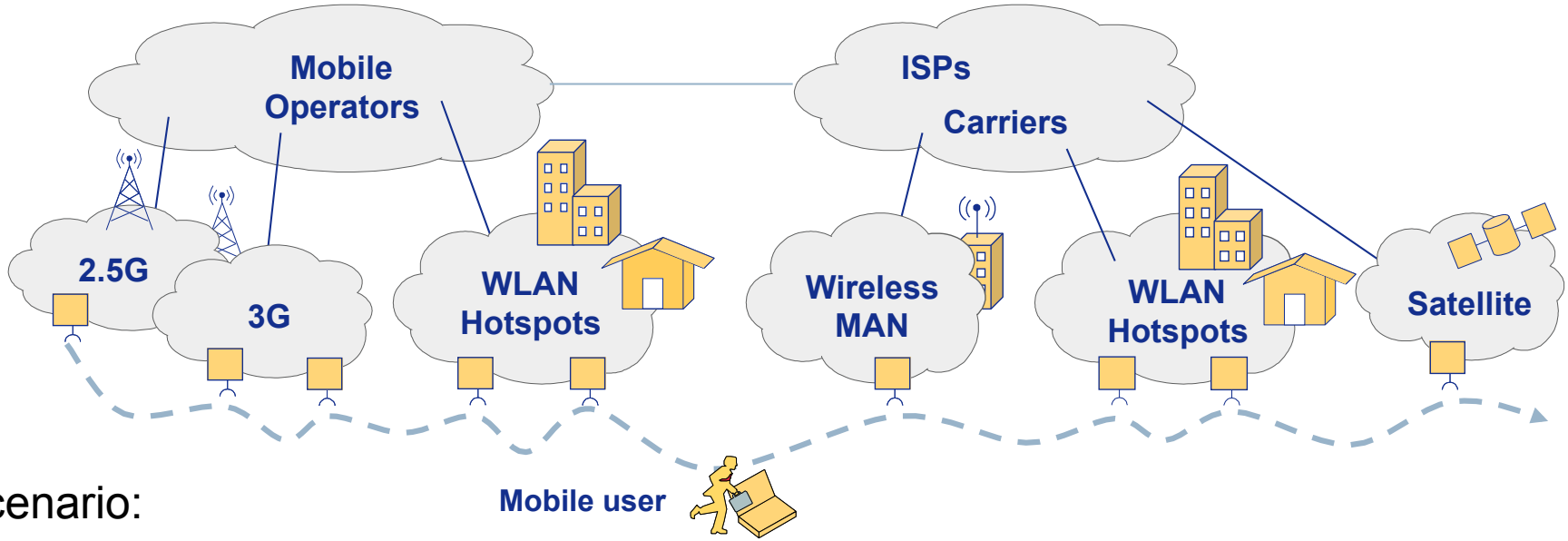
Advantages:

- IPv6 removes the need for NAT boxes
  - Allows an efficient end-to-end security approach using IPsec
- Secure Neighbor Discovery (SEND) allows secure configuration of hosts in governmental LANs

Challenges:

- End-to-end changes the security perimeter
  - New mechanisms are required for preventing DoS attacks
- Lack of support of SEND in implementations, e.g. on Windows
  - Use of alternative mechanisms to protect against ICMPv6 attacks, e.g.
    - Detect RA messages from attackers (router on wrong port, with wrong IP or MAC address, …)
    - Detect contradicting NS and NA messages
    - …

Mobile User: Overview



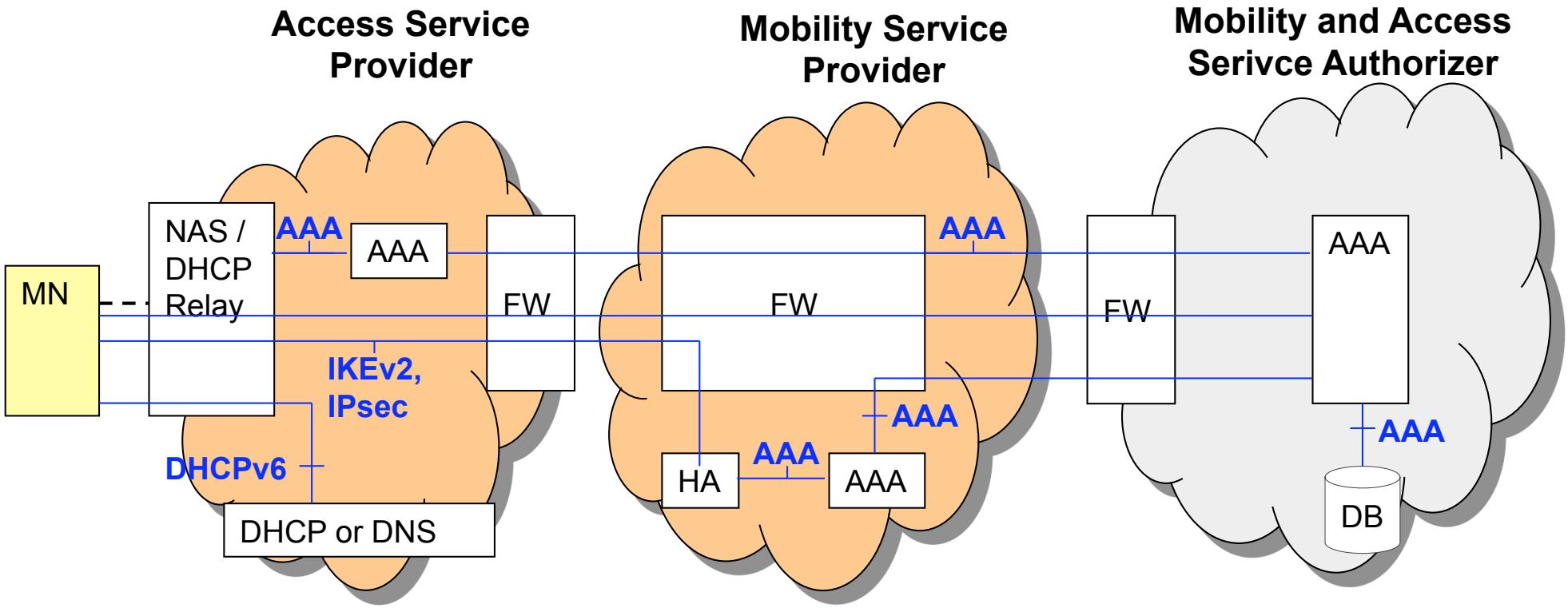
Scenario:

- A business or private user is on a trip and is roaming between different access networks and service providers
- Strong requirement for (seamless) session continuity

IPv6 relevance:

- Huge demand for address space due to fast growing number of mobile devices and diversity of wireless access networks
- Efficient autoconfiguration mechanisms required for mobile devices
- Mobile IPv6 is envisaged by 3GPP and WiMax forum for handover between different access technologies

Mobile User: Security architecture



Secure bootstrapping and deployment of Mobile IPv6 required

- MIPv6 bootstrapping mechanisms standardized by IETF: mobile device securely configures information about Home Agent, Home Address, and Keying material
  - Mobility and Access Service Authorizer is one organization: MIPv6 bootstrapping information is provided during network access, e.g. using DHCPv6 or EAP
  - Mobility and Access Service Authorizer are different organizations: MIPv6 bootstrapping information is provided by DNS
- IPsec / IKEv2 protects information exchange between MN and HA
- Return routability protects information exchange between MN and CN

Mobile User: Key IPv6 security advantages and challenges

Advantages:

- Secure bootstrapping of mobility support (HA, home address, keying material) is only standardized for Mobile IPv6
- Secure route optimization (direct communication between MN and CN) is only standardized for Mobile IPv6 (return routability)

  (IPv6 privacy extensions prevent from location tracking)

Challenges:

- Firewalls and other middleboxes need to allow Mobile IPv6 and bootstrapping control information
  - Manual configuration is difficult and middlebox traversal mechanisms (e.g. NSIS) are still not mature enough
- Deploying IPv6 privacy extensions makes firewalling / monitoring more difficult due to dynamically changing addresses
  - New mechanisms, e.g. using random interface identifiers, are required

Further general aspects for secure IPv6 deployment

Further general aspects for secure IPv6 deployment

- General aspects to be considered:
  - IPv6 needs to be considered in the security policy
  - Filtering / monitoring rules have to be adapted
    - More friendly to ICMP (address autoconfiguration, PMTU discovery, …) and IP multicast
    - Many combinations of extension headers possible
      - … also having a performance impact for filtering
  - Network devices have to be hardened appropriately
    - Install latest software and bug fixes
    - Allow advanced services like Mobile IPv6 only when they are really needed
  - If possible prefer dual stack for transition against tunnel
    - Easier for monitoring and inspection
    - Issues like identification of legitimate 6to4 relays or Teredo servers, reflection attacks, opening permanent holes in NATs/firewalls, …
  - Security functionality like application appliances of firewalls or anti-virus checks are only partly available
  - Staff has to be trained
  - …

More information concerning this study under

http://ec.europa.eu/information_society/policy/ipv6/index_en.htm

Conclusion

Conclusion

- IPv6 brings many advantages not directly related to security …
  - large address space, stateless autoconfiguration, efficient integration of mobility, clear header structure, …
- … plus further advantages related to security
  - allowing efficient large scale end-to-end security, secure neighbor discovery, secure Mobile IPv6 bootstrapping, secure Mobile IPv6 route optimization, …

- There are some challenges to be dealt with …
  - lack of SEND implementation, required new approach to prevent DoS attacks in end-to-end scenarios,
- … plus some tasks to be done
  - specification of IPv6 security policy, adapt monitoring / filtering rules to IPv6, harden network devices, perform IPv6 (security) trainings, …

Dealing with IPv6 security challenges and tasks will allow you an efficient and secure IPv6 deployment

Contact

Contact

Wolfgang Fritsche

Head of Internet Competence Center

Phone: +49 89 6088-2897
Email: fritsche@iabg.de

AUTOMOTIVE | INFOCOM | TRANSPORT & ENVIRONMENT | AERONAUTICS | SPACE | DEFENCE & SECURITY

Secure IPv6 deployment

IPv6 conference, 14.12.2010, Ghent

Wolfgang Fritsche, IABG

