Title: **Deliverable D4.2** **Cross-Border pilot governance**	**Document Version:** 1.0

Project Number: 297239	**Project Acronym:** GEN6	**Project Title:** Governments ENabled with IPv6

Contractual Delivery Date: 31/12/2013	**Actual Delivery Date:** 06/01/2014	**Deliverable Type* - Security**:** R – PU

* Type:	P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class:	PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author: Martin Krengel	**Organization:** Citkomm	**Contributing WP:** WP4

Authors (organisations):

Martin Krengel (Citkomm), Gerold Gruber (Citkomm), Carlos Gómez (MINHAP), Mojca Volk (ULFE), Gabriela Gheorghe (University Luxembourg), Antonio Skarmeta (University Murcia)

Abstract:

This deliverable presents the governance principles and tools defined to monitor the pilots operation In particular, this deliverable focuses on the pilot for IPv6-readiness for cross-border services.

Keywords:

IPv6, Governments, monitoring, measurement, pilots, national, cross-border, partners, outcome, impact, governance, ticket system, trend

Revision History

The following table describes the main changes done in this document since its creation.

Revision	Date	Description	Author (Organization)
v0.1	24-09-2013	Document creation, initial ToC	Martin Krengel (Citkomm)
V0.2	3-12-2013	Addition of information from MINHAP	Carlos Gómez (MINHAP)
V0.3	18-12-2013	Consolidation input from different partners	Martin Krengel (Citkomm)
V0.4	02-12-2013	Consolidation, Executive Summary	Martin Krengel (Citkomm)
V1.0	06-01-2014	Final Version	Martin Krengel (Citkomm)

Disclaimer

The GEN6 project (number 261584) is co-funded by the European Commission under the ICT Policy Support Programme (PSP) as part of the Competitiveness and Innovation framework Programme (CIP). This document contains material that is the copyright of certain GEN6 partners and the EC, and that may be shared, reproduced or copied "as is", following the Creative Commons "Attribution-NonCommercial-NoDerivs 3.0 Unported (CC BY-NC-NC 3.0) licence. Consequently, you're free to share (copy, distribute, transmit) this work, but you need to respect the attribution (respecting the project and authors names, organizations, logos and including the project web site URL "http://www.gen6.eu"), for non-commercial use only, and without any alteration, transformation or build upon this work.

The information herein does not necessarily express the opinion of the EC. The EC is not responsible for any use that might be made of data appearing herein. The GEN6 partners do not warrant that the information contained herein is capable of use, or that use of the information is free from risk, and so do not accept liability for loss or damage suffered by any person using this information.

Executive Summary

The cross border pilots in GEN6 will enable IPv6 connected services involving infrastructures from several partners. To set up a control and operation level for this infrastructure a central monitoring and trouble handling instance is set up for GEN6.

The IPv6-readiness for cross-border services uses existing infrastructures of secures networks of governmental networks in its core. For the demonstration of IPv6 connectivity special service connection will be established. The operational services for the core infrastructure are well established, because they are part of the existing infrastructures. An extended Monitoring is required for the specific services being involved in the pilot as well as for the national network extensions that must be made available for the pilot connectivity.

The IPv6 Safety pilot integrates components and networks directly used over public networks with focus in the Internet. The components are connected for the purpose of this pilot, so the set up and the operation of the monitoring is part of the GEN6 activities.

The monitoring and the event handling will be supported using three well known tools. All tools are web based and will be made available to all involved partners. For the event handling the tool ‘Icinga’ will be used. Icinga allows the definition and monitoring of relevant connections and system parameters and controls the operation between set thresholds. Performance and trend data, that are not relevant for event notifications, will be integrated in a “Munin” system. This gives long term trend statics and produces graphs to view network and application latency und such things more. In case of recognized problems a ticket system based on OTRS is established. All partners are integrated as role with responsibility for their infrastructure components.

Table of Contents

Figure Index

1. INTRODUCTION

This Deliverable 4.2 describes the governance principles and tools to monitor the pilots operation and identifies the required tools to evaluate system operation and integration architecture. Gen6 deals with existing infrastructures as well as pilot infrastructures only implemented for the purpose of demonstration in GEN6. This deliverable focuses those parts of infrastructure being outside of the existing infrastructures for pilot use only.

Within this a trouble management system is set up and operated during the whole pilot production. Additionally an appropriate system monitoring is performed. The goal for the system monitoring is twofold. First, a database is created which allows an efficient validation and verification of the overall concept. The second goal of the monitoring is the support of the pilot in case of problems.

2. Requirements for Monitoring

2.1 IPv6-readiness for cross-border services

2.1.1 Pilot Description

Connection between administrations is often performed through private administrative networks (e.g. sTESTA). Most of these networks (either public or private) are not ready for the use of IPv6 nowadays.

The IPv6 readiness pilot describes current network architecture for public administration accessing cross-border services, emphasising on the most promising network to provide IPv6-based interconnection between administrative networks of the different Member States: sTESTA. Therefore a communications architecture is established where current infrastructure can evolve towards an IPv6-readiness, assuring the seamless IPv6 interconnection between different Member States in a foreseen uneven IPv6 transition scenario.

As a practical check the project has to implement a pilot that demonstrates the feasibility of the IPv6-based cross-border service, involving two of the Member States participating in the pilot: Spain and Germany. This Pilot focuses on the IPv6-readiness of currently in-production cross-border eID authentication services (i.e. STORK and German eID system).

Details on the pilot are described in the deliverable 4.1.1 of the GEN6 project.

2.1.2 Architecture

German site

Starting from the Citkomm network the connection to the Spanish site over secured networks first connects to the national government backbone. The customer edge of this network is a PE router and a cryptographic gateway. On the Citkomm site a specific firewall secures the interface.

All further infrastructure of the network is hidden, because only authorized ports are open and so no availability management from the customer edge is possible. The next possible check is the test of the connectivity through the established tunnel to the systems on the remote site.

Due to this for connectivity check only a few checkpoints can be established

In the pilot two different tunnel technologies have been proved. One using OpenVPN, the other one based on a SIT tunnel. Because those communications are established using different gateways two monitoring scenarios exist.

For Open VPN

- VPN-Gateway (on IPv6)
- VPN-Gateway (on IPv4 – transport layer)
- DOI-Gateway (on IPv4 – transport layer)

- Crypto-Gateway (on IPv4 – transport layer)
- IPv6 destination near to tunnel-end point on remote site

For SIT tunnel

- SIT-Gateway (on IPv6)
- SIT-Gateway (on IPv4 – transport layer)
- DOI-Gateway (on IPv4 – transport layer)
- Crypto-Gateway (on IPv4 – transport layer)
- IPv6 destination near to tunnel-end point on remote site

For the extension of the cross border pilot to an application test based on eID-services from the Citkomm site a network connection to Fraunhofer FOKUS test site in Berlin is established. On this network all components can be part of a detailed monitoring. The involved components are

- VPN-Gateway Citkomm site
- VPN-Gateway FOKUS site
- Business application server at FOKUS site

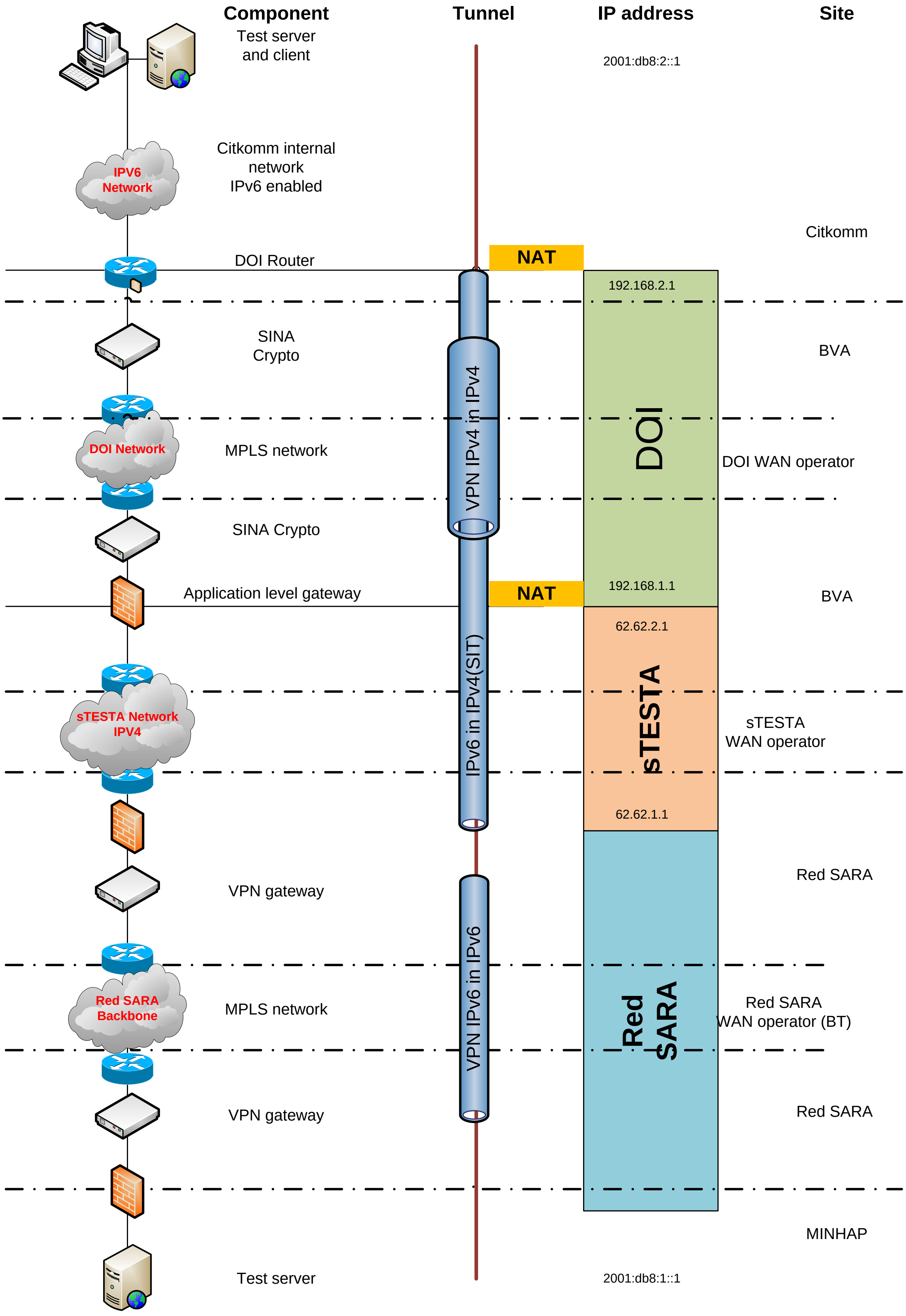

Figure 1: Core Connection over governmental networks

Spanish side

In the case of the Spanish side, the systems and networks involved in the pilot are managed by two different organizations: MINHAP and UMU

Components from MINHAP involved in the pilot

The following elements of the MINHAP infrastructure will be supporting the cross-border pilot:

- The elements for closing the tunnel through sTESTA that connects the German and the Spanish side
- The platform upon which the Spanish PEPS (the electronic identity interoperability node from the STORK project) is running
- The connection area with RedIRIS, the Spanish academic and research network, required to create the private IPv6 path to UMU

It will be also involved the TAP (Turnkey Access Point) of sTESTA, but this is managed and monitored directly by sTESTA operators, so MINHAP has no control over it.

The elements describe above use the following components:

- Servers, running
  - OpenVPN for the sTESTA tunnel
  - Firewalls: Firewall 1, Stonegate
  - Web servers and application servers for the PEPS
  - Other network services hosted in the connection area, such as DNS
- Appliances
  - Fortigate firewalls
  - Load balancers: F5 and Alteon
- Switches
  - Cisco
- Routers

    - Cisco and Juniper

Extension UMU

As it has been mentioned before, in the Spanish side two organisations, MINHAP and UMU are involved. The Extension of the network for UMU involves further components as follows

- IPv6 connectivity to MINHAP done through the native IPv6 connection between UMU-RedIRIS
- Networking elements
    - Switches
        - Cisco
    - Routers
        - Cisco
- Server Element
    - Linux based Server for Authentication and Authorization testing

2.1.3 Monitoring requirements

The main focus on the monitoring is the availability test that the established connections are up an operational. Therefore the basic test is an event check based on the ping test. To make it easier to locate a problem the components on the transport level of the used tunnel service are each monitored via ping also, as far as the components allow this check.

For the tunnel gateways furthermore the used bandwidth on the tunnel interface is integrated for trend monitoring. Also the ping delay is stored in trend monitoring.

Citkomm monitoring requirements

All components for the connection from FOKUS to the national government backbone DOI and furthermore to sTESTA are part of the standard infrastructure and not kind to special implementation for the GEN6 pilot. Therefore all involved components are integrated in the day by day operating and monitoring of Citkomm. There is no special need for further monitoring of these components.

MINHAP monitoring requirements

In the case of MINHAP, the main requirement for the pilot is the full compatibility with the existing monitoring infrastructure.

This monitoring infrastructure is based currently in two platforms:

- Nagios as general purpose platform
- CISCO works for CISCO devices

Monitoring with Nagios

In the case of routers, Nagios monitors, by ICMP, the network layer interface responses, and also the responses of the virtual IP of the LAN side.

In the case of switches, it monitors the ICMP response of the management IP

In the case of servers, there are different parameters monitored, using different tools:

- By means of ICMP messages, network layer interface responses are checked
- By means of IPMI, and making use of the Dell's DRAC installed in the servers, disk status and temperature are monitored in some servers
- By means of SNMP, different HW parameters are also controlled
    - Disk status
    - Temperature
    - Power supply status
    - Voltage
    - Fan status
    - Disk space used by folders

- Also by means of SNMP, some services running in the servers are checked, such as the clustering SW
- By means of http or https calls, Internet services are monitored, checking that they are up and running and also their response time

Monitoring with CISCO works

CISCO works provides a deeper insight on the status of the switches and routers, but it is restricted to the CISCO elements (Juniper routers, also used, are excluded).

The communication is performed using SNMP, and it can get additional information to that managed by Nagios, such as the packet loss in the interfaces, and handle alerts, such us temperature alerts.

Conclusion

So in conclusion there are no special requirements to include components in a specific GEN6 monitoring for the connection paths between Citkomm and MIHAP, because there are fully operated and monitoring as part of the regular infrastructure of the operators. Within only the network extension and the services provided resp. accessed to and from FOKUS and UMU are relevant for further monitoring. In one with this an end to end monitoring for the used cross border service can be provided.

As technical implementation a connection check based on “ping” will be set up. Furthermore the provided services will be checked by connection test on the service port http. For prove of administrative check the access via ssh for Linux servers resp. rdp for Windows servers will be continuously monitored also.

2.2 IPv6 Safety

2.2.1 Pilot Description

2.2.1.1 Overview

The problem of interoperability of communication technologies is one of the main barriers that disaster handling agencies – police, fire brigade, ambulance, SWAT – have to face. The purpose of the cross-border safety pilot is to demonstrate cross-border seamless communication during a crisis situation, in order to emphasize the advantages of IP protocols, and especially of IPv6. The pilot stresses the interoperability of usable communication solutions in a crisis that spreads across country borders.

The pilot involves three GEN6 partners (ULFE, UL and UMU) and covers two relevant use cases to illustrate an IP-based communication and the advantages of IPv6 when actors from different locations need to exchange information (voice, and data). In particular, IPv6 is useful in the situations in which the administrative support from an emergency control point needs to reach a field team moving from one communication network segment to another. In foreign networks, devices can benefit from seamless connectivity when passing between voice-only and data-enabled networks. Moreover, if end-user devices of field responders have unique public IPv6 addresses, they can be easier to reach by a coordination entity.

The IPv6 cross-border safety pilot will concentrate on two main use cases:

- **International on-site intervention,** describing the interconnectivity needs among field teams that need to communicate on-site, in the disaster area.
- **Cross-border remote assistance,** describing the cross-country interconnectivity between on-site teams with resources located in different or remote places; such resources can be for example an expert located remotely from the place of the incident, a database or specific sensors or detectors in a different area from the field teams.

More detailed information about the interoperability needs in cross-border emergencies, as well as the advantages of IP-based communication and the design approach of the GEN6 safety pilot, can be found in the GEN6 D4.1.2 deliverable.

2.2.1.2 Core A-ERCS

The Slovenian pilot, Advanced Emergency Response Communication System (A-ERCS), represents a unique effort in terms of national IPv6 pilots in the GEN6 project by addressing IPv6 communication needs of a specific domain, that is, a fire fighter unit utilizing advanced communications and IoT services during an on-site intervention. Our vision is to contribute to further developments and adoption of advanced, reliable and highly convergent communication systems available for professional use in different emergency and catastrophic situations, and thus take the telecommunication services to the next level in serving for security and wellbeing of mankind. We would like to demonstrate that today a variety of powerful and efficient communication technologies exist that, if combined and orchestrated appropriately with advanced intelligent overlay solutions, can deliver survivable, resilient and autonomous communications able to serve and protect in extreme conditions where communication can represent a vital element of survival. Such solution is called Advanced Emergency Response Communication System (A-ERCS).

In particular, the A-ERCS pilot will demonstrate:

- a scalable and robust overlay system for data transport and rich multimedia service built across professional (e.g. DMR, TETRA, Satellite), commercial networks (e.g. UMTS/HSPA, LTE) and ruggedized commercial-of-the-shelf (COTS) systems (mesh Wi-Fi and ad-hoc WiMax),
- the ability of such a system to deliver seamless connectivity from targeted/affected areas across heterogeneous technologies and public networks, locally as well as on national and cross-border levels,
- capabilities of the IPv6 technology to assist in deployment of automatic network planning and deployment capabilities, vital to all A-ERCS systems,
- IPv6 support for advanced features, such as network, node and host auto configuration,
- the ability of such a system to assure secure and QoS-enabled transmission of data, voice and multimedia-rich services system by relying upon modern professional and commercial telecommunications networks, IoT-based services and IPv6-based technologies and features.

Four preconditions were taken into account during system architecture planning:

1. all A-ERCS system segments are IPv6 enabled (as indicated also in Figure 1-1);
2. architecture and functionalities of existent ERCS system and services remain intact, in an attempt to strictly follow the precondition defined by the SECCSU and OZRCO that the implementation of the A-ERCS pilot must not interrupt current SECCSU operation and service availability but is allowed only to complement and upgrade these while preserving intact reliability, availability and resilience of the current ERCS;
3. the system targets fulfilment of the defined A-ERCS system and services requirements, with a specific focus on the delivery of the required services, as depicted in Figure 1-2;

4. further domain-specific requirements for operational service design of the A-ERCS system must match organizational structure of the emergency rescue intervention procedures, defined by the government bodies and followed in the SECCSU and OZRCO.

The A-ERCS is depicted in Figure 2. It comprises the following system segments (right to left):

- on-site infrastructure, termed **A-ERCS node extension**, comprising:
    - A-ERCS mobile devices for communication throughout the intervention among members of the on-site unit as well as with the Strategic Emergency Control Centre Support Unit (SECCSU);
    - sensor systems, such as water level sensors, earthquake monitoring system, heat sensors, etc., and on-site communication infrastructure, such as Mesh WiFi;
- communication infrastructure, located in the SECCSU vehicle, supporting intervention coordination and communication with the Strategic Emergency Control Centre (SECC) leading the entire operation; the core element of the A-ERCS system, an **A-ERCS node**, is implemented in the SECCSU vehicle;
- an **A-ERCS backhaul supported system**, constructed as a heterogeneous communication infrastructure comprising core network(s) and different professional and commercial networks and ruggedized COTS systems in the role of a (redundant) access infrastructure;
- and an **A-ERCS Strategic Emergency Control Centre** (SECC) located in distributed sites and responsible for the control and cross-communication of the entire operation on a national level (including cooperation and communication with other civil protection, rescue or military services) as well as cross-border connectivity.

The integrated segments together build a converged emergency response infrastructure, capable of providing operational assistance services for the on-site fire fighter unit and the SECCSU team, as well as surveillance of the on-site situation. The targeted services are required to support the defined use case scenarios, delivering communication, multimedia and data services for intervention and situation surveillance purposes. A high-level overview of targeted services is presented in Figure 3.

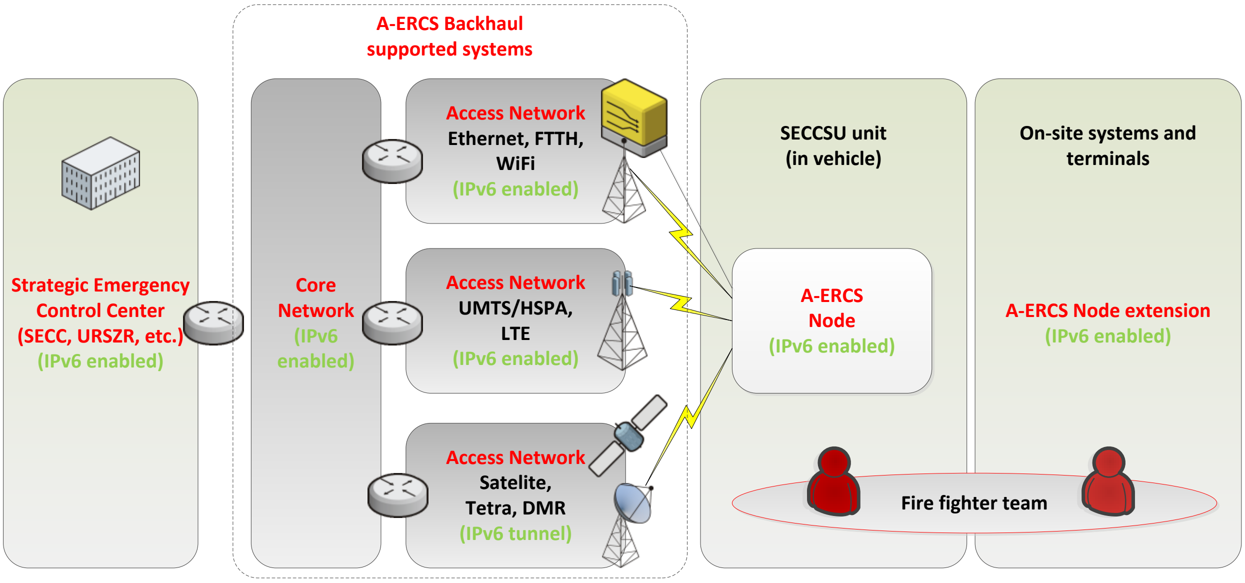
A-ERCS Backhaul supported systems
Strategic Emergency Control Center (SECC, URSZR, etc.) (IPv6 enabled)
Core Network (IPv6 enabled)
Access Network Ethernet, FTTH, WiFi (IPv6 enabled)
Access Network UMTS/HSPA, LTE (IPv6 enabled)
Access Network Satelite, Tetra, DMR (IPv6 tunnel)
SECCSU unit (in vehicle)
A-ERCS Node (IPv6 enabled)
On-site systems and terminals
A-ERCS Node extension (IPv6 enabled)
Fire fighter team

Figure 2: High-level A-ERCS system overview

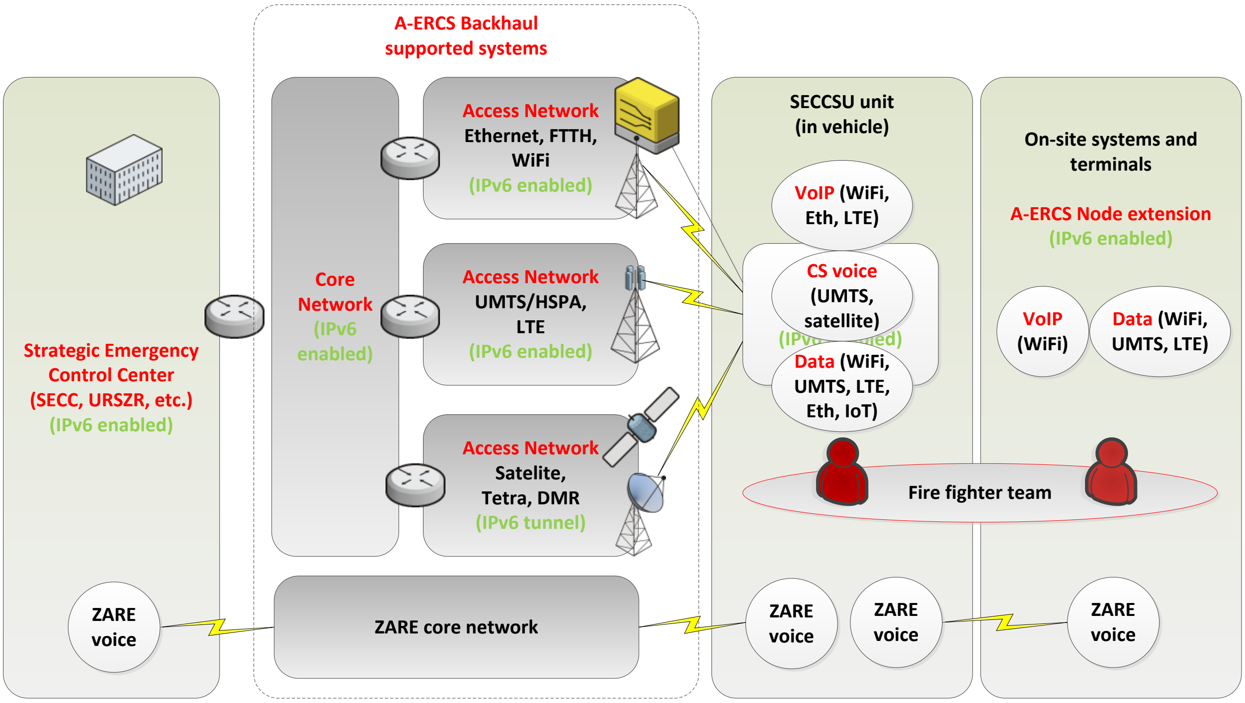
A-ERCS Backhaul supported systems
Strategic Emergency Control Center (SECC, URSZR, etc.) (IPv6 enabled)
Core Network (IPv6 enabled)
Access Network Ethernet, FTTH, WiFi (IPv6 enabled)
Access Network UMTS/HSPA, LTE (IPv6 enabled)
Access Network Satelite, Tetra, DMR (IPv6 tunnel)
SECCSU unit (in vehicle)
VoIP (WiFi, Eth, LTE)
CS voice (UMTS, satellite)
Data (WiFi, UMTS, LTE, Eth, IoT)
On-site systems and terminals
A-ERCS Node extension (IPv6 enabled)
VoIP (WiFi)
Data (WiFi, UMTS, LTE)
Fire fighter team
ZARE voice
ZARE core network
ZARE voice
ZARE voice
ZARE voice

Figure 3: High-level A-ERCS services overview

2.2.1.3 Cross Border extension A-ERCS

The cross-border safety scenario demonstrates IPv6-based capability to set up communications interconnectivity between different first responder communications systems to assist in an on-site intervention.

Part of the use cases will be based on the interconnection of a local A-ERCS system with other existent national communication systems for emergency response purposes by exposing a predefined IPv6-based InterOperability Point (GEN6 IOP), allowing foreign teams to connect into the on-site emergency response infrastructure, and provide the foreign team with certain communication services that are essential for the execution of the intervention via their own national systems and terminal equipment (e.g., data service, access to registrars, IPv6-based PTT radio service). Automatic IPv6-based provisioning services of the A-ERCS system will be used to automatically activate and provision foreign first responder teams in the A-ERCS.

2.2.2 Architecture

As depicted in Figure 4, the following systems will be interconnected:

- A-ERCS system in the Slovenian GEN6 pilot (ULFE), serving as the local and backhaul national ECS system,
- 6onMOBILE-based sensing solution in use in Slovenia as part of the A-ERCS Node extension (ULFE),
- IPv6-enabled PTT system for first responders, available in Luxembourg (UL),
- 6LowPAN-based environmental sensor deployment in Murcia (UMU),
- Radiation measurement readings available in Luxembourg (UL).

The interconnectivity will make use of the GEN6 IOP interface and will cover two interconnectivity scenarios, as follows.

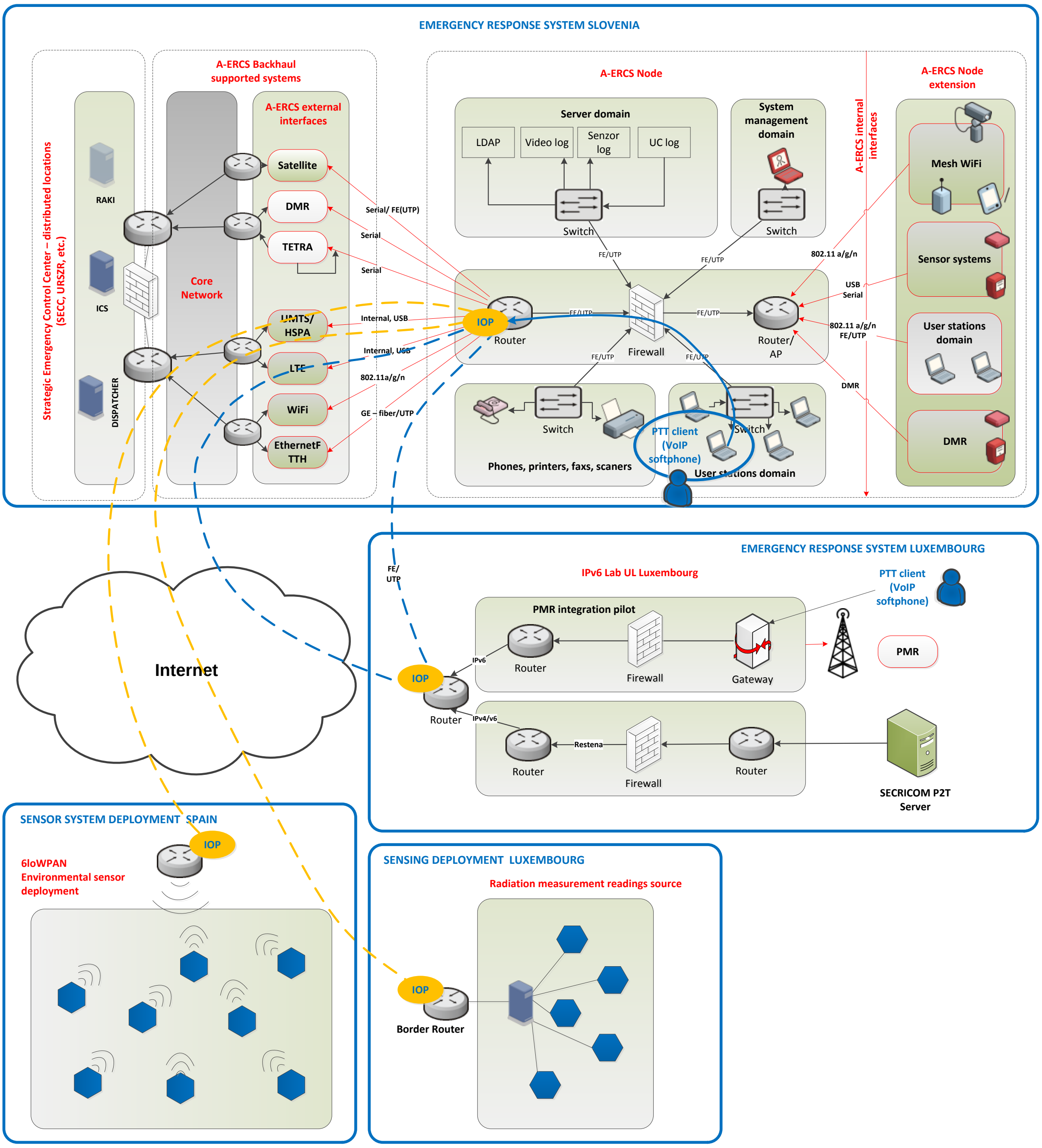

Figure 4: On-site international intervention architecture

The GEN6 D4.1.2 deliverable describes the details of the design.

6LoWPAN sensor integration

The provided solution consists of three parts. The first one is the 6LoWPAN mote: this device is composed by a Jennic JN5148 and a developer board. The developer board contains a set of sensors such as temperature sensor, luminosity sensor and humidity sensor. Furthermore, the Operative System Contiki selected to implement the solution includes 6LoWPAN implementation that allow us an easy fit over the network protocol. The second element is the 6LoWPAN bridge that allow connectivity to IPv6 networks in a transparent mode. Finally the CoAP functionality provided for delivering services to the end nodes based a web based approach for sensor integration.

Mobility Support

In this point we describe briefly the procedures within the mobile nodes for networking & transport layer to allow a mobile nod to maintain continuous IPv6 connectivity while changing its point of attachment to the network. This is ensured by the IPv6 mobility support module within the IPv6 protocol block in ITS stack. The IPv6 mobility support module comprises mechanisms for maintaining IPv6 global addressing, Internet reachability, session connectivity and media-independent handovers (handover between different access technologies) for in-vehicle networks. This module mostly combines Network Mobility Basic Support (NemoBS) and M Multiple Care-of Addresses Registration (MCoA).

2.2.3 Monitoring requirements

The requirements for the monitoring for this cross border pilot can be defined on an abstract level as

- Reachability and therefore availability of all the actors and resources
- Notifications as soon as possible when actors or resources change status from available to unavailable
- Performance parameters of the communication lines (bandwidth, delays, etc.)

The used ITS architecture can be monitored checking the presence of the involved machines and routers and verifying the services provided. The required tools that will allow us monitoring its behaviour and detect malfunctions are the following:

* ping: this tool allow us the detection of the presence of a machine in a network. This will be useful to see if routers and important machines of the network are present and working well. But sometimes is not enough. We need to verify if the services that are running in them are working successfully as well. Ping cannot do this. See next points to see how to address it.

* ps: this tool can detect the presence of an application running in a machine. It cannot be run remotely but we can use the SSH tool that allow us running any command remotely. This tool is important to assure that a determined service is present. For the case of mobility service, we only need to test if the daemon called "mip6d" is launched and running inside the Home Agent, that is the machine in charge of deploying this service. But again, this is not enough to see if a service is working well. We need more specific tool. Follow to the next point to see an example.

* telnet: this tool enable us to interact with the monitorized service in a very basic way. For example, to see if a service is active in a determined port. In the case of a web server, we can test the port 80. In the mobility case, the "mip6d" daemon has a open port (7777) we can connect to interact with the daemon and see the internal status of the mobility. For example, we can see an snapshot of the binding cache table. These cache entries associates HoAs with CoAs. In this way we can obtain further information about a service, but the way to do this will be different, depending of the service in question.

* tcpdump: this tool goes further in the detection of a service, looking for the messages produced by the daemons. In case of mobility, the presence of "router advertisements" in the network is vital for mobility, because the Mobile Nodes or Mobile Routers have to be a way of detecting the presence of new Access Routers.

All this tools can be launched and controlled with scripting languages like for example "bash" in linux. Also "perl" language can be used to analyze network captures produced by tcpdump, and summarize its output.

3. Tools

For the operation monitoring of the pilots a basic infrastructure is established, that is unique for all pilots. For this purpose standard tools are established. The tools and their operational embedding are described in this chapter.

To get use of the results of the tools all project partner need access to dashboards. Therefore the system must be available in the internet. To satisfy the internal check requirements the systems are localized in the internal network of the Citkomm infrastructure and access is granted only via a certificate based authentication.

In the case of Citkomm and MINHAP, since they have already their own network management systems, the intended approach is integrating with the monitoring platform of the pilot by means of these systems, instead of having the monitored elements sending information directly to the pilots monitoring platform. Event Monitoring

3.1 Event Monitoring

The event monitoring aims to the ongoing inspection of all involved systems on availability of specific services or off-limit conditions for regular operation. For this purpose the event monitoring only covers those aspects that are crucial for the current operation.

As module for this pilot monitoring the open source suite Icinga has been chosen. Icinga is well known by most operators. Furthermore Icinga offers a wide number of pre-defined checks that can be used out of the box but also can be modified due to specific requirements.

The GEN6 Icinga probe must monitor the components off different pilots. Due to the structure of the pilots they operate in different networks. The components of the “IPv6 safety” pilot are connected directly to the Internet. Several components for the “IPv6-readiness for cross-border services” pilot on the other hand are operated in closed networks like S-TESTA, DOI or Red-SARA. For this reason the event monitoring needs connections to the Internet as well as into the involved closed networks.

Icinga supports different kinds of checks. There are passive checks, which are performed from a monitoring server connecting to a system to be checked. Those checks are connections like ping, ssh, LDAP, http etc. The check is successful, when the called service is online. As a further information point the reaction time may be used for analysis on being off-limit. Possible monitoring with passive checks is limited. To get a more inside view of a system two common ways are available. The first one is the use of system information accessible via SNMP. So all the in MIB defined parameter can be monitored. For open operating systems furthermore so called active checks are available. In this case an Icinga probe software is installed on the monitored server. On demand of the Icinga server this software module starts an operation system specific check on the system itself, pick out the relevant information out of the results and transfer them to the requesting Icinga server.

However, as it has been mentioned before, in the case of Citkomm and MINHAP, the intended approach is not based on the sending of SNMP messages to Icinga, or the installation of Icinga probe SW on the monitored elements. Event monitoring integration would be achieved by using existing monitoring systems, so all the relevant information are collected with the existing infrastructure of SNMP and SW probes management

3.2 Trend Monitoring

As part of the event monitoring off-limit analyses are established for relevant data points. But still before getting off-limit it may be useful to know about the development of a data point over a given period. This is common known as trend analyses. The results may help to identify potential weak points in the infrastructure, as long you can see that a specific data points tends to get continuously out of its long time bandwidth or closer to a known limit.

Trend analyses are sometimes on the same data points that are objects for the event monitoring. But in other cases only the trend of a data point is relevant, because there is no adequate action that could be performed to act against the situation. Furthermore trend analyses handle with huge date volume for long time trend analyses, the response time of the processing of those analyses is in common not production critical. Form event monitoring systems on the other user expect immediate reaction, if a critical state is detected. To avoid potential conflict of these different purposes the monitoring systems are divided into an event monitoring and a separated trend monitoring.

For the trend monitoring the open source tool “Munin” is used. Munin can get system information via standard interfaces like SNMP or via an own client, that is especially for server installation useful.

3.3 Ticket System

To manage events and enable a clear communication for problems in the WP4 pilots a ticket system will be set up. As infrastructure the well known OTRS has been chosen, which is still in use at some partners. All partners operating infrastructure in the pilot will be owner of own ticket handling groups, to get information about potential problems in their production area. In combination with the integrated information and escalations mails the handling of those events will be structured and monitored, especially if several partners are involved. Furthermore via the tickets a statistic on occurrence number and frequency can be generated.