



Title:	Document Version:
Deliverable D3.6.4 – e-Government Specific Services with IPv6	1.0

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

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/05/2014	29/07/2014	R – CO

* 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:	Organization:	Contributing WP:
Emre Yüce	ULAKBIM	WP3

Authors (organisations):

Emre Yuce (ULAKBIM), Onur Bektas (ULAKBIM), Carsten Schmoll (Fraunhofer), Juan José Rodríguez Moreno (MINETUR), Gabriela Gheorghe (UL).

Abstract:

This document is the fourth one in a series of deliverables documenting the progress of the three national pilot projects located in Germany, Spain and Turkey. Their goal is the transition of selected, public sector services from IPv4 to IPv6 operation. Additionally progress of the Luxembourg pilot is presented.

Keywords:

IPv6, e-Government, IPv6-enabled services, Public Sector, specific services

Revision History

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

Revision	Date	Description	Author (Organization)
v0.1	17.04.2014	Document creation	Emre Yüce (ULAKBIM)
v0.2	29.05.2014	Addition of Fraunhofer contribution, general enhancements.	Emre Yüce (ULAKBIM)
v0.3	04.07.2014	Turkish pilot contribution	Emre Yüce (ULAKBIM)
v0.4	15.07.2014	Spanish and Luxembourg pilot contributions added.	Emre Yüce (ULAKBIM)
v0.5	27.07.2014	Review	Carsten Schmoll (Fraunhofer)
v1.0	29.07.2014	Finalization and Delivery	Uwe Kaiser (Fraunhofer)

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-ND 3.0) licence. Consequently, you are 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-project.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 information 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 of risk, and so do not accept liability for loss or damage suffered by any person using this information.

Executive Summary

The national pilots of the GEN6 project in Germany, Spain, and Turkey show significant similarities, and they are grouped under the “IPv6 upgrade of e-Government Network Infrastructures, e-Identification, Services and Applications” topic. The efforts of these three pilots are expected to reveal common as well as different aspects of IPv6 transition, taking into account the different approaches to IPv6 transition in these pilots.

This deliverable differs from D3.6.1, D3.6.2 and D3.6.3 by investigating pilot specific services in each pilot separately. Hence one may observe the detailed IPv6 transition process of a pilot specific service. In this context each pilot has been asked if the pilot contains a pilot specific service such as custom written scripts or custom developed gateways (e.g. VPN, AAA) or special hardware like SMS gateways or NAS devices. Additionally this document is presenting the current status of the Luxembourg pilot focusing on the specific services within the pilot.

This deliverable is the fourth snapshot of a living document. It focuses on pilot specific service elements. The series of deliverables (D3.6.x) will be grouped under the D3.6 document which will be showing commonalities and differences of the pilots so that it becomes more useful for a government audience. GEN6 documents can be taken as a starting point to introduce IPv6 based services on the best practises of various documented pilots.

Table of Contents

1	Introduction.....	7
2	German Pilot.....	8
2.1	IPv6-Testbed	8
2.1.1	Basic Use Cases.....	9
2.1.2	Basic Approach	10
2.2	Test Setup	10
2.2.1	Adapted Use Cases	10
2.2.2	Approach	11
2.2.3	Application scenarios	11
2.2.4	Management Interface	12
2.2.5	Configuration of security policies.....	12
2.3	Results.....	12
2.3.1	Management Interface	13
2.3.2	Configuration of (Security) Policies	13
2.4	Evaluation of the Results	13
3	Spanish Pilot	15
3.1	eITV application description	15
3.2	eITV application users.....	17
3.3	Infrastructure and software used by eITV	19
3.4	Security policies	20

3.5	Evaluation of the Results	21
4	Turkish Pilot.....	22
4.1	Certification	22
4.2	Logging.....	22
4.3	Testbed	23
4.4	Public Integration Box	23
5	Luxembourg Pilot	24
5.1	Description of the service.....	24
5.2	Transition to IPv6.....	26
5.3	Monitoring considerations	27
6	Conclusions.....	33
7	Figure Index.....	34
8	Table Index	Fehler! Textmarke nicht definiert.

1 INTRODUCTION

This document is the fourth one in a series of deliverables documenting the progress of three national pilot projects which are focused on transition of selected e-Government services to IPv6 within GEN6 project. These three pilots are being carried out by German, Spanish and Turkish GEN6 consortium members.

Unlike the previous versions of the deliverables, this one will be investigating pilot specific services. At the preparation phase of this deliverable, the pilot participants were asked to find out the specific services for their own pilots such as custom scripts or custom developed gateways (e.g. VPN, AAA), or special hardware like SMS gateways or NAS devices. Then participants shared their experience which they had gained through the IPv6 transition of these services. Since this kind of experience is to be pilot-specific, the content of this deliverable has been separated in different sections, one per pilot. Additionally to the documentation of specific services, the current status of the Luxembourg pilot has been presented.

Finally, the conclusion section summarizes the topics identified in the document.

2 GERMAN PILOT

2.1 IPv6-Testbed

The testbed of Fraunhofer FOKUS allows testing of infrastructure devices in an IPv4-only, dual-stack and IPv6-only environment. The main goal of the performed tests lies in realistic end-to-end test scenarios.

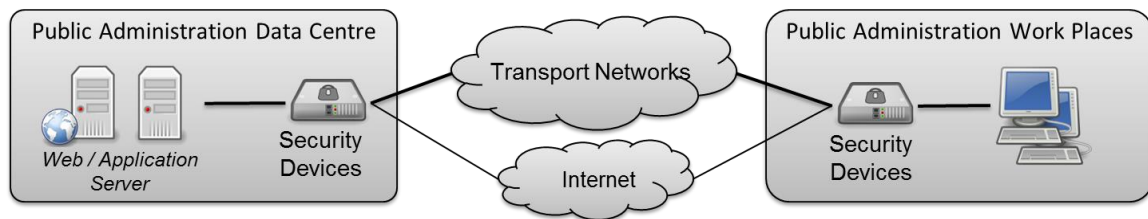


Figure 1 Reference Architecture

The locally used testbed adheres to our reference architecture that is used to provide an environment similar to the ones used by public administrations in the field. In the practice of the testbed this includes not only the network structure and network elements but also typical end systems and installed software. This is shown in the following Figure 2.

Based on the performed application scenarios, one side of the setup will “play” the role of a public administration while the other side will play the “remote data center” role. In this data center we run the domain-specific applications that are accessed by the administration’s desktop computers. In this setup, we can realistically evaluate hardware appliances as well as software applications in IPv4-only, IPv6-only and dual-stack environments.

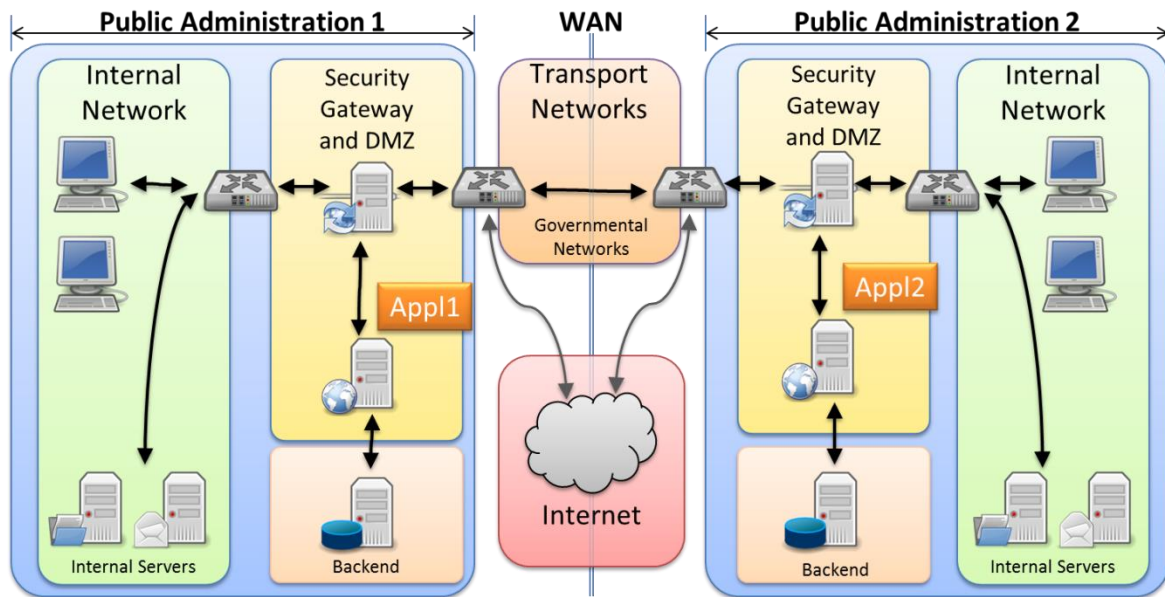


Figure 2 Reference Architecture

2.1.1 Basic Use Cases

In our test environment we systematically performed the analysis of different communication patterns, depending on the device type, as there are:

- Inside to outside
 - Connecting from workplace systems to the Internet
- Outside to inside
 - Connecting from external clients to internal services (e.g. servers in the DMZ)
- Network Services
 - Communication to network infrastructure services (e.g. DNS)
- Management interfaces
 - Administrative access for configuration and management of devices
- Configuration of (Security-)Policies
 - Adaptation of existing policies and/or creation of new policies

2.1.2 Basic Approach

Our tests of hardware and software have been typically split into the following phases:

- Configuration IPv4-only
 - Where the starting point is the currently existing configuration
- Partial migration to IPv6
 - Migration of parts the network infrastructure; e.g. with IPv6 connections over IPv4-VPN-Tunnels
- Dual-Stack operation
 - Using IPv4 plus IPv6 across the whole network infrastructure as far as possible; with the mix of applications also using IPv4 and IPv6 in parallel in the network
- IPv6-only
 - Using no IPv4 traffic whatsoever in the network infrastructure

2.2 Test Setup

2.2.1 Adapted Use Cases

This work performs an analysis of application-relevant communication aspects, also tailored to the specific device type under test (where the device in our case is a special „VPN-box“ used by German administrations for secure LAN-to-LAN tunnels). This work consisted of:

- Installation and Base configuration of the VPN system via its management interface
 - Including network services such as LDAP and NTP
- VPN system management: Configuration of security relations between local and remote subnets
 - Including adaptation of existing policies or adding new policies (management permissions, filter rules, group policies) to reflect the current policies on IPv6
- Connectivity tests across the configured VPN

2.2.2 Approach

The following steps were taken while integrating the VPN systems into the FOKUS IPv6 testbed:

1. IPv4-only configuration

Configuration of IPv4 addresses and communication relationships between IPv4 networks plus integration of VPN systems into the testbed

2. Dual-Stack operation

All active network interfaces and services (as far as possible) inside the testbed network are activated with IPv6 in addition to the above IPv4 configuration

3. IPv6-only configuration

Disabling of IPv4 on all testbed components (hardware and software)

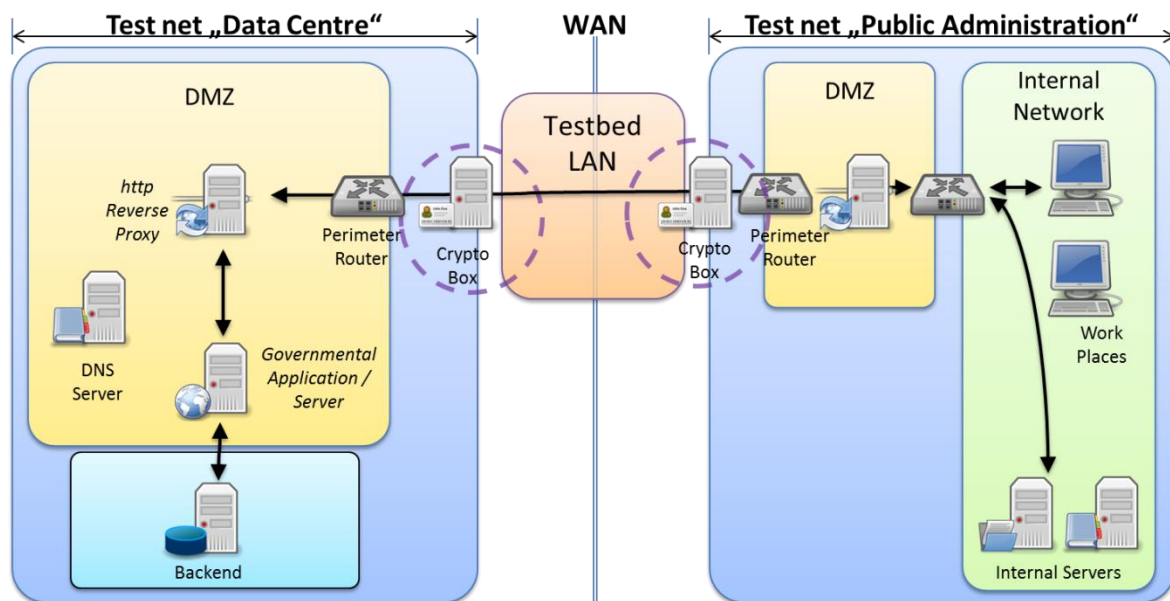


Figure 3 Logical view of VPN systems and their management inside the FOKUS IPv6 testbed

2.2.3 Application scenarios

The following application scenarios were tested after each phase of configuration (see previous section). The focus of the testing is on the typical use of these VPN solutions with the German public administration's LAN-to-LAN VPN coupling.

The goal of the tests is running secure connections from one premise to another (remote one), across possibly insecure networks. The VPN system connects a LAN subnet on one side to another LAN subnet on the other side (contrary to e.g. VPN-secured dial-in connections). Therefore the main focus of our tests lies on the connectivity between these subnets, as well as application connectivity and performance between clients on one side and servers on the other side, across the encrypted VPN connection (using IPsec in tunnel mode). The allowed connections were guarded by the configuration of the security policies on the VPN systems on both ends of the secured connection. In these tests we did not check connectivity to or from the Internet, only government to government (G2G) use cases.

2.2.4 Management Interface

The VPN system is configured only by using its own management software. This software has been installed in our testbed on a dedicated virtual PC (with IPv6 support). As part of the setup process, the used smart cards have been enabled by writing the target configuration on them. Those smart cards are the secure way of transferring the final configuration to the VPN systems. When booted with the correct configuration on the smart cards, the VPN systems could be enabled with online management functionality, which then allows for remote management using the VPN system's console.

2.2.5 Configuration of security policies

During the configuration and test of the different application scenarios, we also checked the usability of the management interface with regards to IPv4 versus IPv6 configuration. This means checking whether IPv6 rules will be added automatically, or a place-holder will be generated (and values asked from the operator) in the case of dual stack operation, or if IPv6 rules have to be added manually later on, after the configuration of the IPv4 rules.

2.3 Results

The results will be described in the following text, based on the different application scenarios. Since we are not going to describe in detail the concrete VPN system here from a specific manufacturer, these results should be viewed by the reader as a set of best-practices and what-to-take-care-of findings to be taken into account in general when running VPN systems' setup in an IPv4 plus IPv6 environment.

Note: To be sure whether IPv4 or IPv6 connections were used in our tests (e.g. by a web browser

application), we have used only literal IP addresses (IPv4 and IPv6) instead of host names.

2.3.1 Management Interface

Initially, the VPN system's management software had been installed inside a virtual Linux machine in the FOKUS IPv6 testbed. During installation it needs to be made sure that the machine's operating system, network configuration and the management application for the VPN system are IPv6-aware. Check with the manufacturer whether this is already the case (and just needs to be configured), or a newer version of the VPN system's management software is needed. With our system we noted that the documentation for the management software did not cover IPv6 configuration in a way that was fully consistent with the real software. So, some practical probing of the effective features of software for IPv6 configuration is always recommended, before recommending it to others. To our experience, the actual software is usually ahead of its documentation, i.e. can do more than is documented.

However, in our concrete case we could not setup a dual-stack configuration of the management interface using the graphical management software – if only because of the fact that only one IP-Address (IPv4 or IPv6) could be given in the configuration menu. If the management interface of the VPN system is indeed dual-stack reachable then the actual upload of configurations tries connecting via IPv6 first and then (if IPv6 fails) via IPv4.

2.3.2 Configuration of (Security) Policies

For configuring security policies (and security associations between coupled subnets) we also tried a partial migration, i.e. coupling networks with IPv6 traffic across IPv4 networks (IPv6 in IPv4 packets), and vice versa (IPv4 over IPv6 networks). In our experience this works quite as expected, in both cases. We only noticed that the user interface one could also try to couple an IPv4 subnet with an IPv6 subnet, which will not work due to the incompatibility of the IP protocols. Only when the configuration of all coupled networks was set to final, the user interface would issue an error message. Sometimes, also the default selection of a subnet on the other side of a VPN tunnel was suggesting a network of the wrong IP type. This could be fixed easily during the configuration, but could be avoided by the user interface in the first place.

2.4 Evaluation of the Results

The used VPN system's tunnelling functionality has been proven capable for IPv4-only, IPv6-only and dual-stack operation mode in our tests in the FOKUS testbed.

Yet, all its functions are configured over its proprietary management software – and this software (not the VPN box itself) showed some drawbacks, mainly related to dual-stack configurations, e.g. the fact that management server could not be configured over the user interface with IPv4 and IPv6 addresses. Secondly, the automatic selection for IP subnets on the remote side would always default to selecting an IPv4 subnet, even in the local subnet was an IPv6-only network.

Finally, the installation process of the management software was somewhat tricky, due to somewhat dated installation documentation. When running such systems one should always contact the manufacturer and ask (or download) the very latest documentation for it, since the (possibly printed) documentation that is delivered together with the system may not yet reflect all the features of the system with regards to IPv6, especially when the IPv6 support in the system is much “younger” than the IPv4 support, as it is the case with most systems (to our experience).

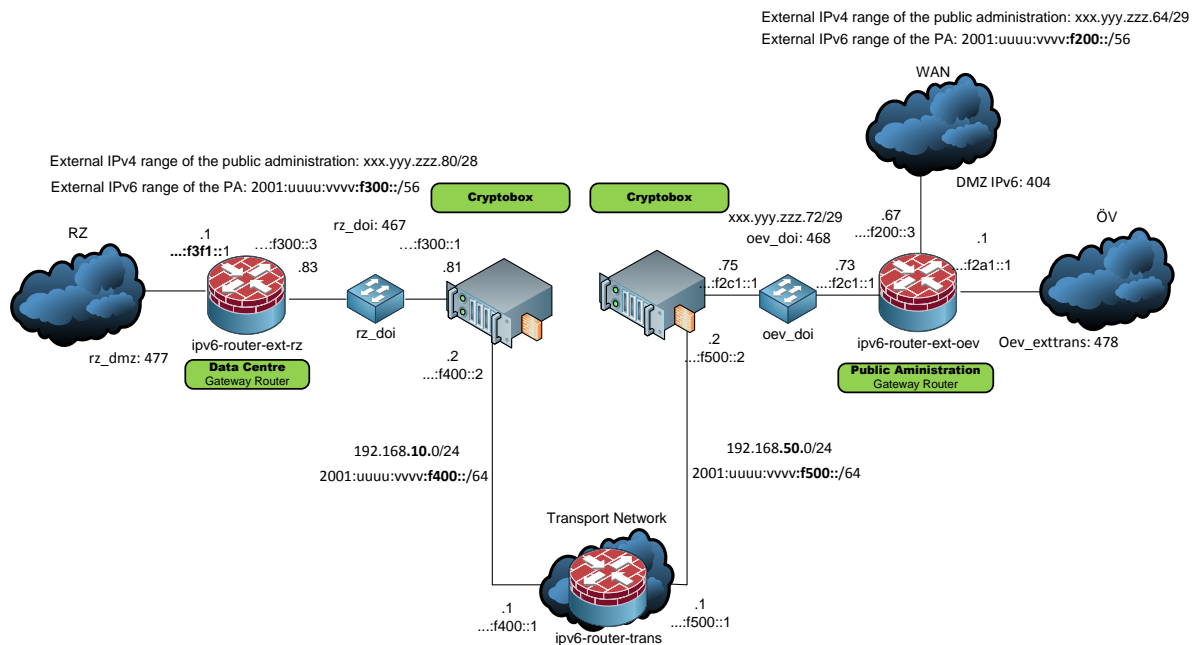


Figure 4 Setup with two testbeds connected via encrypted VPN connection

3 SPANISH PILOT

One of the purposes of the Spanish pilot is the use of IPv6 connections between different government departments. All these departments communicate with each other through a network called RedSara (SARA Network), which has been updated to transport IPv6 natively.

In this pilot, as a demonstration of enabling IPv6 eGovernment services between different government units, eITV application, related to the registration of a motor vehicle, has been selected. The Ministry of Industry, Energy and Tourism (MINETUR) provides eITV application to another administrative unit of another ministry, the DGT (Directorate General for Traffic) as well as vehicle manufacturers.

3.1 eITV application description

eITV replaces the traditional paper-based ITV card (Vehicle Technical Inspection card) by an electronic card and all face-to-face procedures required for registering a motor vehicle by electronic procedures.

The eITV application consists of the management of eITV cards made by the Ministry of Industry, Energy and Tourism. The Ministry provides the necessary tools to vehicle manufacturers and DGT for the request and query of the eITV cards.

It is a web application with public and private part and a web service for data exchange that uses digital signatures to ensure authentication, integrity and non-repudiation. The information sent is stored in electronic records.

The necessary steps are:

- ITV electronic cards are requested and created.
- The Ministry authorization process is fully electronic.
- The eITV card is electronically sent to all stakeholders (Ministry, DGT, vehicle manufacturers, etc.)
- The electronic matriculation procedure includes the acquisition by manufacturers of electronic cards issued by the Ministry. These cards are filled with information of the vehicle by the manufacturer and send to MINETUR and DGT for further registration.

- The matriculation process by the DGT is fully electronic.

The flow of data exchanged for the registration of a vehicle is as follows:

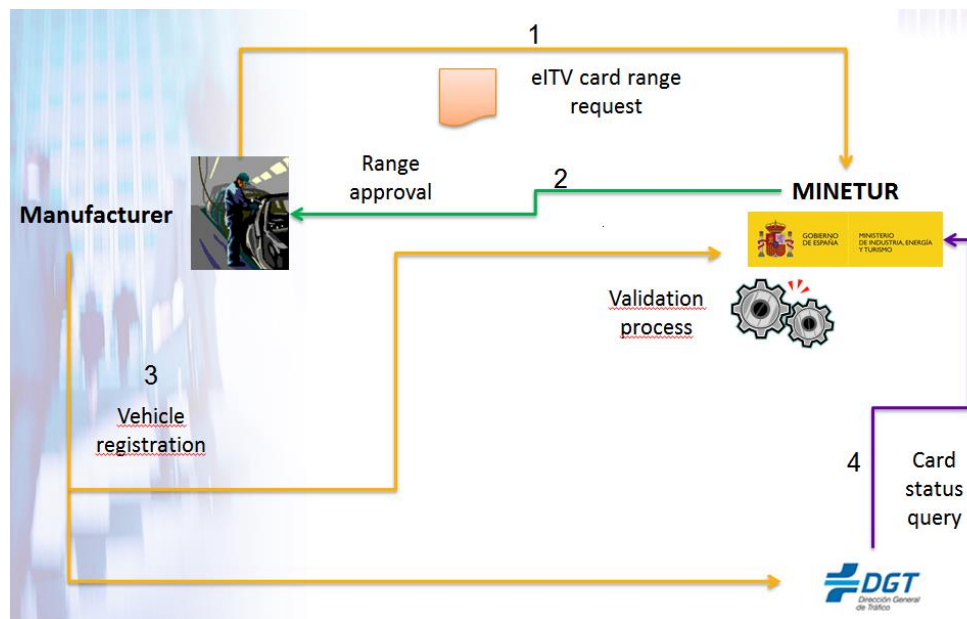


Figure 5 eITV application data flow

1. eITV card range request. Manufacturers ask MINETUR for eITV cards ranges.
2. MINETUR grants eITV cards ranges.
3. eITV cards are filled by manufacturers with vehicle information and data are sent to MINETUR and DGT simultaneously.
4. Both MINETUR and DGT check the cards sent. For that reason, DGT will query the MINETUR data.

As a result of the fully electronic procedure, the following benefits occur:

- Saving time and money in the process of registration.
- Safety in the transmission of the data (errors and fraud are avoided).
- Quality of data stored for query and reference.

3.2 eITV application users

You can access the application in two ways: through the classic user / password system and using digital certificate as shown in the following screen:

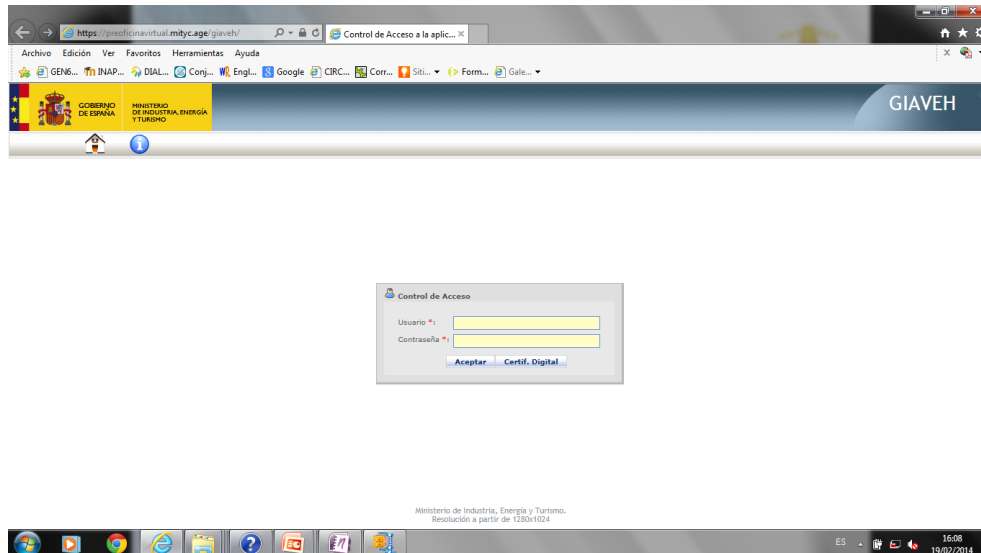


Figure 6 eITV access screen

Once inside, the processes are different for each type of user:

- External users (vehicle manufacturers) may request eITV cards, check the status of cards requested and send data with information of the vehicles for registration to MINETUR and DGT.

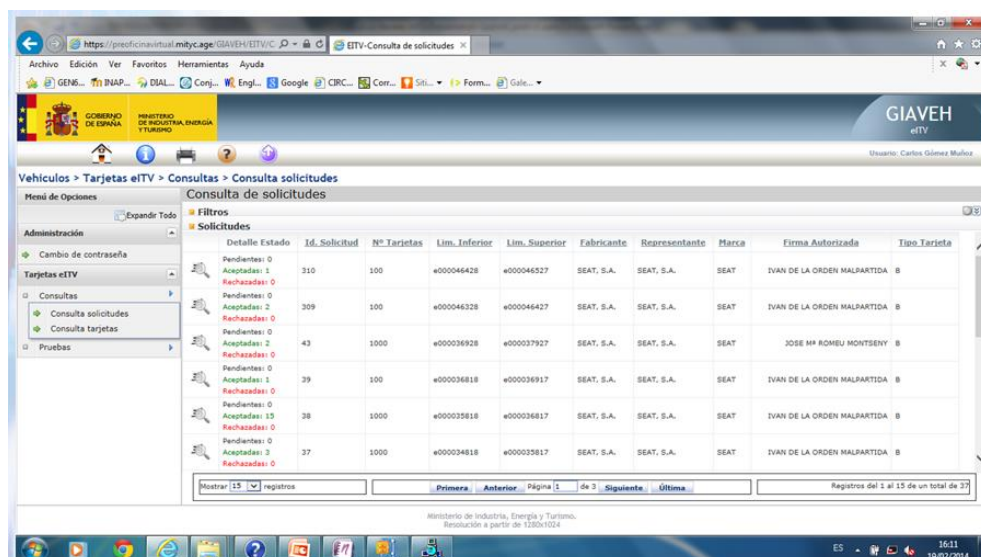


Figure 7 eITV card range query

- Internal users (MINETUR) will access management options and application control as well as validation of electronic cards requested by the manufacturers.

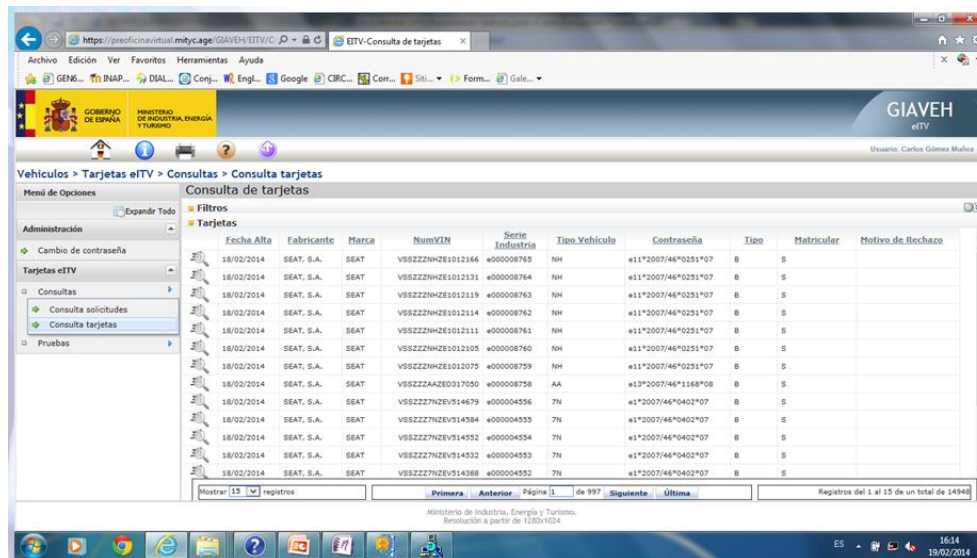


Figure 8 eITV card authorization query

- Government users (DGT) can check the status and data of the electronic cards sent by the manufacturers.

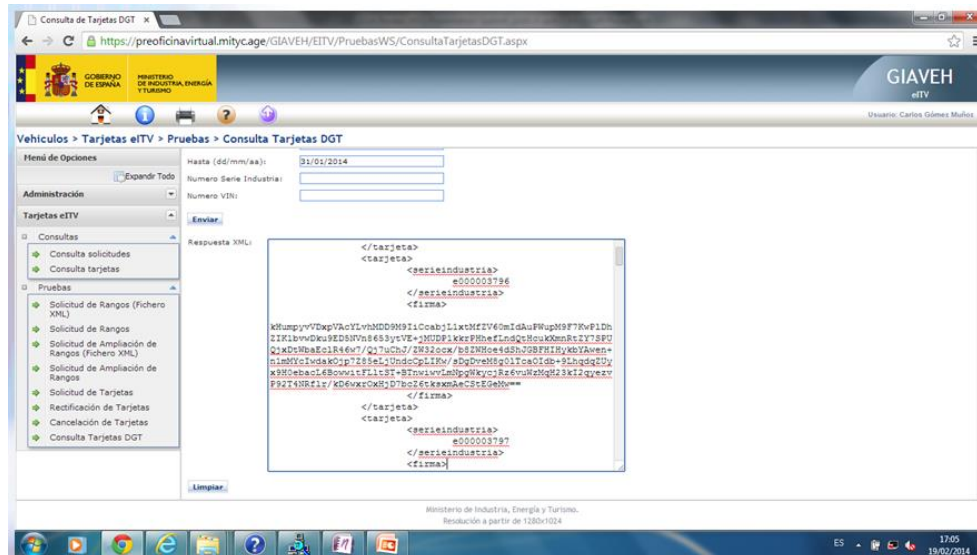


Figure 9 eITV card status query for DGT

The following figure shows where the different types of users are located within the scheme of the infrastructure required by the application and the different protocols used by each of them

to access the system.

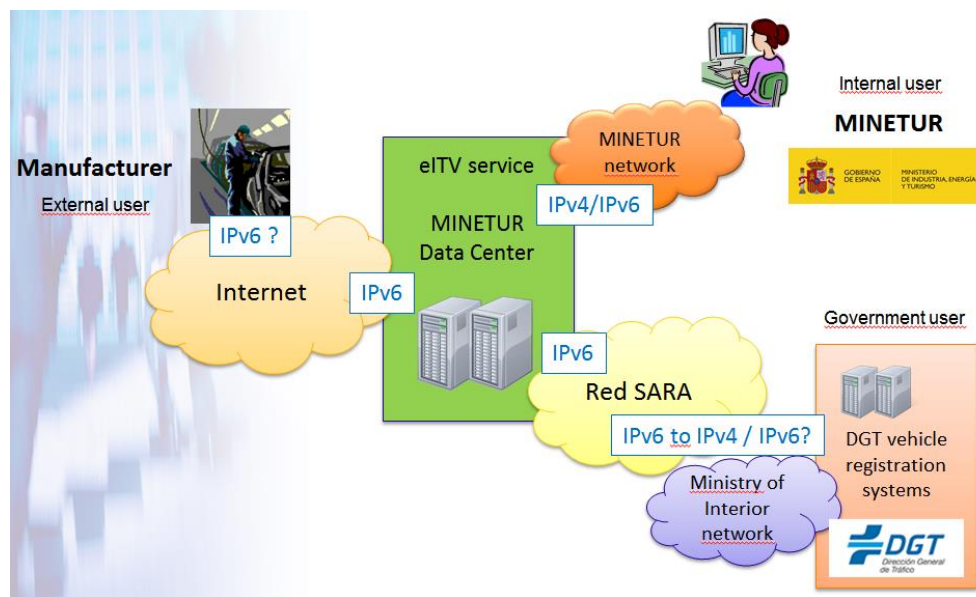


Figure 10 Users and protocols used

As seen in the figure, we have no certainty whether the manufacturers are going to use IPv6 protocol or not. It is not in our hands but we are having contacts so that they use this protocol.

Regarding the internal users, our internal network is IPv4. The users are able to access eITV using IPv6 only from specific subnets on our data centre or by means of a portable computer configured with IPv6 and connected through our Wi-Fi connection that is able to serve IPv6 addresses with DHCPv6.

Concerning the DGT users, this department belongs to another Ministry and the data must pass through a network where IPv6 is not implemented. We are in contact in order to use IPv6 end-to-end.

3.3 Infrastructure and software used by eITV

The general outline of the infrastructure used by the eITV application is:

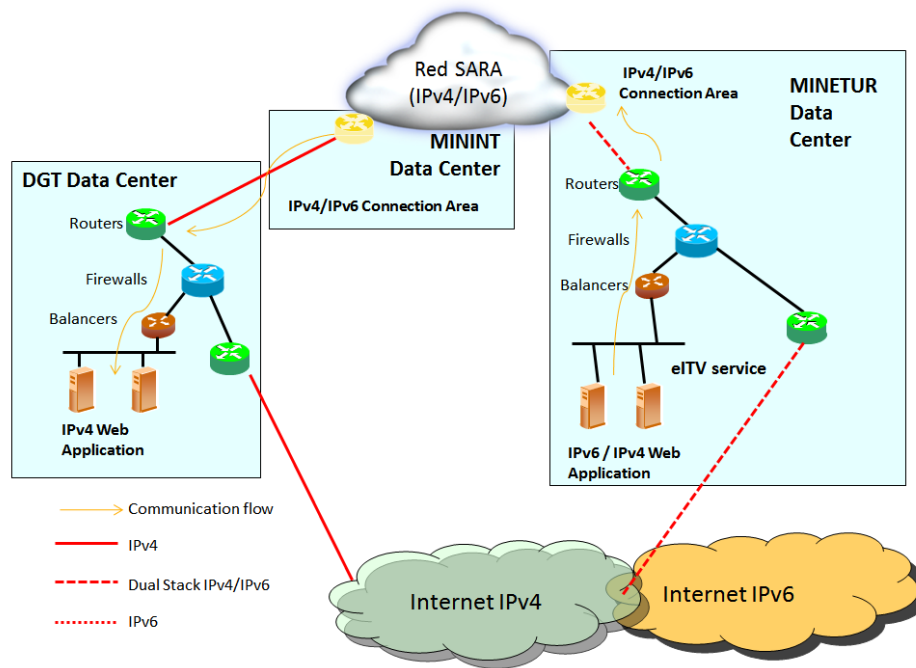


Figure 11 Reference architecture

As we can see in the figure, the communication between the Data centre of DGT and MINETUR will use the connecting areas between ministries that SARA Network provides.

The connections from the Internet will be made by vehicle manufacturers to communicate with MINETUR and DGT.

eITV is a web application with a web service for data exchange. It uses .NET Framework 4.0 and the database is Oracle 11.6. The servers are Windows 2008 64bit with IIS 5.0.

3.4 Security policies

Our security policies relays mainly in our firewall. Firewall rules have been added to allow only IPv6 traffic through HTTP and HTTPS to the eITV service.

We have taken advantage of the IDS capabilities of the firewall as well as the malware and antivirus detection. We are using these capabilities to block threats although no specific changes have been made for IPv6. The firewall logs are also analysed and correlated to detect threats and attacks.

The use of digital certificates when data is exchanged between different users of the application guarantees the integrity and security of data.

3.5 Evaluation of the Results

No problem with commercial products needed to implement eITV application. They all are adapted to IPv6.

Initially, eITV application was developed for an IPv4 environment. Therefore, the migration to an IPv6 environment has required the review and adaptation of the source code.

The problems have been similar to those of IPv4. The difficulties found have not been too great since some basic considerations have been taken into account as the exclusion of IPv4 addresses in the program code and the use of stable identifiers to connect to other nodes (host names resolved by DNS).

4 TURKISH PILOT

The Turkish eGovernment Gateway (EGG) is composed of a web portal which is serving approximately 1000 services to more than 18 million citizens and the backend connections to the respective governmental institutions. Hence, the Turkish pilot consists of two main phases. The first phase of the Turkish pilot includes the IPv6 transition of EGG portal which is the frontend of EGG. This phase has been successfully completed through the first year of the project. The second phase of the project is to make the backend communication between TURKSAT and the selected service provider governmental institutions IPv6-enabled.

The Turkish EGG is designed to serve millions of users via high available architecture. This brings many different challenges and complexity to be managed so usage of industry standard equipment and software is important. Hence, vendor produced and licensed applications are preferred rather than in-house produced scripts and applications which will be programmer dependent.

4.1 Certification

One of the main components of the Turkish pilot is the EGG web portal which should comply with standards defined for W3C Web Content Accessibility Guidelines and Ergonomics of human-system interaction. For this purpose TURKSAT has applied for the following standards and Turkish EGG web portal has been approved for satisfying the appropriate standards.

- ISO 9241-151:2008 Ergonomics of human-system interaction – Part 151: Guidance on World Wide Web user interfaces
- ISO/IEC 40500:2012 Information technology -- W3C Web Content Accessibility Guidelines (WCAG) 2.0

Tests have been carried out by Human-Computer Interaction Research and Application Laboratory (<http://hci.cc.metu.edu.tr/>) in Middle East Technical University, which is one of the leading universities of Turkey. Through accessibility tests, communication over IPv6 has been tested and the results were successful.

4.2 Logging

In the EGG, logging is one of the building blocks in order to keep the system secure, manageable and accountable. Enabling IPv6 on services and portal caused the upgrade of commercial logging

server solution to support IPv6. Throughout the Turkish pilot, security configurations have been updated to support IPv6 as well. In general these configurations include firewall rules or access control lists. Specifically for Turkish pilot, user access logs are kept for forensics purposes. Through work in the Turkish pilot, these logs have been IPv6-enabled. Some self-developed web scripts were patched to support IPv6, such as the script that shows the users the last three IP addresses for login on the web page.

4.3 Testbed

As the Turkish EGG has a complex structure, it is difficult to make a testbed to represent all the operations taking place. Besides, as most of the institutions do not have a test service that TURKSAT test service can interact, simulating communications between TURKSAT and remote institutions and setting up a production level testbed for EGG is not feasible. However TURKSAT has setup a local testbed where tests have been launched for new applications, software and hardware.

4.4 Public Integration Box

On the backend of the Turkish pilot there exist VPN connections between TURKSAT and the remote institutions. In order to decrease the setup effort, TURKSAT has developed a plug-and-play hardware which enables VPN tunnels (both IPv4 and IPv6) between end points. These boxes (called Public Integration Boxes) have been deployed in the remote sites throughout Turkish pilot. During the development progress, the box was designed to be IPv6 enabled.

5 LUXEMBOURG PILOT

5.1 Description of the service

UL has developed a pilot together with Citkomm in order to support local elections in Germany. This pilot is the first of its kind to combine cloud computing and IPv6, and moreover to integrate a cloud deployment into a production infrastructure in order to serve peak traffic. It has successfully managed to serve IPv6 traffic on the first election round on May 25th: 5% of the total traffic was over IPv6 and it passed through the IPv6-only cloud servers at UL during the initial election day. The same setup was used in a second election round on June 15th 2014, and it served up to 2% of the total traffic.

The service that is supported by the pilot is the election website presentation. Throughout the election days, citizens of various municipalities in North-Rhine-Westfalia (NRW) could access the current voting count on a Citkomm-hosted website (<http://wahlen.citkomm.de/>). The backend web server for this website has traditionally been IPv4-only, and with this pilot the intention was to showcase two novelties at the same time:

- IPv6 enablement of website needed especially by those citizens accessing it from mobile devices that have IPv6 connections.
- Cloud computing assurance (availability, resilience and scalability) when it comes to handling large amounts of user traffic.

In terms of the implementation, this pilot featured several elements:

- The use of the OpenStack “Havana” open-source cloud computing distribution that was fully adapted to support IPv6. Note here that IPv6 support in this software is not yet an officially advertised feature.
- Intensive testing phase that included heavy load generation.
- QoS monitoring during test and production phase, complemented by extensive data collection of different kinds:
 - User-level data elicited from monitoring web site performance from various locations in Europe and abroad.
 - Hypervisor data, elicited from monitoring the way the hosting cloud platform

reacts to increasing loads on the resources allotted to the application running on top of it.

- Hardware data, elicited from monitoring the load of the bare metal resources hosting the cloud operating system that in its turn hosts the high-level application.

The architecture of the testbed is shown in Figure 12. The lower part of the diagram shows the cloud infrastructure as a private virtual network hosting several Ubuntu virtual machines (VMs), of which two are Citkomm's website servers. These two VMs have IPv6 addresses and are hence reachable from the outside, and can be configured from within the Citkomm backend network. The middle part of the diagram shows the physical servers at UL that host the virtual network in the cloud, and their connection with the outside world via dual IPv4-IPv6 connectivity.

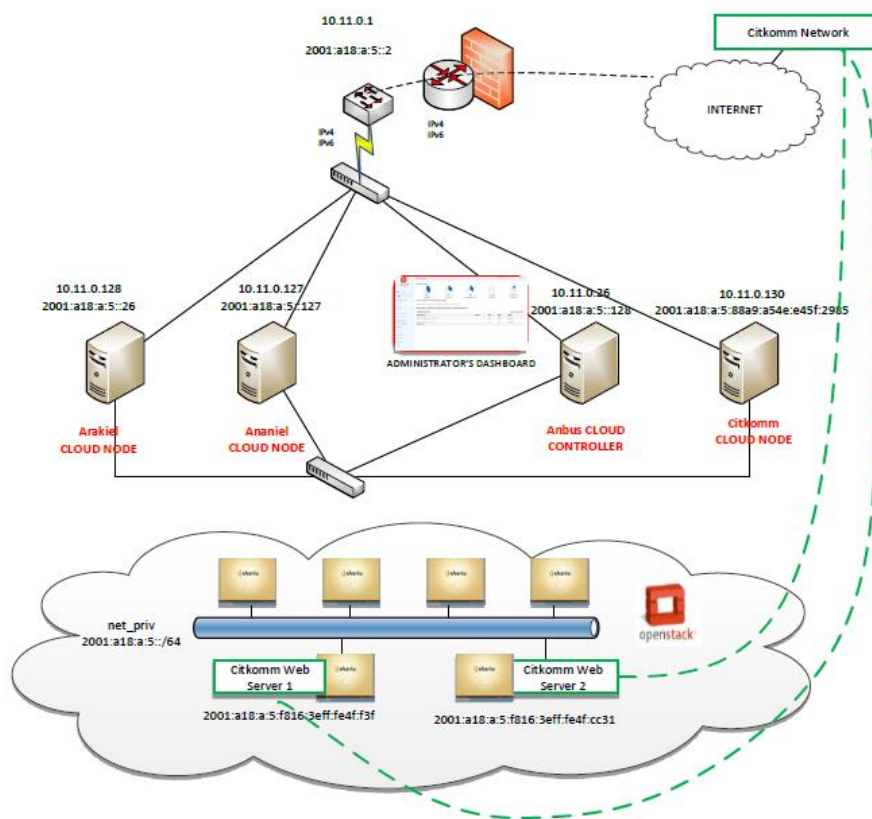


Figure 12 Reference architecture for UL-Citkomm pilot

In Figure 13 we can see the integration of the two sites – one in Germany (QSC) and the other one in Luxembourg – within the same infrastructure used in the election presentation. As mentioned before, the Luxembourg infrastructure was IPv6 only, and it was fully integrated in

the DNS entry with a central URL (wahlen.citkomm.de) for all servers. All citizens accessing this URL via IPv6 were directed to the Luxembourg servers, while all the others, to the QSC site.

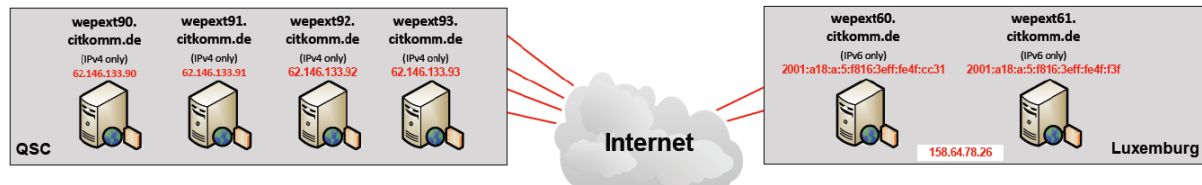


Figure 13 Integration of the machines in Luxembourg and Germany in the same testbed

The two main pilot objectives – to enable existing e-government services with IPv6, and to handle peak loads on existing applications with the support of cloud computing – have been achieved so far.

5.2 Transition to IPv6

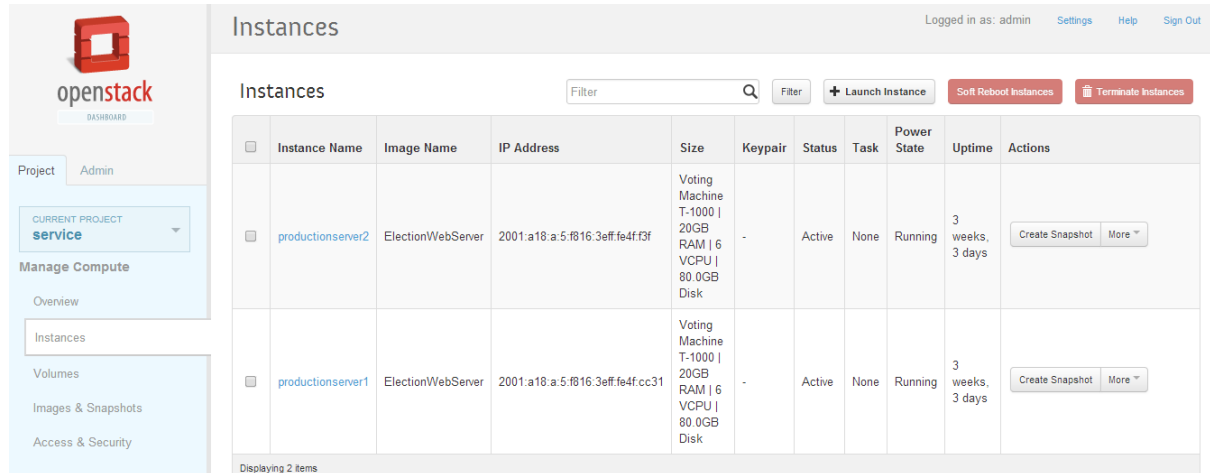
There are clear advantages of cloud infrastructures on IPv6. The addressing space being large, there is more room for addressability of resources in the cloud. Virtual networks and resources can be managed easier, because they can be added, removed, or changed easily.

As mentioned earlier, the integration of IPv6 in OpenStack is not yet officially achieved in the open-source community. At UL, the OpenStack Havana testbed has been patched for full IPv6 support with the help from Nephos6, a company in the US. All details of the patch can be found in a previously published whitepaper¹, while here we only give a few pointers on the biggest shortcomings that were addressed by the patch:

- Router advertisements were not being sent properly between routers and virtual networks, and consequently traffic from virtual networks would not reach IPv6 routers but rather OpenStack's DHCP servers.
- Duplicate address detection had to be turned off at interface level, to bridge a potential kernel bug generating "IPv6 duplicate address detected" messages in the VMs running Ubuntu 13.10 / 64 bits.
- Generation of SLAAC IPv6 addresses and configuring IP6table rules.

¹ see <http://www.nephos6.com/pdf/OpenStack-Havana-on-IPv6.pdf>

With the patch in place, we could launch virtual machine instances with native IPv6 addresses, as shown in the screenshot below.



The screenshot shows the OpenStack Horizon dashboard. On the left is a sidebar with the OpenStack logo and navigation links for Project, Admin, and Manage Compute. The main area is titled 'Instances' and shows a table of two instances. Both instances are named 'productionserver1' and 'productionserver2', using the 'ElectionWebServer' image. They have IPv6 addresses starting with '2001:a18:a:5:f816:3eff:fe4f:cc31'. The table columns include Instance Name, Image Name, IP Address, Size, Keypair, Status, Task, Power State, Uptime, and Actions. The status of both instances is 'Active' and 'Running'.

Instance Name	Image Name	IP Address	Size	Keypair	Status	Task	Power State	Uptime	Actions
productionserver2	ElectionWebServer	2001:a18:a:5:f816:3eff:fe4f:cc31	Voting Machine T-1000 20GB RAM 6 VCPU 80.0GB Disk	-	Active	None	Running	3 weeks, 3 days	Create Snapshot More
productionserver1	ElectionWebServer	2001:a18:a:5:f816:3eff:fe4f:cc31	Voting Machine T-1000 20GB RAM 6 VCPU 80.0GB Disk	-	Active	None	Running	3 weeks, 3 days	Create Snapshot More

Figure 14 Instances with IPv6 addresses in OpenStack Havana (UL testbed)

5.3 Monitoring considerations

It is essential for the infrastructure/service provider (e.g. the administration) to have detailed and timely control over the system, in order to be able to react to events as soon as possible. Activity and traffic monitoring are essential, in that sense, for event management and advanced reaction: for example, identification of denial for service attacks needs to be done as soon as possible and an appropriate system mitigation to be taken, in order to minimize the impact of the attack and suppress further exploitation. Recognizing security events as soon as possible implies runtime monitoring of the infrastructure: for example, is the DNS handling the load now? Are the virtual machines hosting the election website handling the load? If they are not, is it a web server problem? Is the hypervisor or the network service overloaded?

Monitoring of the runtime system is already provided in OpenStack since versions earlier than Havana. The cloud administrator can use the dashboard offered by Horizon, the presentation server in OpenStack. The figure below shows what the administrator can see in the dashboard of the managed project: an overview, in this case, of the instances (number of virtual machines currently deployed), virtual CPUs of the compute server, the current amount of RAM used of the total available amount, the security groups and the virtual IPs (called “floating IPs”) if any were used in the project by the instances.

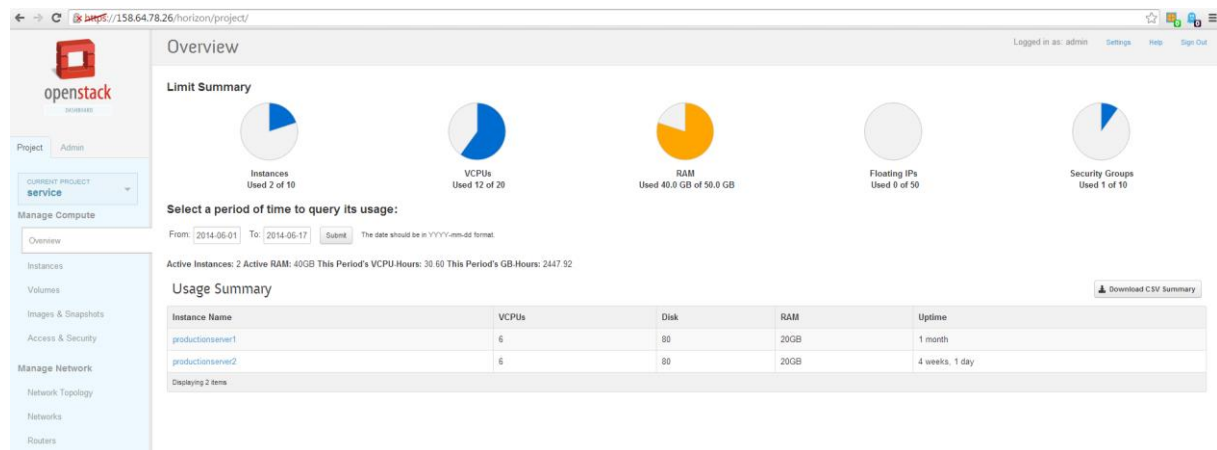


Figure 15 The dashboard in OpenStack's Horizon

Equally, this graphical interface can show the network topology for the virtual networks hosted by OpenStack, some security features related to the firewall (see Figure 16 Firewall rules in the OpenStack election setup) as well as the access control to the projects, graphical interface, VMs and OpenStack resources.

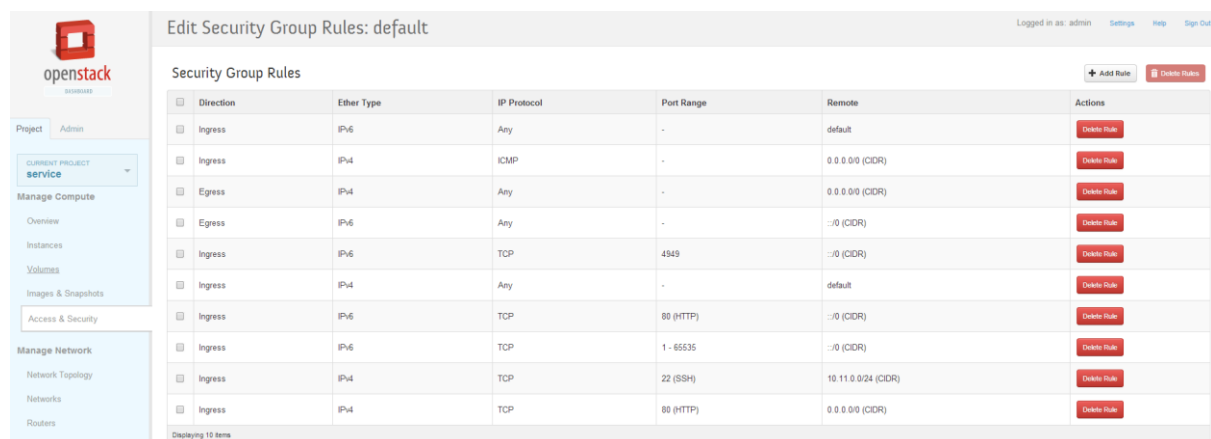


Figure 16 Firewall rules in the OpenStack election setup

For a better idea of the actual resource usage, runtime monitoring for the current cloud infrastructure was done at several layers:

- Infrastructure-wide for the entire election infrastructure, done by Citkomm.
- Hypervisor level from OpenStack's resource statistics service, for the UL cloud setup, which was part of the Citkomm election infrastructure. This is shown in figures 19 and 20.

- Virtual Machine level, from Munin running in the election VMs on top of OpenStack. See Figure 21 for this information.
- End-user level, running from the Internet and measuring the user-perceived performance of the application. See Figure 17 and Figure 18.

The end-user monitoring involved the use of Sonar agents provided by colleagues from Nephos6, a set of scripts running at several locations: one in Luxembourg, and two in Germany. Thanks to Nephos6's dashboard specially adapted for this setup, Figure 6 shows a how potential end-users could experience the election website on May 25th, between 1h20pm and 2h15pm. The performance measurement agents would look at ping and http requests when retrieving the election website index. The election website was periodically updated throughout the election day, in order to show the current voting count per each municipality included in the elections in North-Rhine-Westphalia. The VMs had only IPv6 addresses, as mentioned earlier. Their overall performance before and around May 25th is shown in Figure 7. In our setup, it is also possible to separate how the traffic was split to the virtual machines.

We believe that by providing detailed data at different levels at application runtime, we can provide valuable monitoring information that the infrastructure provider/administrator can use to identify security events, together with their causes and possible suitable remediation.

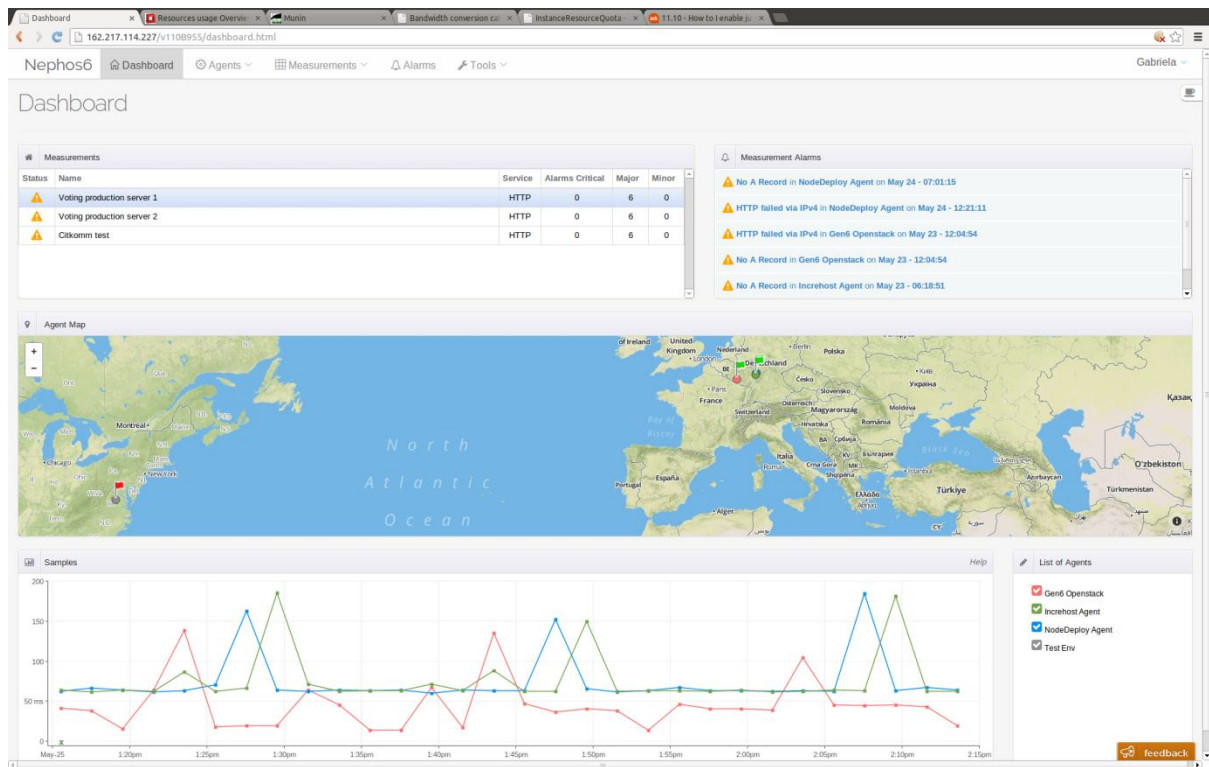


Figure 17 User-perceived performance (blue and green lines) against local performance (red line) of election website on the election day. The website was hosted on two virtual machines hosted by the OpenStack setup at UL, while the flags in the map in the figure

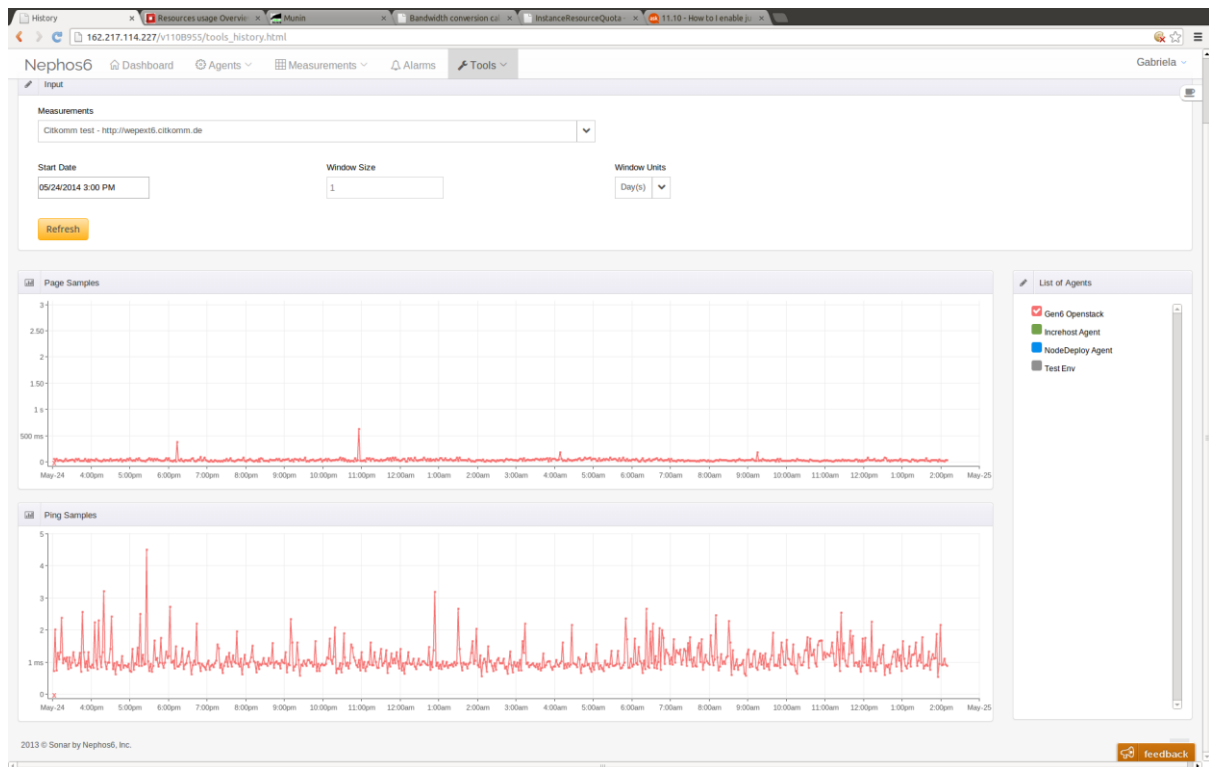


Figure 18 Performance of the election website on IPv6, for one day starting from May 24th at 3pm

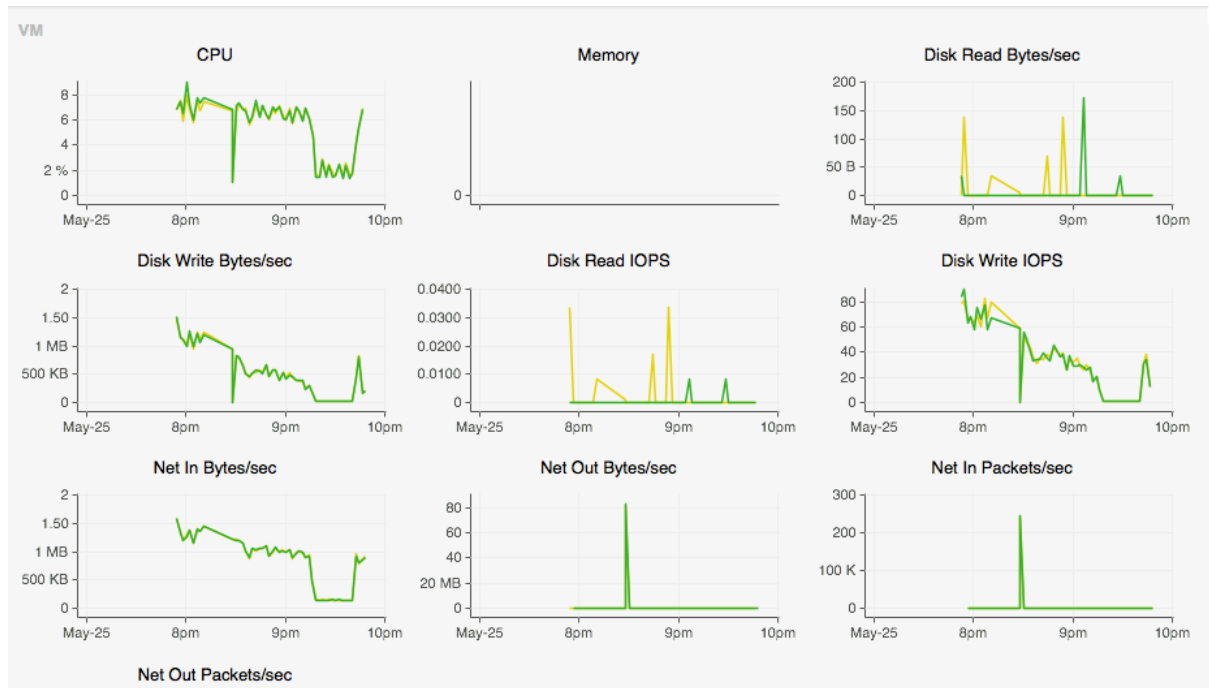


Figure 19 Yellow and green lines showing the evolution of parameters of the two VMs hosting the website on IPv6, on the evening of the election day.

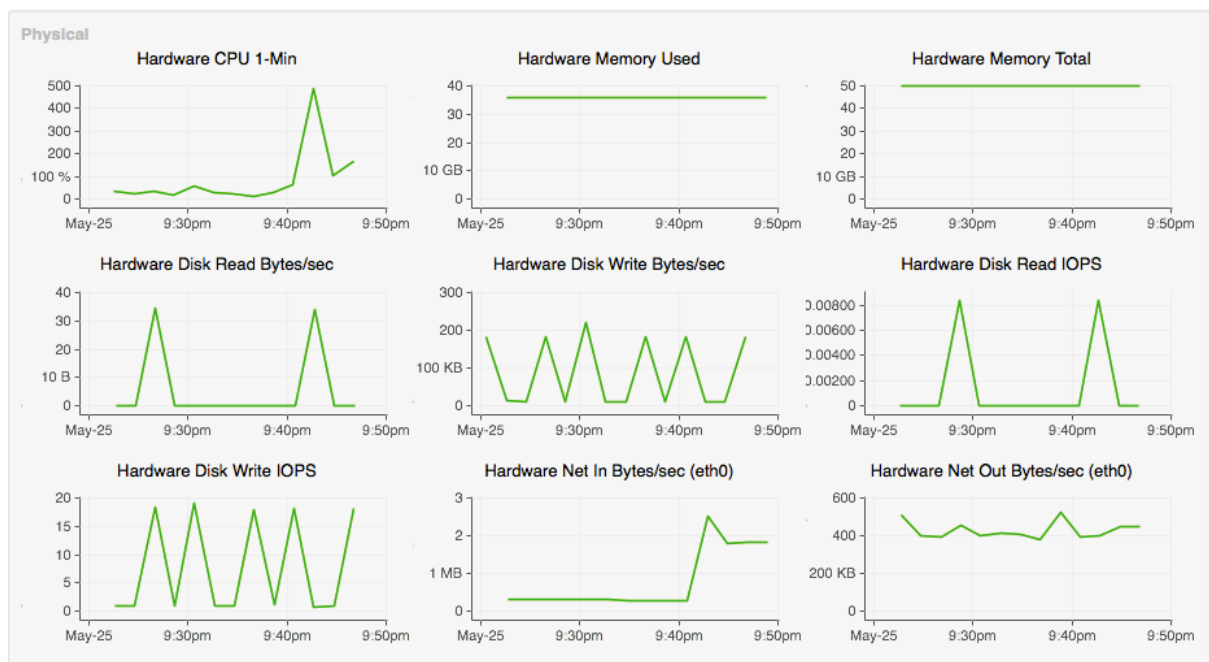


Figure 20 The evolution of the hardware resource usage for the testbed at UL, on the election evening.

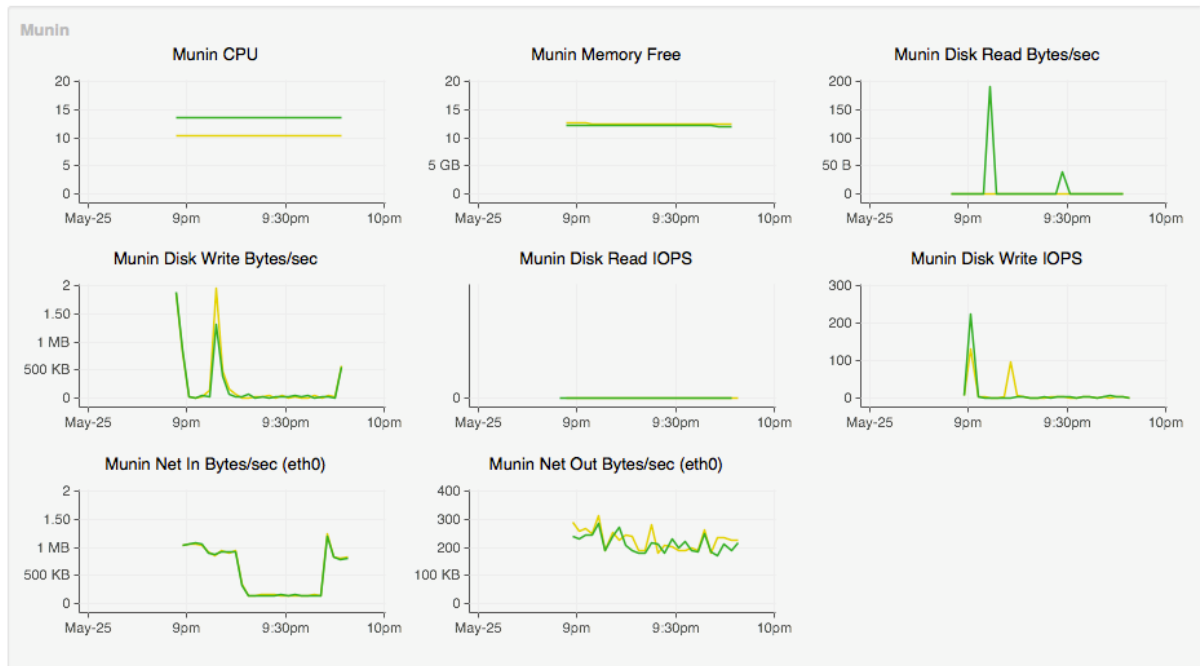


Figure 21 The evolution of the VM performance for two VMs on the election evening.

The figures above show various graphs that a system administrator or manager can see in the dashboard. The information covers the following performance aspects of the cloud infrastructure:

- Per each virtual machine (one drawn in green and another in yellow²), the amount of CPU, memory, disk read and disk writes, network in and network out bytes or packets (Figure 19)
- Hardware resource usage (CPU, memory, disk read, disk write, network in and out) at the level of the hypervisor of OpenStack (Figure 20)
- Internal to each virtual machine, another set of statistics on the CPU, Memory, disk read and write, and network in and out. These statistics are gathered by means of Munin³, a known system monitoring tool (Figure 21).

² Sometimes the green line covers up the yellow one in the drawing so that just the green one is visible.

³ Munin, an open-source networked resource monitoring tool, <http://munin-monitoring.org/>.

6 CONCLUSIONS

GEN6 project WP3 focuses on national pilots where the participants are working to implement IPv6 support on the currently working systems. Three of these national pilots, which are located in Germany, Spain and Turkey, are considered under the same title namely “IPv6 upgrade of e-Government network infrastructures, e-identification, services and applications”. Their targets are similar: examining existing e-Government services currently based on IPv4 and building a pilot for selected services to ease the transition to IPv6. Additionally, current status of the Luxembourg pilot by focusing on the specific services has been presented in the document.

Participants have already prepared several deliverables including the requirement analysis, best practices and experiences gained to guide other governmental institutions. This document is also a part of the deliverable series that is focusing on the progress of these national pilots. Apart from the other deliverables in this series, this document mainly focuses on the specific services of an IPv6 landscape.

7 FIGURE INDEX

Figure 1 Reference Architecture	8
Figure 2 Reference Architecture	9
Figure 3 Logical view of VPN systems and their management inside the FOKUS IPv6 testbed ...	11
Figure 4 Setup with two testbeds connected via encrypted VPN connection.....	14
Figure 5 eITV application data flow.....	16
Figure 6 eITV access screen.....	17
Figure 7 eITV card range query	17
Figure 8 eITV card authorization query.....	18
Figure 9 eITV card status query for DGT	18
Figure 10 Users and protocols used.....	19
Figure 11 Reference architecture.....	20
Figure 12 Reference architecture for UL-Citkomm pilot.....	25
Figure 13 Integration of the machines in Luxembourg and Germany in the same testbed.....	26
Figure 14 Instances with IPv6 addresses in OpenStack Havana (UL testbed)	27
Figure 15 The dashboard in OpenStack's Horizon	28
Figure 16 Firewall rules in the OpenStack election setup.....	28
Figure 17 User-perceived performance (blue and green lines) against local performance (red line) of election website on the election day. The website was hosted on two virtual machines hosted by the OpenStack setup at UL, while the flags in the map in the figure	30
Figure 18 Performance of the election website on IPv6, for one day starting from May 24th at 3pm.....	30
Figure 19 Yellow and green lines showing the evolution of parameters of the two VMs hosting	

the website on IPv6, on the evening of the election day.31

Figure 20 The evolution of the hardware resource usage for the testbed at UL, on the election evening.31

Figure 21 The evolution of the VM performance for two VMs on the election evening.32