Title:	Document Version:
Deliverable D3.6.3 – e-Government Generic 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**:
28/02/2014	07/04/2014	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), Martin Krengel (Citkomm), Gerold Gruber (Citkomm), Timo Baumgart (Citkomm), Carlos Gómez Muñoz (MINHAP), Juan José Rodríguez Moreno (MINETUR)

Abstract:

This document is the third one in a series of deliverables documenting the progress of the three national pilot projects within GEN6. The national pilots are located in Germany, Spain, and Turkey. Their goal is the transition of selected, public sector services from IPv4 to IPv6 operation.

Keywords:

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

Revision History

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

Revision	Date	Description	Author (Organization)
v0.1	16.01.2014	Document creation	Emre Yüce (ULAKBIM)
v0.2	07.02.2014	Added German pilot	Martin Krengel (Citkomm)
v0.3	12.02.2014	Turkish pilot contribution	Emre Yüce (ULAKBIM)
v0.4	14.02.2014	Added Spanish pilot	Carlos Gómez Muñoz (MINHAP)
v0.5	17.02.2014	Additions for German pilot	Gerold Gruber (Citkomm)
v0.6	18.02.2014	Proof reading, order of the pilots reorganized with respect to DOW, executive summary and conclusion sections added.	Emre Yüce (ULAKBIM), Onur Bektas (ULAKBIM),
v0.6 3/8	14.03.2014	Proof reading, unify style of writing (incomplete)	Gerold Gruber (Citkomm)
v0.7	14.03.2014	Proof reading (mostly grammar)	Carsten Schmoll (Fraunhofer)
v0.8	19.03.2014	Proof reading, complete some content from MINETUR	Juan José Rodríguez Moreno (MINETUR), Carlos Gómez Muñoz (MINHAP)
V0.9	01.04.2014	Finalize	Emre Yüce (ULAKBIM)
V1.0	07.04.2014	Published and send to Commission	Uwe Kaiser (FOKUS)

Disclaimer

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 four 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 document gives an updated overview of the current state of three national GEN6 pilots. For each pilot, it describes its approach on the generic service level (DNS, DHCP, etc.) to the transition. This approach affects how services can be delivered inside the networks. Furthermore, each pilot provides information on affected components, experiences gained during the transition process and some description of the obtained results and if available some tests to verify a successful transition.

This deliverable is the third snapshot of a living document. It focuses on generic service elements, including security elements and their transition to IPv6. Its successor (D3.6.4) will cover customized applications and devices details as the pilots evolve.

All these deliverables will be grouped into D3.6, showing commonalities and differences of the pilots so that it becomes more useful for a government audience. GEN6 can be taken as a starting point to introduce IPv6 based on the best practises of the variety of documented pilots.

Table of Contents

1 INTRODUCTION

This document is the third 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.

An important point for the transition of an existing e-Government service to IPv6 (regardless if done by means of native IPv6 or a dual-stack setup) is not to interrupt the service, or to affect the service as little as possible for existing users. Considering the local technical environment, different techniques are possible for such a transition of an e-Government service.

The preferred one of different possible approaches is building a test bed resembling the real environment as much as possible. This will minimize the risks of dealing with the production environment directly. Challenges, pitfalls and best practices may be studied within this test bed. Building a test bed for application testing is much easier by making use of virtualization technologies. In addition, the steps taken for the transition of the test bed should be documented well for further reference during the later transition of the production environment. Hence, the requirements can be seen better and finally fulfilled during the transition of the production service.

IPv6 transition is expected to affect the network infrastructure and the applications which require network communication. Keeping track of affected IT infrastructures for transition will be a tremendous task if planned unwisely. The GEN6 consortium provides a series of deliverables in order to address this issue. Likewise, the other deliverables of the series D3.6.x, this document includes the experience of the national pilots in Germany, Spain and Turkey which are working on the transition of a municipal data centre, a government backbone and a government portal, respectively. Accompanying other deliverables in the series, the current document mainly focuses on the generic services of an IPv6 landscape. In this context, generic services are defined as the services that are common to all participants in a sense that is probable to be found in other government institutions. These include, but are not limited to application layer services like DNS, DHCP, ALG, proxies, load balance devices, monitoring services like SNMP, web servers, database servers, ftp servers, VPN and so on. Security considerations and lessons learned sections are also provided with respect to these topics.

The forthcoming deliverable D3.6.4 will focus on services that need customized applications

and devices such as custom written monitoring services, scripts, in-house developed gateways (VPN, AAA), legacy programs that are still developed and need updates, special hardware (SMS gateways, NAS devices, etc.) and any other stuff that is in lack of commercial update support.

In this deliverable, generic services are investigated under three different titles, namely: Transition to IPv6, affected network components, and security aspects of using IPv6. Discussions under the transition title deal with application support aspects of enabling IPv6 on services like DNS, DHCP, or other network services.

2 TRANSITION TO IPV6

This chapter documents the chosen high-level decisions for the introduction of IPv6 in each national pilot. It describes the chosen approach for each pilot, how IPv6 has been introduced (e.g. in parallel, new networks, or inside existing ones), which steps were taken to do so (from a top-down perspective) and which goals have already been achieved (and how). In this part of the deliverable, also the pitfalls found during this work are documented.

2.1 Chosen Approach

German Pilot:

For the German pilot, it was decided to start all IPv6 transition work on a dual-stack strategy. The most important reason for this decision was that the real existing infrastructures were very heterogeneous, this fact being related to the applications in use. Up to now, there is no realistic way to implement an IPv6-only infrastructure on the client side. On the server side it is also not useful to separate the IP traffic by protocol version. In this case, the application data would have to be kept in a synchronous state, for both IP worlds. To avoid this additional effort and increased technical complexity, the dual-stack approach was chosen as the basic concept. Wherever possible, a testbed landscape was used first.

The activation of IPv6 was then executed step by step.

Initially, the used network infrastructure components were reviewed. Switches turned out to be non-critical as they are used as simple layer 2 devices in the Citkomm network, and *managing* them via IPv6 was no goal of the project. This results from the use of a separated out-of-band management network with no connection to customer services related traffic.

Then, the basic enabling of IPv6 on the involved servers and clients was considered. To avoid unwanted and therefore uncontrolled communication, IPv6 was deactivated at first in all relevant networks and systems. Then IPv6 was enabled on server side first, and after successful tests on the client side, too. Until this point still all services and applications used IPv4, as all DNS requests resolved to IPv4 addresses only. Afterwards, IPv6 could be enabled application by application, after testing with some clients with specific host-entries overruling, respectively replacing DNS resolution during initial testing.

Following the same basic principle, network segments were enabled for IPv6 one by one. This

way, IPv6 connectivity could be tried in small steps. This was also easy to handle in backbone segments with dynamic routing, because on the installed routers the IPv6 routing is handled by a separate daemon, which is independent from the IPv4 routing service.

This approach gave birth to the opportunity to make an IPv6 roll-out in single steps, allowing possible functional errors to be identified and fixed easily.

Spanish Pilot:

As it has been mentioned in previous deliverables, the Spanish pilot combines two different approaches to the IPv6 transition:

- Dual-stack, as the chosen mechanism for transitioning to IPv6 in the connection areas of Red SARA, and in the infrastructure that supports the eITV service provided by MINETUR.
- IPv6 to IPv4 translation, using reverse proxy and NAT64 equipment located in Red SARA's shared services data centre, for providing a transition mechanism that allows public administrations to offer IPv6-enabled online services.

These two approaches are complemented by the use of tunnelling techniques required by the cross-border pilot (due to the lack of IPv6 native support in sTESTA), which helps the Spanish partners to acquire a solid expertise in deploying IPv6 which other government units can benefit from.

Turkish Pilot:

The Turkish pilot has been in production over IPv4, and the transition should be seamless for the end users (Turkish citizens). Considering this issue, the pilot participants have decided to implement dual-stack through the network.

As stated in other deliverables, the Turkish pilot consists of two parts: Frontend and backend transition. The frontend transition includes the IPv6 enabling of the e-Government gateway (EGG) portal while backend transition includes the establishing of IPv6 communication between TURKSAT and the participating governmental institutions (SGK and PTT). Both cases were suited to work on the dual-stack implementation. Most of the planned IPv6 transition in the Turkish pilot is complete, and participants have observed that dual-stack is the right solution for the pilot. Still, another important observation is: One should keep in mind that dual-stack increases management workload for the network since the administrators are responsible for the security and monitoring of two different protocols.

2.2 Planned Order of Changes due to Transition

German Pilot:

IPv6 was always activated step by step. Due to the global dual-stack approach, the enabling of the new protocol could be started in different subnets at the same time.

To make sure that there will not occur any unwanted side effects from one IPv6 transition area to its legacy neighbour segments, as a very first step all router and gateway systems were checked for their IPv6 state – and IPv6 was strictly deactivated. This way, we made sure that enabling IPv6 in a single network segment was limited to this segment alone and there would be no IPv6 communication happening to other network areas.

After that, the first network areas were enabled with IPv6. We started with the local Internet uplink. Starting from the provider uplink router down through the access components and gateways, the DMZ and the internal gateway routers were enabled with IPv6. As Citkomm uses a fully redundant access network, several failover mechanisms had to prove their IPv6 capability. Because of the used router systems and the separated IPv6 routing daemon this could be performed in the productive environment after passing the testbed successfully without affecting IPv4 in the production networks.

In parallel, the WAN/VPN network with its specific components has been enabled for IPv6. It is based on different VPN solutions, using Internet or MPLS networks as underlying transport facilities. The necessary testing was done with a testbed that represents a typical customer access infrastructure. IPv6 ability could be enabled for the transport layer (if available) as well as for the inside tunnel communication for the VPN solutions.

After finishing the work on the Internet uplink, the first services in the DMZ have been enabled for IPv6. An early adopter was the public Citkomm website. The existing architecture uses reverse proxy servers for all accesses from the Internet to the vast majority of the web servers. IPv6 only had to be enabled on the public side of each reverse proxy. Afterwards, additional services have been enabled with IPv6, namely the public DNS and SMTP servers.

Moving these areas to production state required the monitoring system to be IPv6-aware. Externally available services should be monitored from an external probe. The provider for this system has to be capable of offering IPv6 services, namely connectivity for the monitoring appliance. The latter had to be enabled for IPv6 with its longer addresses, and checks had to be adapted manually in many cases.

The work on the implementation of IPv6 in the local area networks (LAN) – has been started independently from the work described before. In the Citkomm pilot work on the LANs started after the server transition due to the involvement of the same staff. The LAN consists of "Linux enhanced" Windows networks, meaning it is based on an Active Directory with integrated Exchange and MS SQL Servers and some Linux servers for additional services, like e.g. Wikis. The clients are Windows systems (mostly Windows7), and some Linux desktops. As part of the German pilot, also a transition for a Linux-based network has been started. Due to strategic decisions, the former Linux server based environment of the Citkomm LAN was migrated to Windows. Inside the LAN, servers were enabled for IPv6 first. In this state they started to use IPv6 with link local addresses to other machines reachable on IPv6. All Windows-internal communication switched to IPv6 in this scenario - more or less automatically. To get into the chosen addressing concept, the addresses from the Citkomm range of the national government address scheme have been configured on the servers. Additional auto-configured addresses have been suppressed. DHCPv6 has been used to provide clients with IPv6 addresses. The router advertisements for the network were supplied from the segment's router that connects the LAN to other network areas. By using static address assignments with DHCP, it was possible to get the clients in production step by step. The further roll out of IPv6 could be grouped and sorted by application use and the criticality of the touched workstations.

In the beginning, external communication to other governmental institutions using the national government backbone was thought to be the first area for transition. However, the enabling of the external network link itself had been delayed for many months. Furthermore, the use of real IPv6 communication needs active IPv6-enabled paths to internal server segments when passing the backbone of Citkomm. Due to load and change rate related issues with the IPv4 routing daemons, the central backbone was one of the last components brought into an IPv6 production state. In fact the services in the national government backbone for DNS and SMTP had not been IPv6-enabled until the writing of this document. Yet, recent success notifications have stirred new optimism in this work area.

Spanish Pilot:

In the Spanish pilot, the planned order of changes has been:

1. Setting up the platform for providing shared services for IPv6 access to e-Government web sites. This involves ensuring external IPv6 connectivity to Internet, by configuring the network devices, hosts and applications located in Red SARA data centre.
2. Upgrading the backbone of the network of Red SARA to IPv6, as well as the links

connecting the institutions' sites to this backbone, carried out by Red SARA's telecommunications provider, under the guidance and supervision from MINHAP.

3. Configuring the equipment located in the connection areas of the entities linked to Red SARA to operate in dual-stack, including the connection areas of MINETUR and MININT involved in the eITV service.

In parallel, the adaptation to IPv6 of the eITV service has been carried out.

Turkish Pilot:

The Turkish pilot has prioritised the frontend IPv6 transition. Hence the first phase of the pilot focused on the IPv6 support of e-Government gateway portal. At first, the local ISP has been queried for an IPv6 uplink. After the receipt of a positive answer on having an IPv6 uplink from the current ISP, the internal network infrastructure components had been analysed, and requirements regarding the internal network had been enlisted. This list was made, starting from the outmost network components and continuing with the inner ones. To be more precise: The EGG portal backbone router, layer 3 switches, firewalls, load balancers and web servers have been checked if they are IPv6 ready in the sense that they can have basic IPv6 capabilities like identifying and routing IPv6 packages and running IPv6 routing protocols (OSPFv3, BGP). In other words: At this stage, more advanced IPv6 support such as IP mobility was not considered a must for the IPv6 support of network appliances. After being sure that every network appliance on the EGG's road was IPv6-capable, an IPv6 address plan has been created and implemented in the same order: Starting from the outermost level.

The first phase had been completed throughout the first year of the pilot. As the first result of the pilot, the EGG web portal had been IPv6-enabled.

The second phase of the pilot focused on the IPv6 transition of the communication between TURKSAT and the other governmental institutions which provide the backend services. In this phase IPv6 was working over either dedicated lines or by deploying VPNs between the institutions. For the pilot VPNs, tunnels for secure communication have been deployed between the institutions. For this purpose, public integration boxes have been developed and deployed on the end points of the communication. These boxes create a VPN tunnel over IPv6 to secure the communication. Currently they have been successfully deployed in SGK and PTT.

2.3 Successfully Moved Components Till Now

German Pilot:

At this point in time, most components and areas of Citkomm are enabled for IPv6. In detail these are:

WAN Network

The WAN routers are Linux-based appliances, using OpenVPN for tunnelling. A recent version of OpenVPN was tested successfully with IPv6 on both, the outer and the inner side of the tunnel tube. Basic services like NTP, DNS and proxy are enabled for IPv6 in dual-stack use. The approved design has not been integrated in the default setup procedure for the network components so far. But it has been tested in several installations extensively and it expected to make its way into the next release of the routing appliances.

Internet Access

The Internet Access network of Citkomm is fully IPv6-enabled. All components run in dual-stack mode. All fail-over mechanisms of the high availability design support IPv6 and IPv4. Several servers with connections to the public Internet are enabled for IPv6. Most IPv6-enabled Web servers use the reverse proxy as IPv6 termination point, due to security considerations. Servers such as DNS or SMTP use IPv6 directly, but are protected by firewalls.

Local Area Networks

In the local networks, the IPv6 transition has been successful implemented in different testbeds, covering a variety of server systems. In productive networks of a customer and Citkomm itself, the implementation has just started.

Other Networks

The connection to the national government backbone is IPv6-enabled. No services are in production so far due to the outstanding IPv6 empowering in the core backbone.

Spanish Pilot:

As it has been described in D3.6.2, in the Spanish pilot several components have been successfully moved to IPv6 so far.

Regarding the shared service platform for providing IPv6 connectivity to e-Government Web Portals, it has been implemented using two different approaches:

- Initially, based on a Reverse Proxy, combined with NAT64 for services in which the

validation of the user's electronic certificate was required

- After operating the service for some time, and adding new portals, the solution was evolved, having NAT64 not only for the cases in which there is involved a user's electronic certificate validation, but also for all the services based on SSL, since this simplifies the management of the server certificates used in SSL connections.

Using this platform, several Web Portals operated by MINHAP have been made IPv6-enabled:

- e-Government Portal: www.administracionelectronica.gob.es
- Forge of the Technology Transfer Centre: forja-ctt.administracionelectronica.gob.es
- Common Electronic Registry for the Spanish National Administration: https://rec.redsara.es
- Portal to communicate address changes to public administrations: http://cambiodomicilio.redsara.es
- Electronic Signature Validation Service "Valide": http://valide.redsara.es
- Preproduction environment of the Spanish PEPS used in STORK platform: http://prespanishpeps.redsara.es
- Production environment of the Spanish PEPS: https://spanishpeps.redsara.es/

Additionally, a feasibility assessment for moving to a dual-stack platform some of the services operated by MINHAP that currently make use of the IPv6 enablement shared service has been performed, with positive results. This assessment has been considered in order to provide an alternate solution for enabling IPv6 portals, in case scalability problems are found when increasing the number of portals in the shared service platform based on the IPv6-IPv4 gateway. With this approach, e-Government services operated by MINHAP would be made IPv6 ready by means of this dual-stack platform, while the IPv6-to-IPv4 gateway would provide IPv6 readiness to the e-Government services operated by other government units, as a shared service in Red SARA.

Regarding the backbone of Red SARA, all the connection areas of the Ministries have been configured to support IPv6, enabling dual-stack in the equipment. New pseudo interfaces for IPv6 have been added on the routers (WAN and LAN networks) but over the same VLAN at VPLS level, so no change in the VPLS infrastructure has been required.

Additionally, MINETUR is adapting the eITV service to IPv6 as defined in the project. This has

two distinct parts: the IPv6 infrastructure and the modification, to support IPv6, of the application that makes use of that infrastructure. To achieve this goal, both development and systems departments of MINETUR are involved, working on the basis of a coordinate effort.

Regarding the eITV infrastructure, the production environment already deployed and connected to Red SARA and the Internet has been tested, verifying successful IPv6 connectivity from Red SARA and from the Internet.

Due to the need to test the eITV service before offering it to the real users, now we have two environments: preproduction and production. The production environment is IPv6-full while the pre-production environment use IPv4/IPv6 dual stack mode because it is necessary to access to it from the development department computers that use IPv4 protocol.

Turkish Pilot:

For the Turkish pilot, currently TURKSAT and the participating institutions have active IPv6 uplinks from their current service providers. In addition, the EGG portal, which is managed by TURKSAT, is IPv6-enabled for more than a year now. For the time being, TURKSAT is monitoring the activities and requests in EGG portal made by citizens. Monitoring activity is being made for both security purposes and for reporting on the usage of EGG services.

On the other hand, backend infrastructure has been enabled with IPv6 for SGK and PTT services. This means that queries made for services that are provided by SGK (e.g. social security records) or PTT (e.g. postal service records and activities) are being transmitted to them over IPv6, and the answers to these queries are being sent to TURKSAT over IPv6 similarly on the backend.

2.4 Enabling IPv6 in Components

2.4.1 Practical Tests

German Pilot:

- General:

According to the progress in the pilot, different components were involved in the IPv6-enabling process and had to prove their IPv6 capabilities. On the network level, the basic functionality does not cause any harm, however, when it comes to real applications or more complex setups some issues had to be resolved.

Typical test commands for low-level operations are:

ipconfig / ifconfig / ip a (to check the validity of the local configuration)

ping / ping6 and tracert / traceroute / traceroute6 with options to select sender addresses or interfaces to check the connections to targets

route / ip r / ip -6 r to check the routing tables

- Application backbone infrastructure

Citkomm and Fraunhofer have set up three IPv6 test areas with more than 30 virtual servers and clients. Recent operating systems such as Windows Server 2008 R2, Windows7, Ubuntu LTS 12.04, or SLES11 SP3 support IPv6 “out of the box”. Some minor issues needed extra attention (see also the next chapter for details). The basic services DHCP, DNS, and electronic mail operate as expected. Web services also cause not much trouble. If there are issues, then they are related to the applications that are not aware of the longer addresses and the different literal IP address syntax.

- Network infrastructure

The core interconnect network at Citkomm uses Linux-based routers as node systems. On the perimeter, some Cisco systems are in use. From these, the Internet uplink routers are in the focus of the project as they provide the connectivity to the world and interact via OSPF routing protocol with the interior Linux routers. The routing interaction between Cisco and Linux systems works good as well as the OSPF routing information exchange with the Quagga package on Linux. Due to Quagga problems when using a large number of routes and frequent topology changes (and some missing features), BIRD has been tested as an alternative package. The observed problems are not related to the GEN6 project activities. They were observed coincidently at the time of the project as a side effect of some centralisation, homogenisation and expansion of the Citkomm network and appeared only in IPv4. Quagga seems to work well for small environments with only a few number of changes per time. For heavier use, alternatives can better fight the admin’s headaches.

For the wide area network, Citkomm uses the self-developed appliance “iWAN”. All tests are performed with the current iWAN generation, based on Ubuntu LTS 12.04. The distribution includes an OpenVPN implementation that supports IPv6 on the underlying network as well as inside the secure tunnel. Not surprisingly, the use of IPv6 inside the tunnel does not require the

outside tunnel to be IPv6-aware. All communication could be tested successfully with IPv6 and with combinations of IPv4 and IPv6. The scripts that generate routing information dynamically when a tunnel comes up, were adapted to take care of IPv6 routes. This is required as the Citkomm infrastructure includes redundant tunnel terminal systems. Therefore, care must be taken for using the correct routing information, regardless whether or not the iWAN at the customer side has chosen one or the other terminal. Therefore, for any such setup the correctness of the established routes have to be checked carefully.

The generation and distribution of firewall rules in an automated way is an action point for the next period, as well as the automated setup of an iWAN system with respect to IPv6 configuration.

- Customer Environment / LAN

The infrastructure of a typical client network is based on Windows server technology. The setup of address assignment and basic network configuration distribution via stateful DHCP has been described before. The correct setup of Windows and Linux clients was verified successfully.

The tested applications are web browsers, mail clients, RDP and ssh for connections to servers, at this moment. As soon as the server systems for native client/server applications are available, they will be tested, too.

Spanish Pilot:

As it has been mentioned before, at this moment the connection areas of the Ministries are IPv6 capable. To achieve this goal, tests were conducted in three ways:

- Traffic processing through VPNs
- HTTP traffic between two connection areas
- DNS IPv6 capabilities

Traffic processing through VPNs

All the traffic processed through the VPLS backbone of Red SARA is encrypted using the IPsec capabilities offered by the edge firewalls located in the connection areas. This is true for IPv4 traffic and must be configured in the same manner for IPv6 traffic. To do so, new tunnels have been defined on the devices included in the test scenario and IPv6 native traffic has been

injected between these connection areas. The result was successful and, as expected, IPv6 tunnel behaviour was similar to that of IPv4. At this moment, native IPv6 traffic can be processed between the Ministries' sites, and this traffic is encrypted on the edge firewalls. As IPsec connections are defined between networks (tunnel mode), in fact the only IPv6 traffic that can be seen in the backbone is the ESP traffic between edge firewalls.

HTTP traffic between two connection areas

More or less half of the traffic processed in Red SARA is HTTP, therefore it was considered as the best functionality test, to install an HTTP server in one connection area and try to navigate from other server located in another connection area. The chosen connection area to host the HTTP server was the one owned by the Ministry of Industry Energy and Tourism (MINETUR). Navigation was performed from several locations, in different Ministries, using native IPv6. No differences were found while using IPv6, and user experience was similar (speed, latency, …).

DNS IPv6 capabilities

To implement an IPv6 services infrastructure, one key point is DNS. It is necessary to define new DNS entries for direct and reverse resolution using IPv6 addresses (AAAA records for direct resolution and ip6.arpa zones for reverse resolution). The server chosen was the one located at the Central Services connection area (where the e-Government shared services provided by Red SARA are hosted) and the new entries were added at the zones involved in the test. This server was configured in dual-stack operation, and it had no problems in answering queries related to IPv6 services neither when connecting through IPv4 nor when connecting through IPv6.

In the case of MINETUR eITV service, access tests via IPv6 with a private address range have been made in the MINETUR laboratory.

A first line of perimeter security has been designed. It defines the access to the DMZ service and it is delimited by two Cisco 2960S, level 2, systems.

An IPv6 /64 prefix is used. The IP addresses to be used are those obtained automatically when auto-configuring the equipment. Once the IP is obtained, it has been configured manually on the equipment.

This process is the same for the HSRP virtual IP's required for the Cisco equipment.

Three IPs are used for each HSRP, two physical and one virtual.

In the perimeter security equipment, Palo Alto PA-5050, the same procedure is used to obtain the IPs and the high availability system, allocating thee IPv6 addresses, two physical and one virtual.

The configuration of the load balancing equipment, F5 3900, uses the same mechanism as in the previous equipment, with three IPs (two physical and one virtual).

Two DNS servers are used, dns.ipv6.es and dns2.ipv6.es and they are using the same procedure to obtain their IP addresses.

This configuration will be the same as in the production environment and is represented in the following figure.

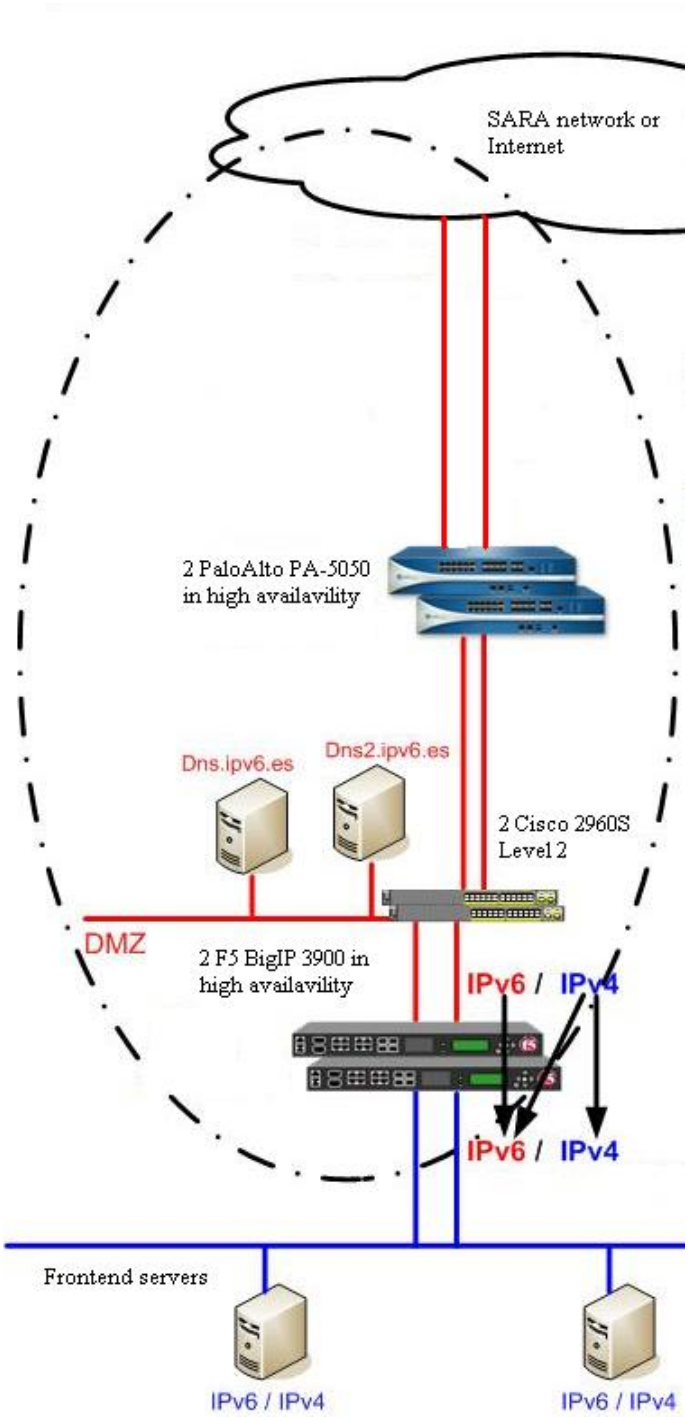

Figure 1 – Spanish Pilot: MINETUR's Network Configuration

Additionally, as it has been mentioned before, MINHAP has performed some test to assess the feasibility of moving to a dual-stack platform some of the applications that currently make use of the IPv6 enablement shared service. These tests were made with the Spanish PEPS (Pan-European Proxy Service), the interoperability node of the STORK platform, by setting a dual-

stack path (involving routers, firewalls, reverse proxies and load balancers) between Internet and the PEPS servers, which have been configured also in dual-stack. Though some problems regarding the configuration of the maximum transfer unit (MTU) were initially found, after solving them the results of the tests were positive, confirming that the designed solution can work properly and can be extended to other services.

Regarding the evolution of the implementation of eITV service, it is installed in the pre-production environment. Preliminary tests have been done having obtained a satisfactory result. Access to the application is successful. Users are validated in the application in two different ways:

- The traditional system of user and password
- By means of digital certificate.

Both validation methods have been tested with successful results.

Turkish Pilot:

Practical tests for Turkish pilot can be assessed under two main headlines: Tests for the EGG frontend and tests for the EGG backend. For the EGG frontend (Web portal), TURKSAT had already built a test environment. The test environment used the same configuration as the production environment and updated respectively. A new feature is first tested in this test environment and if it succeeds, it is ported to the production environment. Although every new update has been tested, deployment of the feature in the production environment may give different performance results as the EGG Web portal is serving over 15 million registered citizens.

In addition, performance and conformance tests have been run for the EGG frontend over IPv6 in the test environment. These tests included access and penetration tests over IPv6. After completing the tests successfully, the new configuration had been moved to the production environment. Also, Load balancer tests were a crucial part in the Turkish pilot transition work.

As the second topic, connection and performance tests (including throughput, jitter etc.) were made while setting up the connections between TURKSAT and the participating governmental institutions (SGK and PTT).

2.4.2 Security Considerations

German Pilot:

- General:

Citkomm has an established security policy for its productive environment. The policy has been designed in an IPv4 world but can and must be extended to the IPv6-enabled world, too. As a dual-stack approach was chosen, the network paths for the permitted traffic are the same for both protocols. To be able to use the known graphical interface for defining firewall rules a new version of the “fwbuilder” tool had to be set up and was installed and a new base system consequently.

More in deep investigation for specific IPv6 issues is on the schedule.

- Application backbone infrastructure

The application servers themselves are treated as being located in a safe area. Nevertheless, the router to the application segment has firewall rules on it that restrict the access to the servers.

- Network infrastructure

For the network infrastructure the general security rules are applied. In addition, the firewalls and application layer gateways (proxies and reverse proxies) must be tested and watched.

- Customer Environment / LAN

These networks are protected by iWAN systems. The basic security considerations are the same used for the network infrastructure above. In addition, a customer administration interface will have to be updated. Among other things, it allows the customer’s administrators to add exception rules to the proxy rule sets. This application has to be extended to allow the handling of client IPv6 addresses.

Spanish Pilot:

In the case of Red SARA, the main security considerations have been:

- Implementing the changes in the firewall rules to deal with IPv6

- Configuring the IPsec tunnels that link the connection areas so that the traffic that crosses the network always travels encrypted

These considerations are explained in more detail in following sections.

In the case of MINETUR, the firewall is our main security system. As we have two environments: preproduction and production, two rules have been enabled in the firewall to allow access to these environments only by http and https protocols.

Turkish Pilot:

Turkish pilot consists of systems that hold critical citizenship information. Hence, security policies had already been in action for IPv4, even before the GEN6 project. These policies include access control rules (firewall rules, access control list rules etc.) and performance criteria in order to protect the whole system from DDoS-like attacks. These policies have been successfully adapted to IPv6, and the system has been made dual-stack capable. After IPv6 transition, security tests were performed by a third party information security company in order to check confidentiality, integrity and availability of the whole system.

For the EGG backend, which constitutes of the connection between TURKSAT and the participating governmental agencies, there exists a direct connection. This connection has been made over IPsec VPN so that this communication has been secured by encryption.

2.4.3 Lessons Learned (Experiences and Pitfalls)

German Pilot:

The Linux kernel supports port mapping in iptables only in latest versions: As a consequence of the lack of NAT in IPv6, the port mapping at a gateway was not implemented until recent Linux kernel versions. For a test scenario and a customer approval check for implemented services it was required to forward an IPv4 connection to a machine that then used IPv6 for the further communication to a final test object.

No packet for Nagios / Icinga nrpe client with IPv6 support available: For monitoring in the well-known Nagios / Icinga monitoring system the nrpe remote node is required. At this moment no nrpe-client with IPv6 support is available for Ubuntu LTS distributions. In consequence, it is necessary to compile the source code with adequate options. This can lead to a fitting package in a local repository or even to a contribution to the Ubuntu project. Maybe newer technical

approaches will make the current nrpe obsolete. But the wide-spread established base justifies the extra efforts in Citkomm's heterogeneous infrastructure where several Linux distributions have to be served.

Spanish Pilot:

One of the main issues has been determining the actual compatibility of the existing equipment and services with IPv6. In the case of Red SARA connection areas, it has been found that not all existing services support IPv6. Though some of them can be easily upgraded, there are others whose updating would require considerable investments. This has led to clearly differentiate between those services that are essential to provide IPv6 transport capabilities and those that support network operation, focusing on the first ones. Therefore, it has been decided not to act on those support services that are not compatible with IPv6 and cannot be made compatible easily, such as the High Availability service, leaving them out of the scope of the pilot.

After the practical tests, the main lesson learned is that IPv6 is not completely different from IPv4, after all. The main concepts of routing, firewalling, tunnels, etc. are similar to IPv4, though special care needs to be taken not to make mistakes due to the new addressing scheme. Once compatibility of the different elements has been ensured, the way to implement security, services and so on is similar to that of IPv4.

There have been also some lessons learned after the tests for assessing the feasibility of a dual-stack platform for MINHAP services, where some problems with the MTU in the reverse proxies were encountered. These reverse proxies are used for security reasons. Since direct access to the services from the Internet is not allowed, they are located in front of the application servers. Since VPN are used in Red SARA for connecting different sites, a header is introduced in the IP packet that increases the MTU above the defined limit. When these packets go through the reverse proxies, a fragmentation request is generated so that the reverse proxies decrease automatically the MTU. However, this was not working properly, so the adopted solution was decreasing the MTU of the interfaces of the reverse proxies manually.

Regarding MINETUR, initially, the 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.

Although laborious, the problems have been similar to those of IPv4. The difficulties found have not been too great provided some basic considerations as, for example, exclude IPv4 addresses in the program code and always use stable identifiers to connect to other nodes (host names,

for example).

Thus, delegating the resolution of the IP addresses to the name resolution system, there will be no problem to access to other hosts.

Turkish Pilot:

One of the experiences gained through the project and IPv6 research is that one of the reasons for an institution not to be IPv6-enabled may be that the respective ISP does not have IPv6 support yet. Another reason is that institutions do not want to modify their already working systems. In Turkish pilot, it is observed that besides the technical issues, one should investigate the administrative and human resource issues in IPv6 transition. In other words, in some situations institutions may need to be convinced about IPv6 transition.

There had been no major IPv6 connectivity problems experienced in the Turkish pilot. Turkish ISP (Turk Telekom) provides native or dual-stack IPv6 connectivity, so by having IPv6-enabled devices, institutions are able to connect to global IPv6 network preferably using dual-stack.

Open source tools are commonly deployed in institutions in Turkey. It has been discovered that some open source tools may be problematic with respect to IPv6 support. For instance; if you do not own commercial support, IPv6 support is often not prioritized in code development.

Another issue may be IPv6 misconfiguration of third party servers. There are major issues in the case that a client has IPv6 support but the destination network has a misconfigured IPv6 Web server.

On the other hand, it is observed that network and security appliances can be problematic in terms of IPv6 deployment. There is no clear and common definition of “IPv6-enabled” for network and security appliances. Therefore, institutions that require getting an IPv6-enabled appliance should list their requirements and level of support, such as e.g. QoS or mobility support.

3 AFFECTED NETWORK COMPONENTS

This chapter takes a deeper, more technical look at certain network elements and servers of an IT infrastructure which are affected by a migration of e-Government services from IPv4-only to running IPv4+IPv6 support (from their users' point of view). These systems include network-level devices such as routers, plus auxiliary services like electronic mail and DNS, which are in direct or indirect use of the migrated e-Government services.

3.1 Routers and Routing

German Pilot:

The router support for IPv6 caused no problems besides the Quagga issue, see above. Most of the routers in the Citkomm network are Linux based. Some systems are Cisco routers. In none of these systems any kind of problem regarding especially to IPv6 occurred. Also the used dynamic routing protocols resulted in no specific problems. Helpful is the fact, that in Linux software routers the OSPF6 daemon is fully separated from the IPv4 daemon. This gives good control for soft transition scenarios, but finally it has to be watched for IPv6 routing independently of IPv4 in either case.

Spanish Pilot:

Regarding Red SARA, at present:

- All Internet routers are capable to route IPv6 traffic. This implies that both the two routers located in the main Data Centre (Cisco 3825) and the two routers located in the back-up Data Centre (Cisco 3845 and Cisco 2851), are already configured to do so.

- In addition, the routers involved in the backbone infrastructure (located in the connection areas) are IPv6 capable as it was mentioned before. So far, only those routers involved in the connection between Ministries have been configured to support IPv6, but the extension of IPv6 to the rest of connected bodies (Autonomous Communities and Singular Entities), not involved in the pilot, should not be a problem, based on the experience acquired with the Ministries.

- Regarding switches, they are Switch Cisco Catalyst 3750E and 3750G, and they have no specific requirements for IPv6 management, since the use of IPv6 for managing devices

is out of the intended scope of the Spanish pilot, as the network will keep dual-stack capabilities and management can still be achieved by means of IPv4. On other hand, switches in connection areas have Cisco IOS c3750e-universalk9-mz.122-44.SE6, which is not IPv6 capable, so an update of the IOS is required to make them support IPv6 natively. This means that an important investment in new licenses is required to manage switches using IPv6.

In the case of MINETUR, the IPv6 networks are directly connected to the firewall PaloAlto PA-5050 which acts as a router, redirecting the traffic to the Cisco 3750 or 2960S switches (depending on the environment) where a VLAN is created only for IPv6 servers .

Turkish Pilot:

Throughout the pilot process, the next step after the addressing plan was configuring routers with IPv6 support. Since routers in the TURKSAT network (as well as other L3 devices) had IPv6 support, this step was not a challenging experience, as the routing protocols for external routing BGP has been configured for the defined networks. The address range 2A01:0358:4F00:0002::/64 has been allocated from Turk Telekom for interface connectivity and BGP configuration. BGP connectivity was established and the address range 2A00:1D58:0::/36 has been announced to the Internet. Similarly for the internal routing static routing had been deployed where necessary.

Static routing had been deployed on the connection between TURKSAT and the participating governmental agencies.

3.2 Affected Central IT Systems

German Pilot:

Out-of-band management networks can remain on IPv4 when systems with connections to the public internet become IPv6-enabled from obvious reasons.

Core infrastructure components cause harm only under rare circumstances when running the IPv6 protocol.

Monitoring systems like our beloved Icinga require often more than less work to have checks IPv6 aware, or to be able to differentiate between the operational state in IPv4 and IPv6. Several approaches for a unified setup of bilingual tests were found but not yet a take-this-and-

forget-the-problem solution could be identified.

Security with IPv6 is expected to become a challenge as the use of the protocol increases. The design has some features that can give a new flexibility. The practical usefulness of these features will have to show that it is worth the risks of non watertight implementations. The re-established respectively possible end-to-end connectivity requires new attention in security and network design. Ease-of-use functions like stateless DHCP or router advertisements also contain a misuse potential. Many more remarks can be given in the security field.

Spanish Pilot:

Regarding the Red SARA network, a comprehensive inventory of the different services mentioned has been conducted, and a deep analysis of the software is being performed to ensure compatibility with IPv6 services.

Public IP addresses have been configured in Internet firewalls to offer IPv6 services natively with associated IPv6 addressing. As it has been mentioned, it has been necessary to upgrade the software used on the Internet firewalls, though the appliance itself has been kept.

To offer the IPv6 services it has been necessary to deploy a new infrastructure dedicated only to support this service, which could be used as a shared service platform. A new cluster of servers based on Linux has been installed on the DMZ of Red SARA to host the different servers:

- NAT64 gateway
- Reverse Proxy
- DNS server
- Mail server

Firewalls located on the connections areas have also been configured to process IPv6 traffic, not only routing and filtering but also ciphering.

Currently, the IPv6 DNS service is provided through the SARA network, so accessing resources published on the network in IPv6 is possible.

Turkish Pilot:

Main central IT systems for the Turkish pilot can be considered as the DNS and the logging

systems, which are deployed and maintained within TURKSAT network. These systems had been already working before the project over IPv4. These systems are affected by the IPv6 transition as expected. These items are investigated and updates have been done as defined in the following sections.

3.2.1 DNS

German Pilot:

The operation of DNS Servers in a dual-stack IPv6-enabled environment is considered as production grade proven. The Citkomm primary DNS is productive and public available since Q1/2013. The Windows DNS is also ok as the tests in the LAN and application backbone testbeds acknowledged.

Spanish Pilot:

The DNS service in each of the connection areas is provided by means of BIND version 9.3.4-6, and BIND 9 fully supports all currently defined forms of IPv6 name to address and address to name lookups. It will also use IPv6 addresses to make queries when running on an IPv6 capable system.

To allow the access from pure IPv6 clients to DNS service, an IPv6 capable DNS server has been installed in the DMZ of Red SARA. This server has been configured as a slave for the different zones for which we are offering IPv6 services (that is, the zones where the IPv6-enabled e-Government services, such as administracionelectronica.gob.es, belong to). This server receives the zone files from the master servers used previously to serve these domains (that of course have had to be configured to do so). In these zone files it has been included the necessary AAAA records to allow the access of the clients using IPv6. At this moment, each domain using IPv6 services from Red SARA has its original name servers plus another one IPv6 capable, the one provided by Red SARA. To do so it has been also necessary to modify the list of NS entries at the registration authority (usually red.es).

Regarding MINETUR network, the DNS service is provided also by means of BIND. As it has been mentioned before, two ranges of IPv6 address are used to provide access through SARA network and from the Internet.

The domain eitv6.mitycia.es has been created to access the test environment of the eITV application with IPv6 protocol. It can be accessed only through the internal network and Red

SARA.

Turkish Pilot:

IPv6 support was added to the DNS servers by configuring IPv6 addresses and reverse DNS records in the respective NIC.TR servers.

3.2.2 DHCP

German Pilot:

Most of the network areas and components affected so far are working with static IP addresses. DHCP will be relevant for the local networks. Testbeds for such local networks have been installed and the DHCP service was one of first investigation points to get these networks ready for operation. See also chapter 9.

Spanish Pilot:

In connection areas, IPv6 is assigned statically, so DHCP is not used in Red SARA.

In the case of MINETUR, IPv6 is assigned through autoconfiguration so DHCP is not used either.

Turkish Pilot:

IPv6 address configuration is being made statically in Turkish pilot for the time being. Hence, DHCPv6 is not be deployed.

3.3 Further Affected Systems/Components

3.3.1 VPN

German Pilot:

The Citkomm WAN network uses VPN services as central infrastructure. Therefore, VPN is vital for the German pilot. The iWAN gateway has been enabled for IPv6 connectivity. These appliances base on Ubuntu Linux LTS distributions and use OpenVPN as one core component. The combination of used packages is performed in a manner useful for the special demands in the Citkomm wide area network and for the connected customers. The ability for IPv6 has been successful implemented for both: the network interface and the tunnel interface. So at this point, the pilot gateway implementation is able to support fully network connectivity for IPv4

and IPv6. To check the functionality even under WAN and productive conditions one gateway was installed in the testbed at Fraunhofer FOKUS in Berlin. This gateway now keeps a permanent connection to a central gateway at Citkomm.

When such a tunnel is brought up (or when it is finished from whatever reason) some scripts must be executed to publish the route to the OSPF system (or to revoke it). These scripts got extensions so they are now IPv6 aware.

Spanish Pilot:

In the Spanish pilot, Red SARA hosts a set of different VPNs. Among them, only the VPN that connects Ministries (National Government), Autonomous Communities (regional Governments) and singular entities (constitutional bodies and such) is within the scope of the pilot.

This VPN must be capable of establishing connections between the entities linked to Red SARA in both IPv6 and IPv4 protocols.

VPN tunnels between different entities connected to Red SARA are created by means of IPsec. VPN endings are located in external Firewalls of connection areas. These firewalls are based on Stonegate version 5.3.3, which support IPv6. IPsec tunnels for IPv6 are defined in a similar way as those of IPv4. It is needed to define both ends and the networks involved in the connection. As there is only one manager which centralise the configuration of all the equipment used in Red SARA, using only this centralised information the firewalls are capable to agree on the different encryption schemas and to negotiate the different IPsec Security Associations (SAs) needed for the communication to take place. Since the procedure is identical to that of IPv4, no significant problem has been found.

Turkish Pilot:

A VPN connection has been deployed in the backend implementation of the Turkish pilot between TURKSAT and other governmental institutions. VPN connections are finalized at the VPN box placed on the public institution side. NETAS CO. worked on this box as an R&D project. The work finished in 2013. VPN connection was being made over IPv4 IPsec before the deployment of PIB. By deploying PIB, IPv6 IPsec has been used natively.

3.3.2 Load Balancing

German Pilot:

Citkomm does not operate load balancer as special solution. Load balancing features are implemented in some server installations, e.g. WTS farms, but have not been investigated until now.

Round robin DNS as poor man's load balancer is considered as working, but not for WTS gateways on Windows 2012 server.

Spanish Pilot:

Regarding the Spanish pilot, in Red SARA load-balancers are not used. In the case of IPv6 access to web portals of public administrations, an IPv6 load balancing function is performed by the firewalls located in the DMZ of the connection between Red SARA and the Internet, so that incoming requests are sent to the appropriate server in one of the two data centres that host Red SARA Internet services. After going through the IPv6-IPv4 gateway, there are load balancers before the servers that host the e-Government web portals, but this balancing is performed in IPv4, once the IPv6 to IPv4 translation has been completed. This will be the approach used initially in the pilot to balance IPv6 traffic; reassessing it can be considered when the IPv6 traffic through Red SARA becomes increasingly significant.

In the case of the tests performed to assess the feasibility for a dual-stack platform, the load balancers before the PEPS servers (F5) were actually configured in dual-stack and therefore are able to do IPv6 balancing. Though there were initially some problems with the setting up of the system, and it was thought that they were caused by a wrong configuration of the balancers, at the end the problem was due to the MTU in the reverse proxies, as it has been previously described.

In the case of MINETUR, load-balancers are needed to send IPv6 traffic to the server farm and to act as IPv6/IPv4 gateway to the backend servers inside the internal network, and have been configured accordingly.

Turkish Pilot:

Load balancers have a critical importance in Turkish pilot since all servers are deployed behind them. Load balancers provide security and performance measurements for EGG. In the scope of GEN6 project, load balancers were updated successfully to support IPv6.

3.3.3 Monitoring

German Pilot:

Citkomm uses central monitoring services based on Icinga. Icinga offers IPv6 support, but most of the job is done by the actual test programs and scripts. Quite a bunch of them is contributed by the community. Fortunately, many of them are already IPv6 aware. Additional efforts in the form of more configurations as well as more tests to be performed leading to more load on the Icinga server result from the approach to check to operation of services per protocol separately.

One bad point is the fact, that the well known remote probe nrpe on the monitored server is not available as packets supporting IPv6 in the Linux distributions used at Citkomm site. This results in additional effort, because the packets have to be compiled from the sources each time until the pain leads to IPv6-enabled package in the Citkomm package repository. This is expected by the end of Q1/2014.

Spanish Pilot:

Because currently the IPv6 traffic to be monitored is very low (restricted only to the external connections to IPv6-enabled web portals), monitoring systems have not been fully adapted yet. IPv6 traffic is being supervised, as a temporary means, using the IPv6 logging capabilities of the firewalls.

Additionally, the reverse proxy service, required by the shared service platform for providing IPv6 connectivity to e-Government Web Portals, is also being monitored.

Regarding MINETUR, the PaloAlto firewall records the traffic to both IPv6 environments created: pre-production and production. Logs are recorded in real time and will be further processed.

Turkish Pilot:

TURKSAT has been monitoring IPv4 networks and services using different tools such as Nagios, NfSen and Microsoft Scom. These tools are also IPv6-enabled. Required configuration has been made for these tools such as IPv6 addresses for services on monitoring tools. No challenge has been experienced during this process.

In addition, there exists a management room where the network and the servers are being monitored 7/24. For instance, PIBs have on their own alert systems for physical intrusion.

3.3.4 Management

German Pilot:

The management for Citkomm data centre operates as far as possible out-of-band, using an own physical infrastructure. This infrastructure is out of the scope of the project and shall be continued with IPv4 only. Due to the isolated character of the network, this will not affect the pilots other activities.

Spanish Pilot:

Regarding servers in connection areas, central management services are provided by means of Dell Remote Access Controllers (DRAC) version 4. This version does not support IPv6 since it was included in version iDRAC6. They are not intended to be updated within the scope of the pilot, since they do not affect the capability of the network to support the provision of e-Government services in IPv6.

In the case of MINETUR, as the number of servers are not very big, they are managed locally.

Turkish Pilot:

TURKSAT network supports IPv6 for the time being. Servers and network appliances in the Turkish pilot are configured dual-stack. Therefore, the management of these devices can be made over both IPv4 and IPv6. Also monitoring software such as Nagios is deployed to ease the management of devices.

3.3.5 SNMP

German Pilot:

SNMP is not so much used in the Citkomm network. In the out-of-band management network IPv6 will not be seen during the next months.

And in this sense is the whole SNMP thing in this project: as no IPv6 only network is to be seen on Citkomm's horizon SNMP data can be fetched via IPv4 further on. The content of the SNMP data was not yet reviewed in relation to IPv6. Functional tests in the monitoring do not use SNMP for obtaining IPv6 service related information so far.

Spanish Pilot:

SNMP is currently used in Red SARA, together with other tools, to monitor the network and therefore all the nodes belonging to it support SNMP. Within the scope of the Spanish pilot it is not expected to use SNMP over IPv6, so the IPv6 support required for the hardware regarding SNMP is the capability to provide information about IPv6 parameters when it is queried by the monitoring system using IPv4 as transport protocol.

Though the configuration of the SNMP systems to deal with IPv6 parameters has not been done yet, once the upgrading of the connection areas has been completed, it is intended to assess the current operation procedures based on SNMP in order to determine which modifications would be required in the SNMP configuration due to the use of IPv6 traffic.

Regarding MINETUR, no SNMP management is used in IPv6 environments.

Turkish Pilot:

SNMP is currently used within TURKSAT network, where EGG is deployed, for monitoring the IPv4 network. SNMP is planned to be used for the IPv6 network as well.

On the backend communication which has been established between TURKSAT and the service provider institutions SNMP is not being used and it is not planned to be deployed within the pilot.

4 SECURITY ASPECTS OF USING IPV6

This chapter documents the security aspects of running an IPv6-capable network for e-Government services. Some of these aspects originate from the involved devices (e.g. firewalls), others from the use of IPv6 addresses Finally, we emphasize that also non-technical aspects such as training for technicians as well as other employees are needed to keep the same level of security, as exists nowadays in an IPv4-only network environment.

German Pilot:

The autoconfiguration features of IPv6 will require some more attention for the things going on at the network level. Router discovery and address autoconfiguration may produce unexpected results and security holes in environments with unattended but IPv6 capable and enabled systems. Many systems deployed over the last years came with IPv6-enabled out of the box. In addition, there might be some test systems that received not so much attention so far as they could not connect to the world via IPv4. That could change with an IPv6 router on the network segment and SLAAC in operation.

Also the by default enabled IPv6 tunnels from Microsoft system attract more attention now. Other areas are better known from IPv4 and covered in the next sections.

The IPv6 implementation of OpenVPN is very similar to that in IPv4. This means that all routes and tunnels can be configured for IPv6 in a similar way as for IPv4.

In fact the dual-stack approach minimizes the effort for transition of security concepts, as in the process all security considerations can be transferred to IPv6 as a one to one image. As for IPv6 sometimes other tools and syntax must be used this lowers the risk of confusion and therefore for security gaps.

Spanish Pilot:

The main security aspect of using IPv6 is the need of configuring properly the IDS/IPS systems and the firewalls. This is explained in more detail later.

Turkish Pilot:

In the case of the Turkish pilot, IPv6 support means there will be a dual-stack network over which both IPv4 and IPv6 traffic will be flowing. It is assumed that security and performance

issues will increase in a dual-stack network since the network will be a target both for IPv4 and IPv6 attacks. In addition, routers and L3 devices should be able to deal more traffic when they are run dual-stack. It is sure that all security and monitoring appliances should be IPv6-enabled and rules and access control lists should be updated appropriately.

Recently several different types of attacks have been observed over IPv6. For the time being, simple attacks like SYN flood are the most common types.

4.1 Firewalls

German Pilot:

Of course, the firewalls had to be made IPv6 aware. In the case of Citkomm's Linux based firewalls this was an issue of updating the firewall management system running fwbuilder. Then new definitions and rule sets with IPv6 sections had to be created. The proper operation of the rule sets had to be verified.

The new protocol with its new special options and features will for sure need more attention as it comes in wider use. It can be expected that many new issues show up on the security level as IPv6 traffic will make up a greater share of the whole Internet traffic.

Fortunately, all rule sets are managed centrally. Therefore, the maintainers for the firewalls will have to be trained before the rollout of IPv6 to more than pilot customers will start.

Spanish Pilot:

As expected, firewalls have been one of the elements more impacted in the deployment of IPv6 in Red SARA. In some cases (border firewalls accessing Internet) it has been necessary to upgrade software versions (Fortigate 4.0 to Fortigate 4.0MR3 with the patch 441), while in others (connection areas) it has been enough to define new rules and elements to fulfil the needs.

As it was mentioned previously, firewall configuration has been changed to fulfil the new requirements in two areas:

- Addressing and rules
- IPsec tunnels

IPv6 stack is completely different from the IPv4 one. If the firewall needs to process IPv6 traffic, it is necessary to translate the IPv4 rules used previously to the new addressing schema (if not all, at least those related to IPv6 traffic). Depending on the product used to implement the firewall service it can be so tedious. In the case of Red SARA, where all the traffic crosses the network encrypted using IPsec tunnels, it is also necessary to define new tunnels to accommodate the new networks.

In the case of MINETUR, two firewall rules have been added (one per environment) to allow only IPv6 traffic through HTTP and HTTPS to the eITV service.

Turkish Pilot:

Through the pilot, all security devices (firewalls, IDS/IPSs etc.) have been configured to support IPv6 deployed in the TURKSAT network. Rules and lists defined in these devices have been updated according to the TURKSAT IPv6 network structure.

An increase in security incidents is expected as the IPv6 traffic increases. An important point is that network and system administrators should be aware of this fact.

4.2 Intrusion Detection/Prevention Systems

German Pilot:

Not to be published

Spanish Pilot:

As far as Red SARA is concerned, one point to highlight is the deployment of the new 2.9 version of Snort. Snort is the open-source IDS/IPS used in Red SARA connection areas[1], and it reports data to CCN-CERT through the logging aggregator. This new version is able to analyse IPv6 traffic.

In the case of MINETUR, PaloAlto firewall has IDS capabilities. We are using these capabilities to block threats although no specific changes have been made for IPv6 environments.

[1] For more information, see http://www.snort.org/

Turkish Pilot:

Several IDS/IPS instance have been deployed within TURKSAT network. These include both hardware and software solutions. All instances are IPv6-enabled and the rules are updated to identify anomalies and attacks on the IPv6 network.

4.3 Application Layer Gateways (ALGs)

German Pilot:

As far as this is related to Citkomm, ALGs and Proxies are considered as one class of devices. The remarks to the proxies can be found there.

Spanish Pilot:

Application Layer Gateways (ALG) are being used in the Spanish pilot in the shared service platform for providing IPv6 access to e-Government websites, by means of reverse proxy servers.

To implement this access to web services using IPv6, Red SARA has installed a reverse proxy server with dual-stack. The proxy is listening in IPv6, waiting for connections from Internet. Once it receives a connection, it finds in the HTTP 1.1 header “Host:” the final service the client is trying to connect to. It uses this information to connect to the correct original server (“parent”) using IPv4 via Red SARA. Once it has received the information, it returns that information to the original client using IPv6. That way, an IPv6 client (who is not aware of all the technical procedures involved) can connect to a service offered only by means of IPv4.

Turkish Pilot:

For the status of the Turkish pilot, there is no deployment of ALGs.

4.4 Proxies

German Pilot:

All affected proxies (squid, nginx, apache in proxy mode) had to be approved for IPv6 operation with or without possible IPv4/IPv6 translations. Subsystems like virus scanners must be included in these tests.

Moreover, especially all filter rule sets have to be checked for IPv6-awareness.

A special point is the Citkomm made local administrator's interface of the iWAN systems. This GUI still has to be extended to become IPv6-enabled and to offer the same opportunities for IPv6 as in IPv4.

Spanish Pilot:

Red SARA provides proxy services to the institutions that are connected to its network. To achieve this, there are proxy servers running in the service cluster located in the connection areas between the institution and Red SARA, which can act both as direct and as reverse proxies.

These services are provided by means of the open-source software Squid 3.1.8[2], which supports IPv6.

Squid is also used as gateway for IPv6 clients to IPv4 world (see previous section about ALG). This software, among its capabilities, has the option to act as reverse proxy or accelerator, and it is installed in the Internet access DMZ of Red SARA with dual-stack configuration, using:

- an IPv6 address to communicate with IPv6 Internet clients, and
- an IPv4 address to talk to e-Government web portal servers.

In this way, as has been described before, it is able to act as bridge between IPv4 portal servers and IPv6 requests from citizens.

Turkish Pilot:

No proxies have been deployed in Turkish pilot as an administrative decision.

4.5 Other Security Aspects

Spanish Pilot:

Regarding NAT64 security issues, a security policy forbids any kind of traffic from the Internet to go through SARA network. Therefore, when using NAT64 to enable IPv6 connection to web portals, traffic from the Internet is routed to IPv6 public addressing, so no data is transmitted through the SARA network in this case.

[2] For more information, see http://www.squid-cache.org/

In the case of MINETUR, a log analyser has been installed. The firewall logs are sent to this system and are analysed and correlated to detect threats and attacks.

5 OUTLOOK

In 2013 and beyond, the GEN6 project's national pilots continue to work on migration of additional parts of their infrastructure to IPv6. This section gives an outlook on the most prominent migration work done and planned for each pilot **regarding the generic services with IPv6**.

5.1 German Pilot

The transition of the local networks (Citkomm, friendly customer) as well as the testing of further applications will be the main focus for the remaining project time in the German pilot. The preconditions for application testing are fulfilled now; the testbeds have seen their first real uses. As the client networks become IPv6-enabled the first applications could really be produced via IPv6.

As next steps afterwards further network areas can be set productive for IPv6, to extend the coverage to more network segments.

5.2 Spanish Pilot

For the remaining time of the project, the work foreseen in the Spanish pilot will be distributed between two action lines:

- IPv6 enablement of public administrations Web Portals through shared services. Apart from the initial approach of developing a shared service located in Red SARA for making e-Government portals IPv6 accessible, after the successful tests for evolving to dual-stack the infrastructure that supports MINHAP services, this new approach is intended to be also used. This way, e-Government services operated by MINHAP would be made IPv6 ready by means of this dual-stack platform, while the IPv6-IPv4 gateway would provide IPv6 readiness to the e-Government services operated by other government units, as a shared service in Red SARA. In the first case, among the MINHAP's services that are being considered to be made IPv6 ready, it is the Spanish Single Point of Contact for the Service Directive (www.eugo.es). In the second case, some tests are already being performed with the Ministry of Justice for making their portals IPv6 ready, and an agreement regarding the architecture of the solution with the Ministry of Defence has been reached, so it is expected to be also tested in the near future.

- Adaptation of MINETUR services to IPv6. In the future months, development works to IPv6 enable eITV application will continue, as well as the preparation of the MINETUR network to support IPv6 connections to this service. Once the development has ended, the IPv6 compatible version of eITV will be deployed and operated.

5.3 Turkish Pilot

Turkish pilot consists of two main phases. 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.

Second phase of the project is to make the backend communication between TURKSAT and the service provider governmental institutions IPv6-enabled. The communication between TURKSAT and two participating institutions (SGK and PTT) has been made IPv6-enabled by the end of second year of the project. This has been achieved by deploying Public Integration Boxes (PIBs) on the end points of the communication.

As the next step throughout the project the IPv6-enabled components will be monitored for both security, performance and reporting purposes. Also pilot participants will be focusing on dissemination activities which are planned to cover various governmental institutions both in national and international level.

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.

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 generic services of an IPv6 landscape.

The next deliverable in this series D3.6.4 will focus on services that need customized application and devices such as, custom written monitoring services, scripts, in-house developed gateways (VPN, AAA), legacy programs that developed and need update, special hardware (SMS gateways, NAS devices etc.) and any other stuff that is lack of commercial update support.

7 FIGURE INDEX

8 TABLE INDEX

No table of figures entries found.