# EU Cross-border e-ID & Safety Services

**Antonio Skarmeta Gómez**
**Universidad de Murcia**

**IPv6@GOV workshop Brussels, 23-24 January, 2013**

# Index

- Motivations
- General objectives
- Cross-border services
- Cross-border safety
- Conclusions


# Motivations

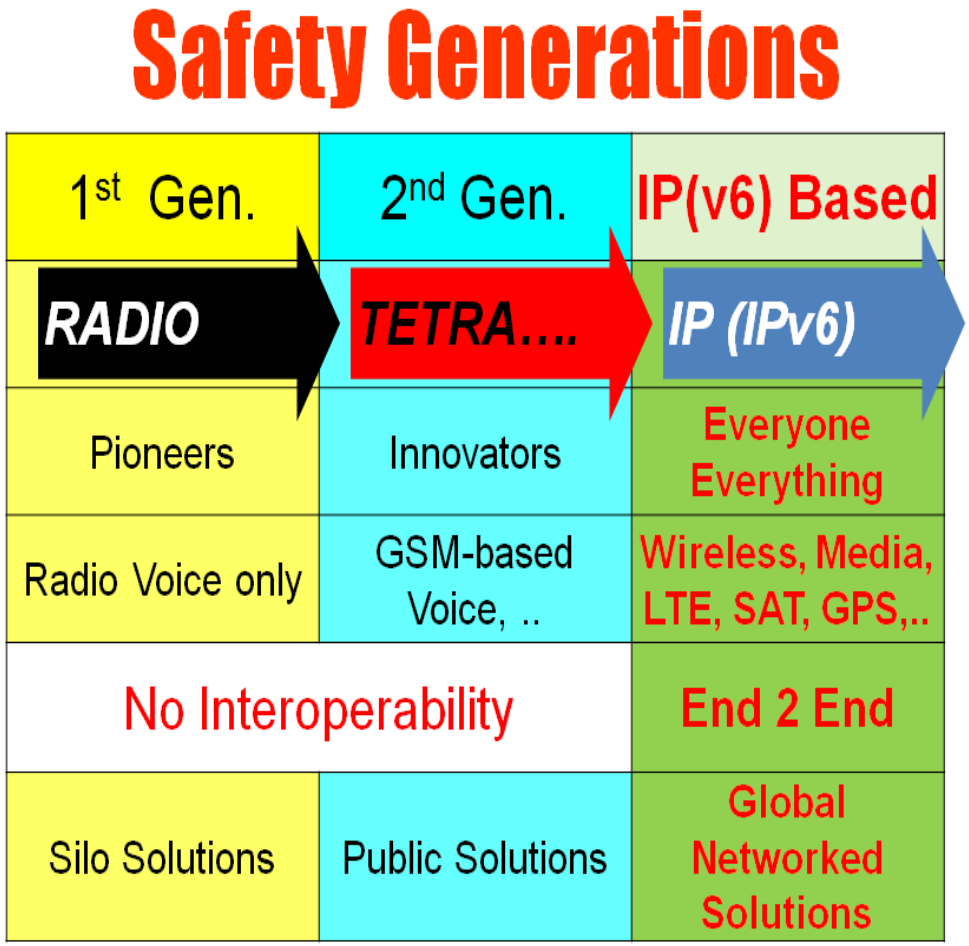
- The development and deployment of new eGovernment cross-border services are going to be done in parallel with IPv6 Transition.
- It is critical to ensure a seamless interoperability between MS in a foreseen uneven IPv6 Transition scenario.
- GEN6 will validate different interoperability scenarios among MS and European Institutions, each of them with a different degree of IPv6 transition.
- GEN6 pilot will be also open to an active collaboration with the European Commission (DIGIT) in order to evaluate the transition to IPv6 of the sTESTA network and provide in collaboration with them strategies for IPv6 support on the LSP (Large Scale Pilots).

- Identification of the needed technical arrangements for interoperability of the IPv6 transition for all domestic strategies.
- Arrange with the Commission the active (IPv6 natively available) or passive (IPv6 not ready, so transition need to be used) role of sTESTA in the pilot, depending on its IPv6-readiness.
- Prepare different transition scenarios in a mixed environment of IPv4 and IPv6 clouds in the government tiers (national, regional, universities, …),
- Test the interoperability scenarios and compile a troubleshooting manual, roadmap of actions developed and guidelines.
- Define a clear and detailed transition plan of an IPv4-based public safety network and service to IPv6-based networks.
- Evaluate the relevance of IPv6 in safety, security, and mobility aspects.
- Define the tools for an easy management and governance of the cross-border pilots.

# General Objectives

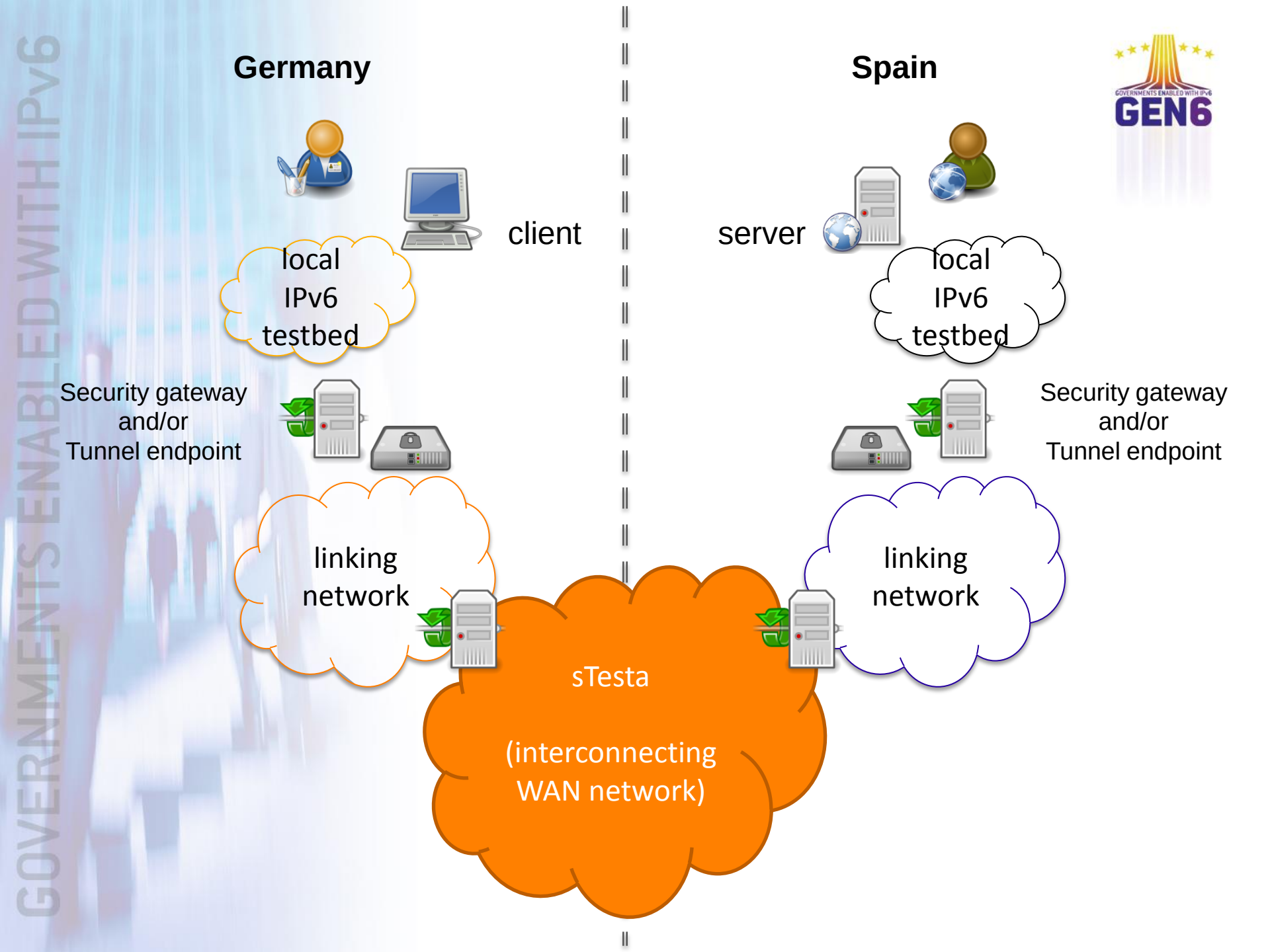
- **IPv6-readiness for cross-border services**
  - To establish the basis of a wider IPv6 readiness for eGovernment cross-border services in Europe.
  - Design and provide end to end IPv6 connectivity for e-goverment services considering the different situations that actually concur on the LSP STORK2.0, SEMIRAMIS, eCODEX, EUCARIS, etc).and operational services like the ones corresponding to ISA (Interoperability Solutions for Administrations),
  - This IPv6 readiness should be based in a set of interoperability networking scenarios taking into account scenarios based on sTESTA
  - Evaluate and collaborate with the national networks in order to make IPv6 enable the PEPs (Pan European Proxy Service) entities that are being used on STORK and STORK2.0 and that now are a key component of the end user authentication process based on national ID on several services around Europe (see for example the ECAS access system).

- **IPv6 Safety**
  - To put in place and evaluate IPv6 in public safety networks and service could substantially improved interoperability and end-to-end security, which is especially crucial for cross-boarder public safety missions.
  - To provide more and advanced functionalities than existing ones based on IPv6, especially in a cross-border scenario.

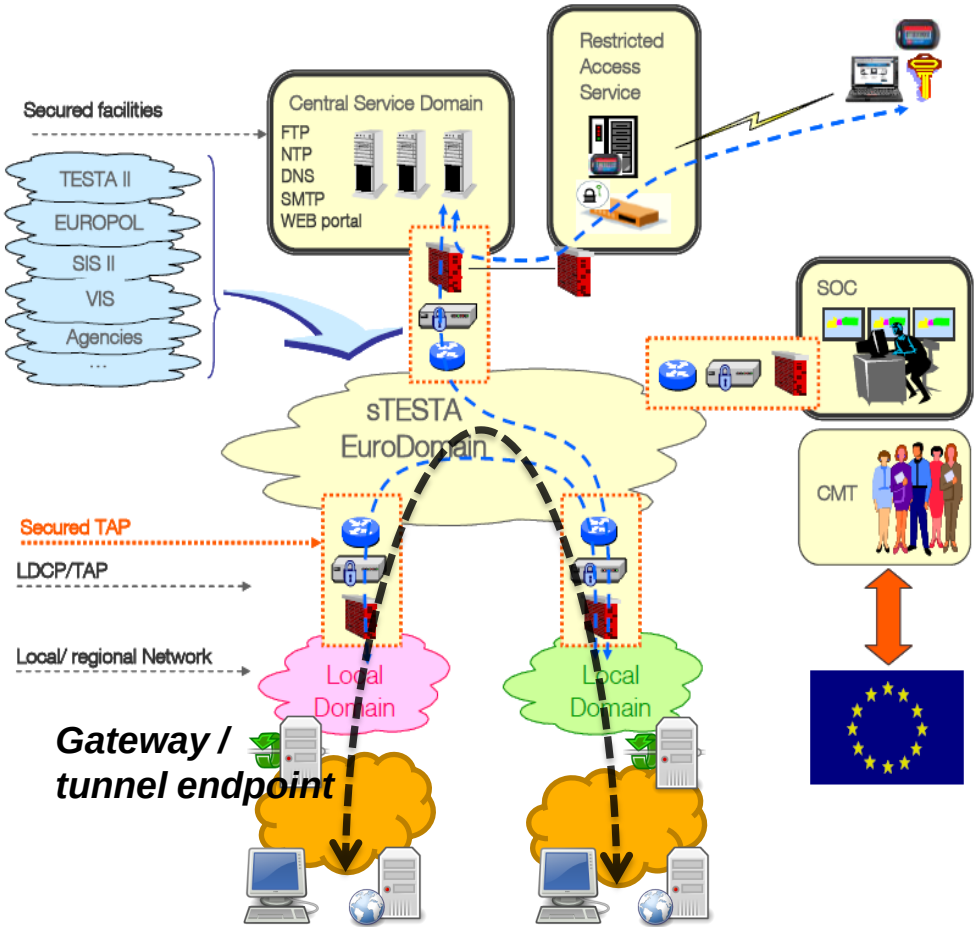


# Cross-border Services

- The pilot will open to an active collaboration with the European Commission (DIGIT) following the model of the STORK project.
- Once the different scenarios of the IPv6 transition are tested in the National networks, the cross-border scenarios will start.
- The project will look for synergies with other projects from past calls (STORK, SEMIRAMIS, ISA Services) to define a portfolio of cross-border services
- Test the interoperability scenarios and compile a trouble-shooting manual, a roadmap of actions developed and guidelines.

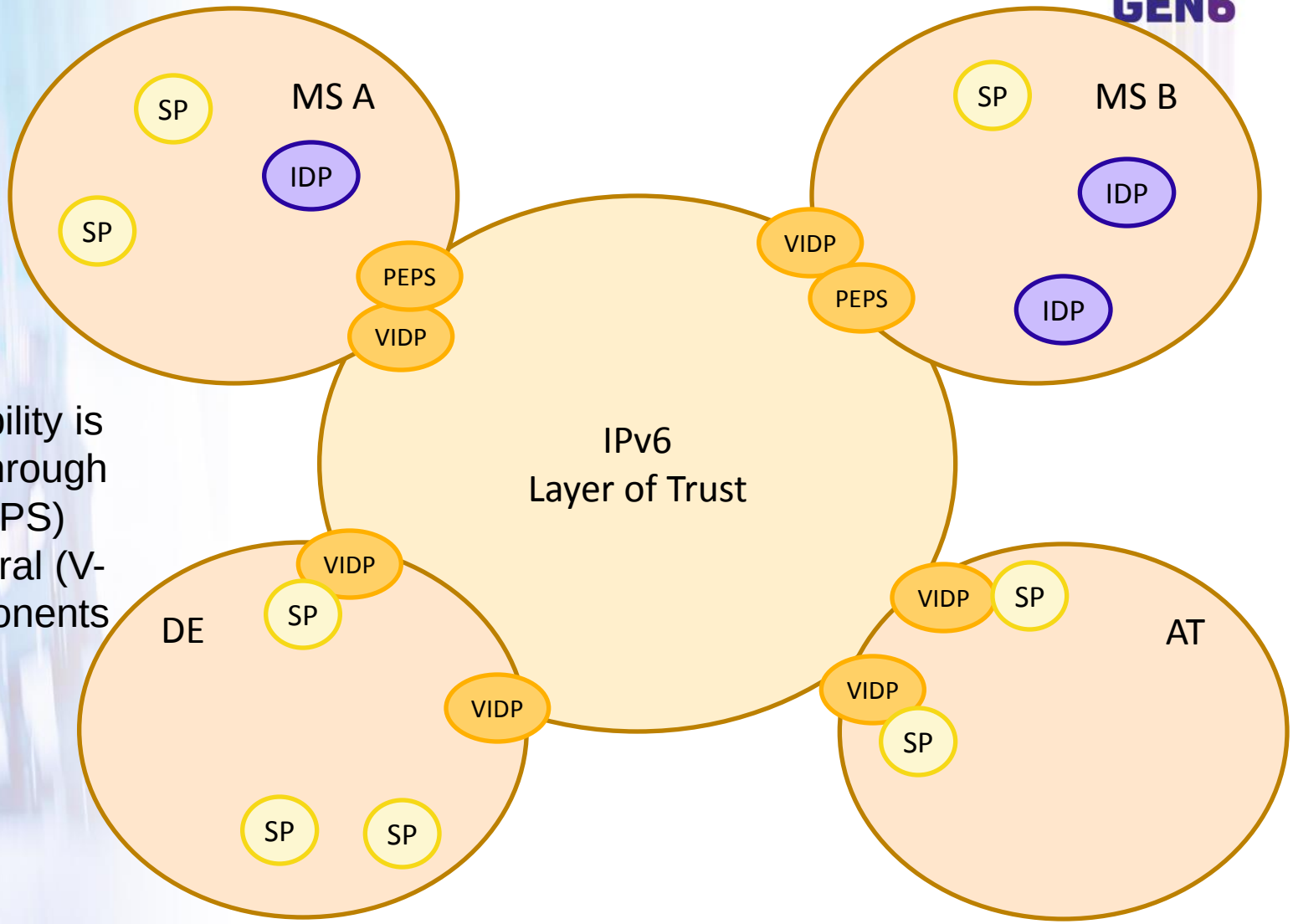

Germany
Spain
client
server
local
IPv6
testbed
local
IPv6
testbed
Security gateway
and/or
Tunnel endpoint
Security gateway
and/or
Tunnel endpoint
linking
network
linking
network
sTesta
(interconnecting
WAN network)
GOVERNMENTS ENABLED WITH IPv6
GEN6

- A Local Domain (LD) can either be directly connected to the EuroDomain via a TAP (Turnkey Access Point) located in its LDCP (Local Domain Connection Point) or be interconnected via another network (e.g. a national network) which eventually hosts the TAP in its LDCP.
- It is important to define the TAP means of supporting IPv6.
- There will be a relevant impact on the security box.

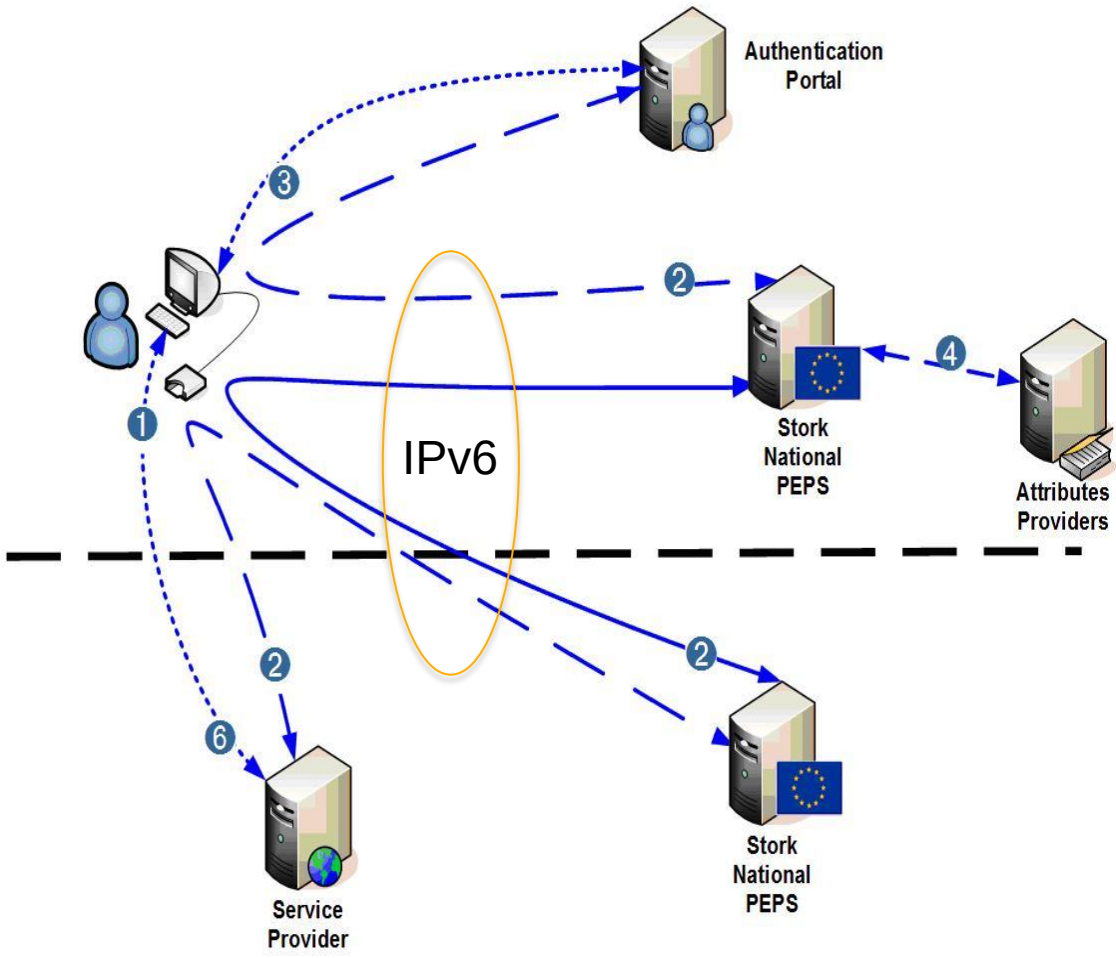



*Local Domain Clients and Services*

eID-Interoperability is achieved through central (PEPS) and decentral (V-IDP) components



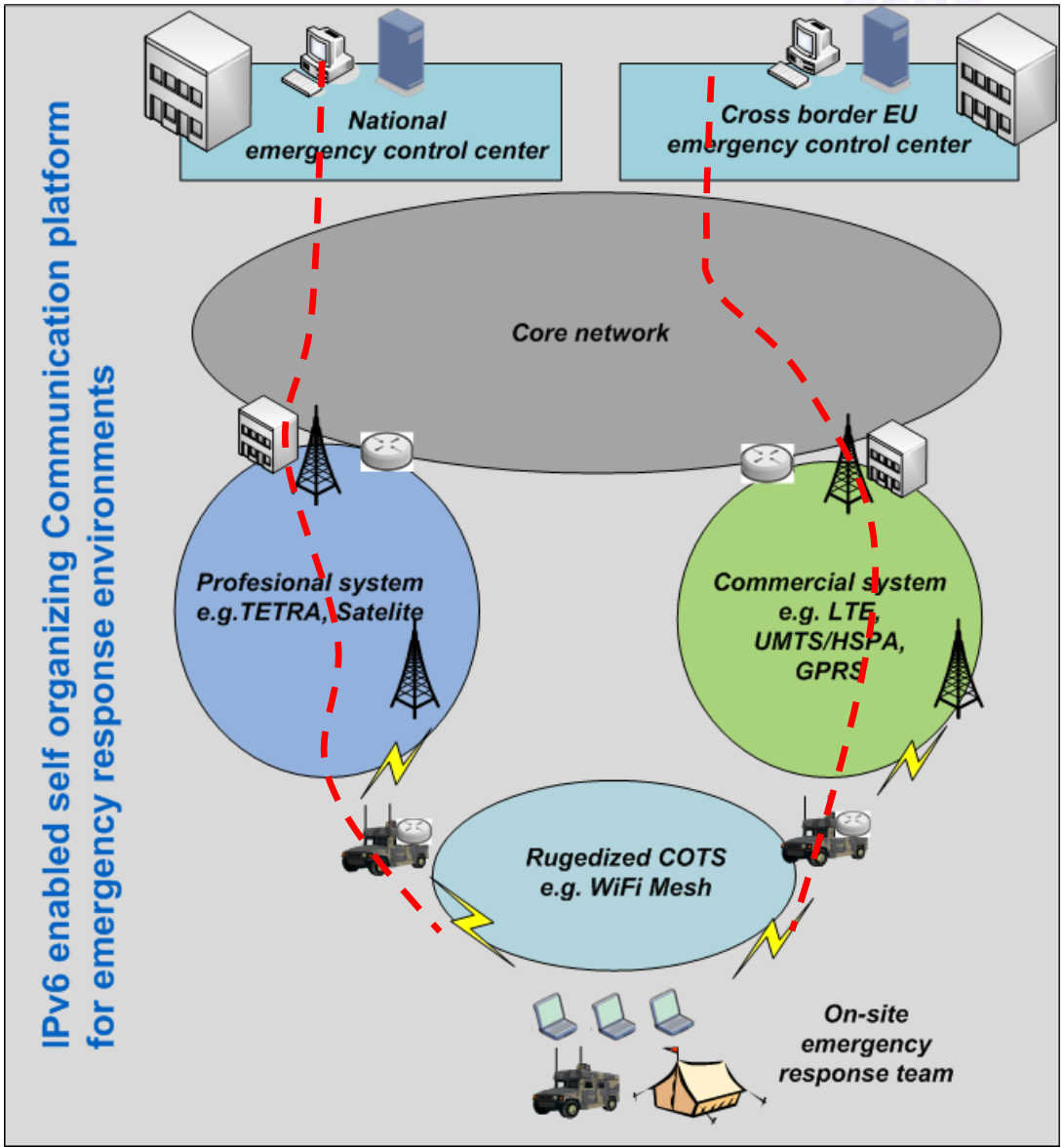
- EID Integration suporting IPv6 in PEPs provided by STORK
- STORK ensures cross-border eID interoperability at European level
- Integrating PEPs in the IPv6 national goverment services provided by GEN6
- Smoothly integration of IPv6 in goverment authenticated services in cross-border



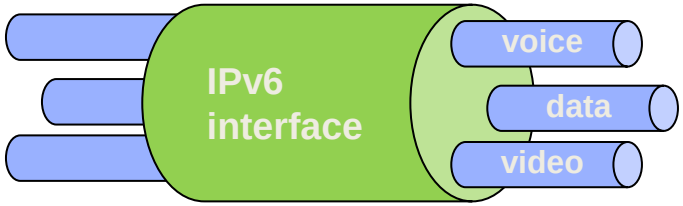
# Cross-border Safety

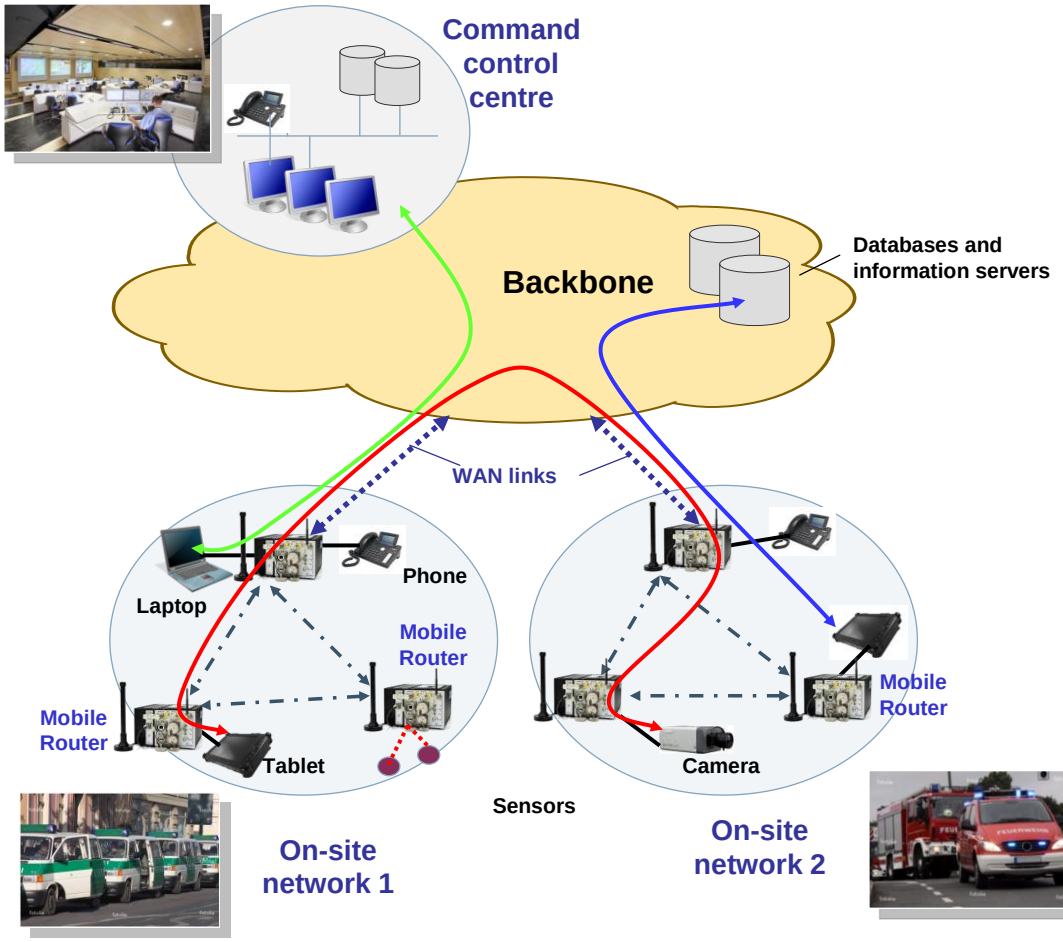
# High level system view

- Communication between different on-site teams in order to:
  - exchange videos or sensor data
  - documents like maps
- Integration of:
  - Sensors
  - Wireless comm.
  - VANET and NEMO
  - MCoA

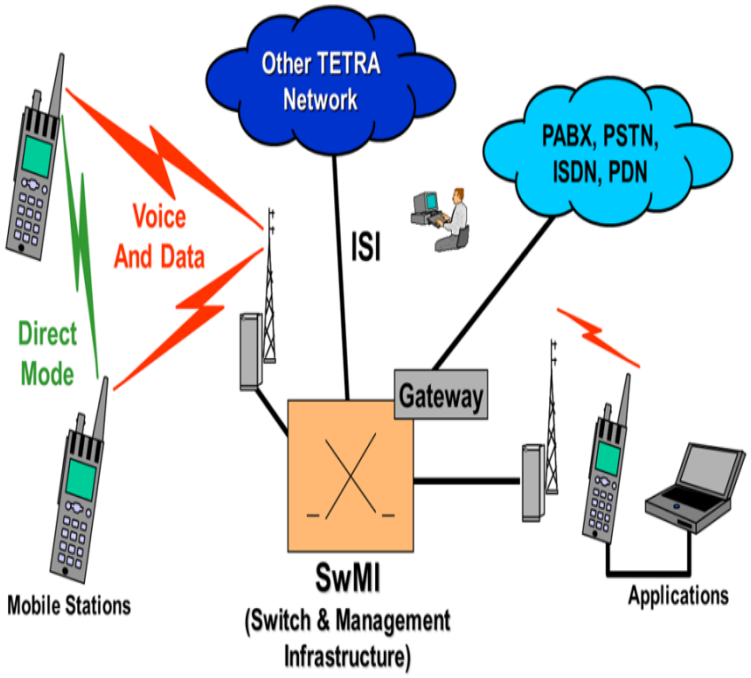


- System setup
  - Connectivity plan (interconnection interfaces, interconnections between sub-systems on a national scale, cross-border connectivity plan)
  - Cross border system functional requirements and configuration profiles
  - IPv6 as interconnect interface for cross border EU public safety response team collaboration
    - Fixed
    - Mobile/wireless



- IP-based communication among on-site end devices (radios, mobile phones, notebooks, etc.)
  - Uses management software to coordinate group calls,
  - Public services actors as end-users
- Ongoing work to extend this testbed into a mobile solution, i.e.:
  - A “Push-To-Talk” server box with a power source (mobile)
  - Deployable WiFi / UMTS / 3G connection
  - Radio gateways
  - End devices – mix of radios, mobile phones, etc.



GOVERNMENTS ENABLED WITH IPv6

# Target environment

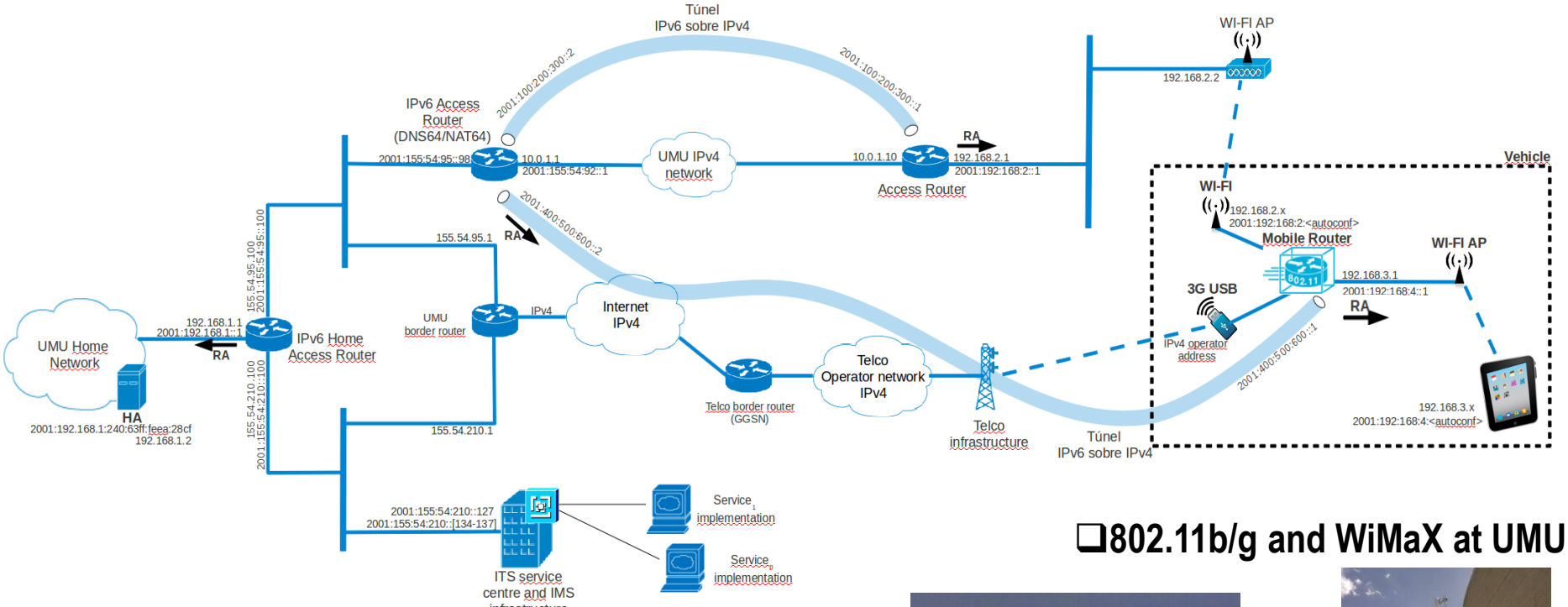
- **Voluntary Fire Brigade** (VFB), Public Fire Fighter Service (PFFS) of the Municipality of Ljubljana (MOL), Department for Protection, Rescue and Civil Defence (URSZR)

- Strategic Emergency Control Centre Support Unit (SECCSU)
  - a mobile on-site command unit with a team of four operators responsible for on-site fire fighter intervention coordination on one side and communication with the Strategic Emergency Control Centre (SECC) on the other side

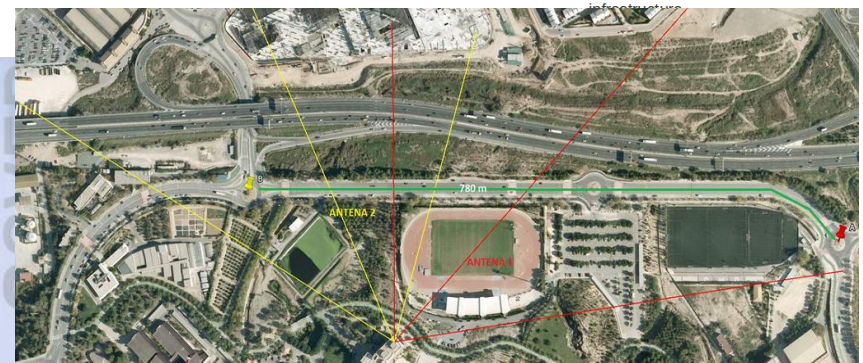

# Interoperability Point Proposal – technical aspects

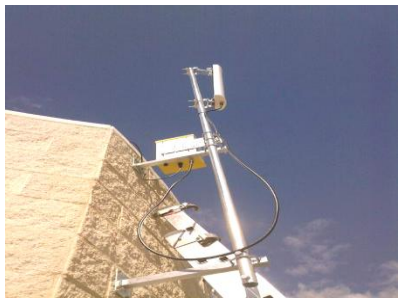
| Interoperability Point | Protocols/Functions | | |
|---|---|---|---|
| GEN6 IOP | Application Layer | HTTP, HTTPS, SIP | |
| | Transport Layer | TCP, UDP,<br>RTP, RTCP | |
| | Network Layer | Unicast and Multicast Forwarding | IPv6,<br>IPv6 with DiffServ |
| | | Unicast Routing | OSPFv3, RIPng,<br>MP-BGP |
| | | Multicast Routing | PIM-SM, PIM-SSM |
| | Link layer | Ethernet (802.3) | |
| | Physical Layer | Electrical: UTP Cat6 | RJ 45 |
| | | Optical: 1000Base-SX | LC connector |

# IPv6 Spain Mobile testbed deployment




❑802.11b/g and WiMaX at UMU



- Need to validate eGovernment cross-border services in parallel with IPv6 Transition.
- Important to define Best Practice:
  - Connectivity scenarios
  - Possible requirements on transition mechanism
  - First design on border-services to be tested
- Evaluate and analysis of existing proposal on other EU projects related to interoperability and testing IPv6 across borders
  - Possible synergies and inputs
  - Platforms or services to be integrated