Title:	Document Version:
Deliverable D3.6.1 **eGovernment Services with IPv6**	1.0.0

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

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/12/2012	07/02/2013	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:
Carsten Schmoll, Joachim Kaeber	FRAUNHOFER	WP3

Authors (organisations):

Emre Yüce (ULAKBİM), Carlos Gómez Muñoz (MINHAP), Antonio Skarmeta (UMU), Carsten Schmoll (Fraunhofer FOKUS), Joachim Kaeber (Fraunhofer FOKUS), Martin Krengel (Citkomm)

Abstract:

This document is the first one in a series of deliverables documenting the progress of 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 networks.

Keywords:

IPv6, eGovernment, 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	29.10.2012	Document creation	Carsten Schmoll (FRAUNHOFER)
v0.2-0.4	12.11.2012	revised TOC	Carsten Schmoll (FRAUNHOFER)
v0.5	28.11.2012	Turkish pilot added	Emre Yüce (ULAKBİM)
v0.5.1	04.12.2012	Spanish pilot updated	Carlos Gómez Muñoz (MINHAP)
v0.5.1	04.12.2012	German pilot updated	Martin Krengel (Citkomm)
v0.5.2-3	05.12.2012	minor editorial corrections	Carsten Schmoll (FRAUNHOFER)
v0.5.2-3	13.12.2012	minor editorial corrections	Antonio Skarmeta (UMU)
V0.6	20.12.2012	Integration of contributions from Turkish team, added table and figure titles	Joachim Kaeber (FRAUNHOFER)
V0.6.4	08.01.2012	Formatting review and some small corrections.	Carsten Schmoll (FRAUNHOFER)
V0.6.5	11.01.2013	Additional small revision	Joachim Kaeber (FRAUNHOFER)
V0.7.0	15.01.2013	Inclusion of final contributions from Turkish team	Joachim Kaeber (FRAUNHOFER)
V0.7.1	18.01.2012	Completing German pilot	Martin Krengel (Citkomm)
V0.7.2	21.01.2012	Accepted most corrections from gabriela.gheorghe@uni.lu (verbatim), leaving comments in the document. Integrated corrections from emre.yuce@tubitak.gov.tr	Joachim Kaeber (FRAUNHOFER)
V0.8.0	31.01.2012	Inserted remarks and corrections from the Spanish team.	Joachim Kaeber (FRAUNHOFER)
V1.0.0	06.02.2013	Final Polish; ready for delivery	Joachim Kaeber (FRAUNHOFER) Uwe Holzmann-Kaiser (FRAUNHOFER)

Disclaimer

Executive Summary

This document gives an overview of the current state of three national GEN6 pilots. For each pilot it describes its respective approach to the transition, including address and network planning, and the envisaged transition process. Furthermore we provide for each pilot information about affected components, experiences gained during the transition process and a description of test to verify the successful transition.

This deliverable should be seen as a first snapshot of a living document. Its successors will cover more aspects and details as the pilots progress.

Table of Contents

Table Index *9*

1 Introduction *10*

1.1 General approach to IPv6 eGovernment services **10**

2 Network architecture and structure *11*

2.1 Upgrade of external connectivity **11**

Figure 2 – German Pilot Architecture *14*

Figure 3 – Turkish Pilot Architecture *16*

2.2 IP Addresses **16**

2.2.1 Allocation and assignment 17

2.2.2 Planning (for the internal subnets) 18

2.2.3 Address configuration 24

2.2.4 Address management 25

2.3 Network planning and/or (re-)design **25**

3 Transition to IPv6 ..... *27*

3.1 Chosen approach **27**

3.2 Planned order of changes due to transition **28**

3.3 First successfully moved components **30**

3.4 Enabling IPv6 in components **33**

3.4.1 Practical tests 33

3.4.2 Experiences and pitfalls 35

4 Affected network elements *37*

4.1 Routers and Routing **38**

4.2 Affected central IT systems **39**

4.2.1 E-Mail 39

4.2.2 DNS 40

4.2.3 NTP 41

4.2.4 DHCP 41

4.2.5 Logging 42

4.2.6 Others 42

4.3 Further affected systems/components 43

4.3.1 VPN 43

4.3.2 Load balancing 44

4.3.3 Printers 44

4.3.4 Monitoring 45

4.3.5 Management 46

4.3.6 SNMP 47

5 Security aspects of using IPv6 48

5.1 Firewalls 48

5.2 Application Layer Gateways (ALGs) 49

5.3 Proxies 49

5.4 Use of secure protocols 50

5.5 Other security aspects 51

6 Link to system requirements 52

6.1 Assessed basic technical requirements (so far) 52

6.2 Assessed extended technical requirements (so far) 52

7 Outlook 54

7.1 Spanish Pilot 54

7.2 German Pilot 55

7.3 Turkish Pilot 58

8 Conclusions 59

Figure Index

Figure 1 – Spanish Pilot Architecture (RED SARA) *13*

Figure 2 – German Pilot Architecture *14*

Figure 3 – Turkish Pilot Architecture *16*

Figure 4 – Spanish Pilot: SARA Architecture #1 ..... *18*

Figure 5 – Spanish Pilot: SARA Architecture #2 ..... *19*

Figure 6 – Spanish Pilot: Connecting Area diagram *20*

Figure 7 – Spanish Pilot: Reverse proxy approach for IPv6 enablement *31*

Figure 8 – German Pilot: test network infrastructure *57*

Table Index

Table 1 – Spanish Pilot: IPv6 adressing for Red SARA *20*

Table 2 – Spanish Pilot: IP assignment for servers *21*

Table 3 – Spanish Pilot: IP assignment for gateways *21*

Table 4 – Number of subnets in IPv6 networks *21*

Table 5 – Spanish Pilot: Use of differently-sized subnets *22*

Table 6 – Spanish Pilot: Data and voice IPv6 subnets *22*

Table 7 – Spanish Pilot: Data and voice IPv6 subnets #2 ..... *23*

Table 8 – Spanish Pilot: Data and voice IPv6 subnets #3 ..... *23*

Table 9 – Spanish Pilot: Used networking hardware *37*

Table 10 – Spanish Pilot: Basic services *38*

1 INTRODUCTION

This document is the first one in a series of deliverables documenting the progress of 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 networks.

1.1 General approach to IPv6 eGovernment services

The single most important aspect of the migration of an existing government service to IPv6 (or dual stack support) is business continuity. Therefore, and depending on the technical environment, different techniques are advisable to add IPv6-support to an eGov service.

One possible approach is to build an IPv4-only test bed first, which resembles as close as possible “the real thing”, and to work on migrating this test bed initially. The steps of this work will have to be well documented, and the knowledge gained in this process will be of invaluable help when the real server or service is going to be migrated later on.

2 NETWORK ARCHITECTURE AND STRUCTURE

2.1 Upgrade of external connectivity

This subchapter documents which steps have been taken or will be taken by the national pilots in order to get external IPv6 connectivity, either from an existing, already used provider or a new provider. This section shall also explain which types of IPv6 addresses (provider dependent or provider independent) were acquired and how access is realized technically (e.g. native, or via MPLS tunnel). If a pilot uses multiple providers for increased availability of external connectivity, then this chapter will also shortly highlight how the newly acquired IPv6 connectivity will integrate into the existing multi-provider setup.

Spanish Pilot:

The relevant eGovernment services within the scope of the Spanish pilot are the following:

- Web Portals operated by Spanish Public Administrations to be made IPv6 accessible through Red SARA.
- Business applications provided by MINETUR to be consumed by other administrative units outside the Ministry. In particular, the application chosen in the pilot for demonstrating IPv6 enablement of eGovernment services is eITV.

The Ministry of Industry, Energy and Tourism, in collaboration with MINHAP, provides the electronic ITV cards management service for its transition to IPv6.

This service will be published using IPv6 to the Ministry of Interior, MINHAP being responsible for the connectivity with the Ministry of Interior through the SARA network.

For the project to be accepted by the different partners, the availability, accessibility and integrity of the data through the IPv6 connectivity should be guaranteed. These guarantees are closely related to the GEN6 project in its respective Working Packages for monitoring and securing the network.

The eITV service consists of several functional modules with the aim of meeting the specifications required by law to control and verify motor-driven vehicles.

The application scope of the eITV service extends to the Ministries MINHAP, MINETUR and DGT.

A key requirement of the project is to provide the service in a completely transparent way to the communications protocol. SARA should be the network responsible for providing IPv6 connectivity to the services published by MINETUR with the DGT, whether it is accessed via IPv4 or IPv6.

In the Spanish pilot, two participants' networks are involved:

- Red SARA, managed by MINHAP (former MPTYAP), acting as the network that interconnects Spanish public administrations and provides a platform for IPv6 connectivity to Internet.
- MINETUR's (formerly MITYC) network, acting as the provider of IPv6 capable service oriented business applications to be consumed by other administrative units outside the Ministry.

Red SARA connectivity requirements are:

- Connectivity to the Internet.
- Connectivity to MINETUR's network.
- Connectivity to the network of the administrative units that are the users of MINETUR's services.
- Connectivity to the networks of the administrative units that want to make their web portals and/or other services accessible through Red SARA using IPv6.

MINETUR's network connectivity requirements are exclusively related to the need of connectivity to Red SARA.

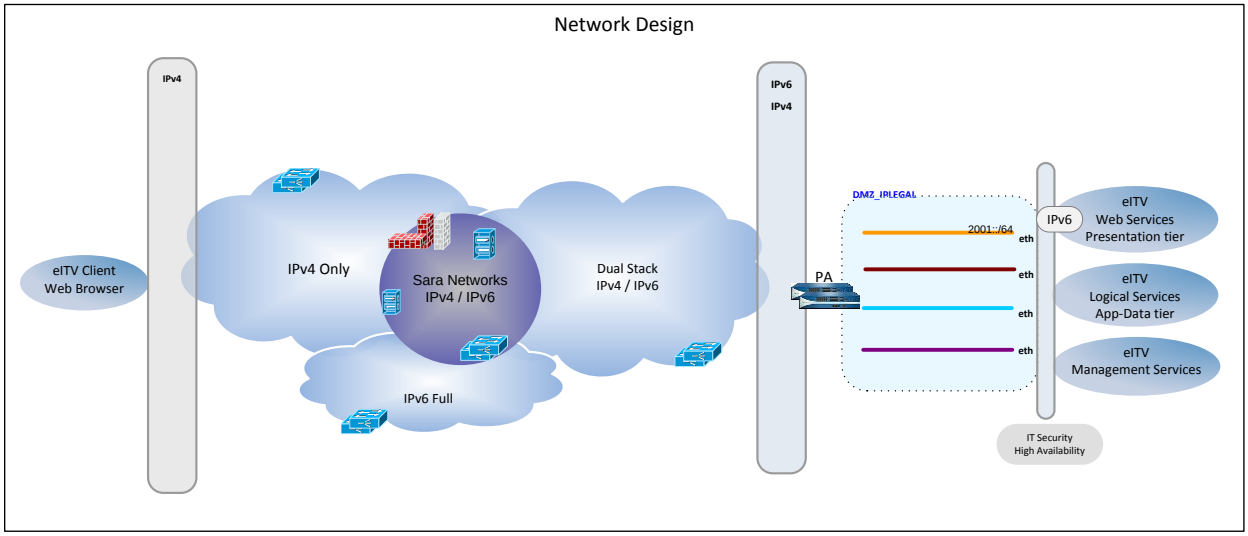

Figure 1 – Spanish Pilot Architecture (RED SARA)

Therefore, the external IPv6 connectivity of the pilot lies in the connection point between Red SARA and the Internet. Currently this connection point is IPv6 enabled, by means of the IPv6 service provided by the telecommunications provider of Red SARA. More details about this connection point are given in section 4.1 regarding routing.

It must be noted that in the Spanish pilot increased availability of external connectivity is provided by means of multiple links to the same ISP, connected to two different Internet Points of Presence through different access nodes, so no integration with a multi-provider setup is needed.

German Pilot:

The Citkomm network is currently connected to the Internet using two independent providers. Outside the GEN6 project, Citkomm started the transition of this network to an autonomous system in late 2011. At that time, the autonomous system was planned for IPv4 only.

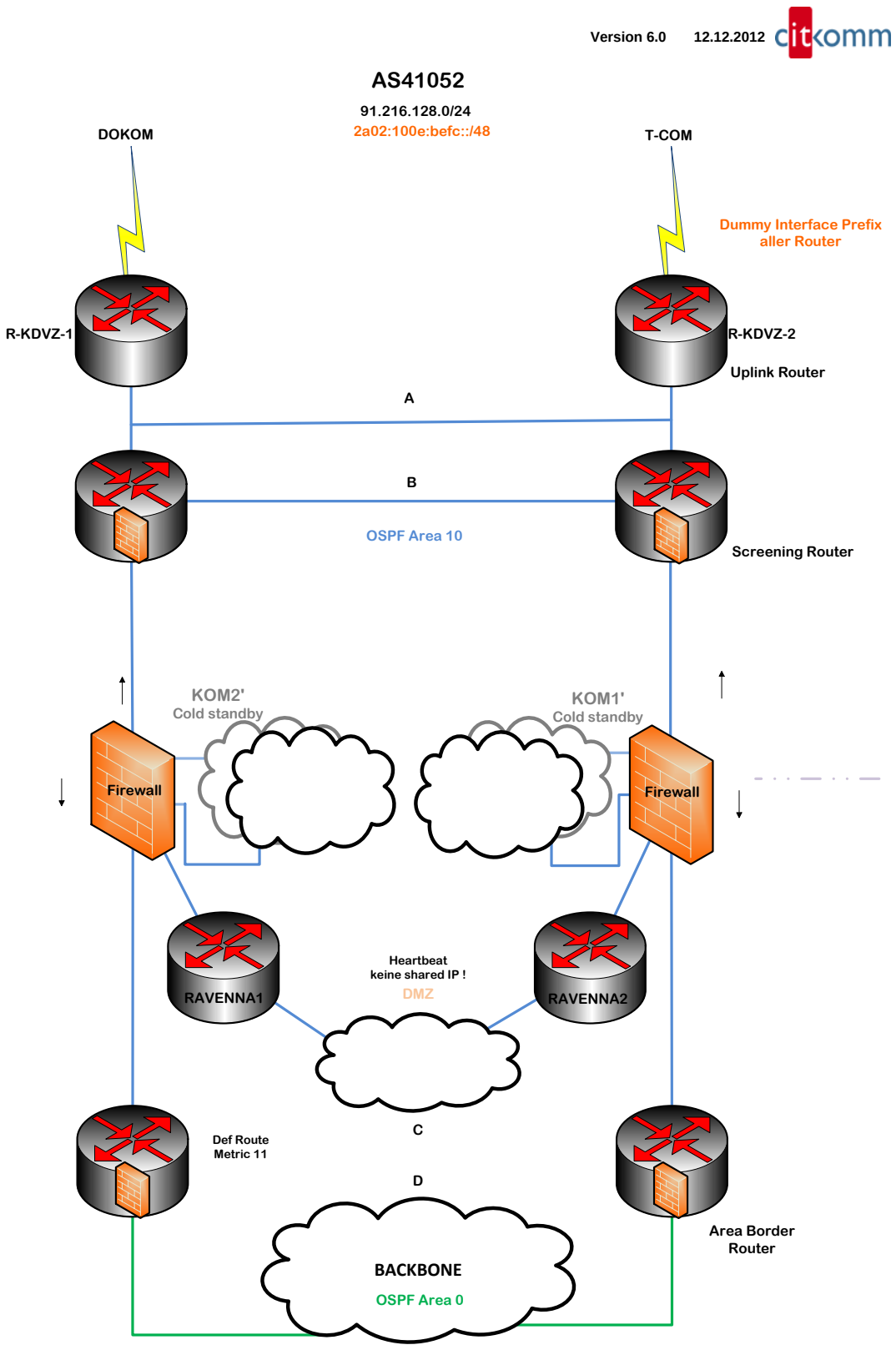

Figure 2 – German Pilot Architecture

In preparation of the “IPv6 Launch Day” in June 2012, shortly after GEN6 project kick off, Citkomm started discussing the IPv6 transition of the existing uplink lines. Several providers were asked whether they could provide IPv6 connectivity using an IP address space from Citkomm. The national provider agreed, while the regional provider had no experience with IPv6 and offered plans for first activities more than one year ahead. This was a problem because one of the uplink providers for the autonomous system is DOKOM21, a regional provider, who also operates the edge routers of the Citkomm network. In further discussions DOKOM21 agreed to support Citkomm’s participation in the pilot. As a first step, IPv6 would be made available via the second uplink provider. DOKOM21 plans to enable their backbone network in later steps. Since of May, 2012, Pv6 connectivity is up and running in this single-homed fashion.

Next, a part of our access infrastructure dedicated for the pilot project was enabled for dual stack operation. All tests originally designed for verifying IPv4 connectivity finally also succeeded for IPv6 connectivity. The whole concept was then successfully reviewed by external security experts without any changes.

All communication between locations of Citkomm and Citkomm customers is operated via a VPN infrastructure. Citkomm uses a self-developed gateway product line, called iWAN. These gateways utilize OpenVPN, i.e. a TLS tunnelling mechanism. The same infrastructure is being used for the GEN6 pilot.

Turkish Pilot:

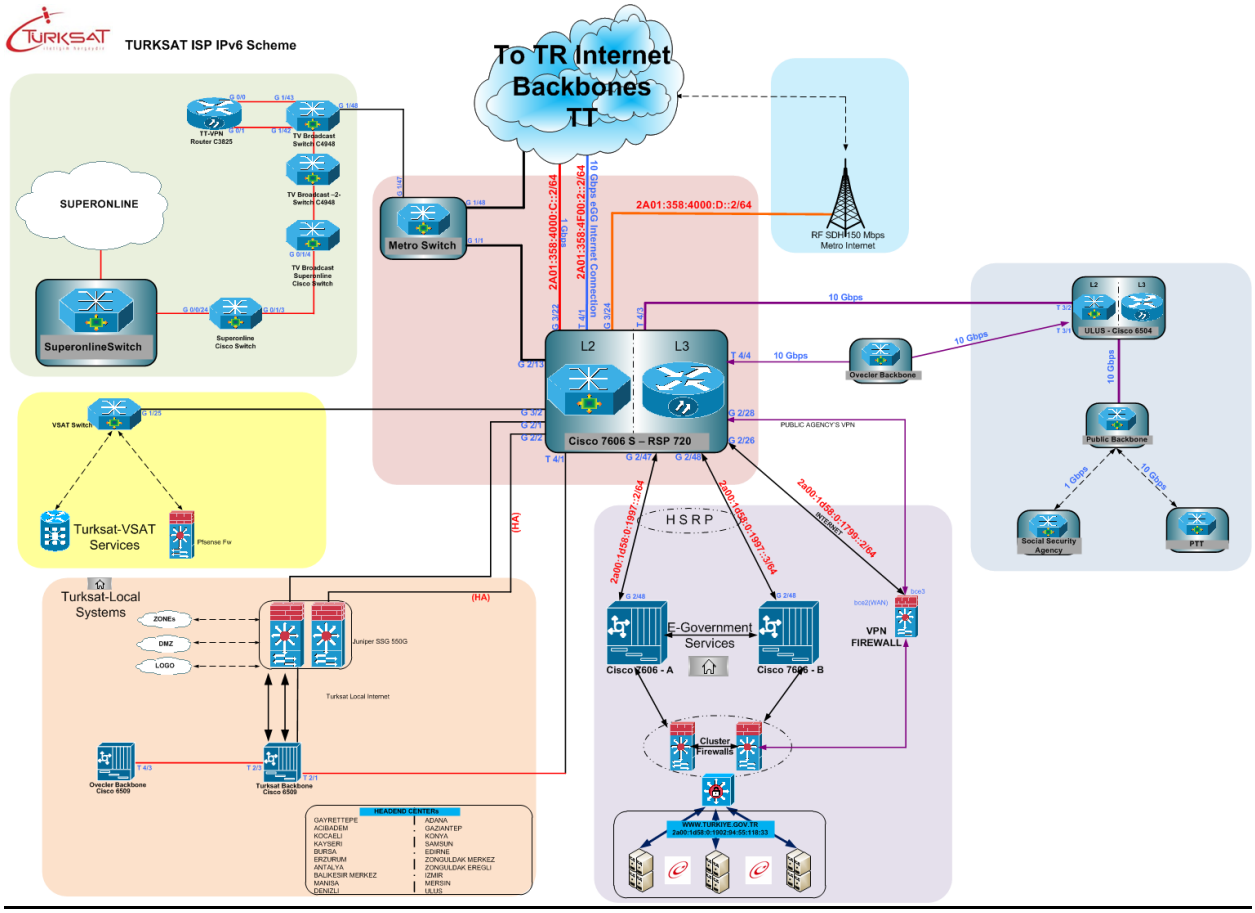

Figure 3 – Turkish Pilot Architecture

For the external connectivity of the Turkish pilot, there are two different cases to be considered: The first case is the external connectivity of a central Web portal to the global IPv6 network to provide IPv6 access for the customers. This connection has been established through the current service provider Turk Telekom by using a native IPv6 connection. The second case is the connection between TURKSAT and the participating governmental agencies (SGK, PTT and ULAKBIM). These connections will be established either using dedicated native IPv6 connections or via VPN on top of the current connection. Turk Telekom is the service provider also for these connections.

2.2 IP Addresses

This subsection will document how IPv6 addresses are being allocated, distributed across the internal networks, configured to local devices and servers and managed in each national pilot.

2.2.1 Allocation and assignment

Spanish Pilot:

In the Spanish pilot two different levels of Addressing Plans are required:

- The Spanish Public Administration Interconnection and Addressing Plan, which defines a common addressing space for Public Administration entities that are connected through Red SARA. At this level, the Addressing Plan allocates different prefixes to the connected entities, and gives some guidelines regarding address distribution. There is therefore only one Public Administration Interconnection and Addressing Plan.
- The organization's Addressing Plan, which distributes the allocated prefixes and assigns addresses to the different elements connected to the organization's network, according to the guidelines provided by the Public Administration Interconnection and Addressing Plan. At this level, there are therefore as many addressing plans as entities connected to Red SARA.

These specific plans depend on the common Plan, and will be developed as soon as the latter is finished. Therefore, in the case of the Spanish pilot a distinction has to be made regarding the mechanisms for the hosts to obtain IPv6 addresses:

- As far as Red SARA is concerned, IPv6 addresses will be assigned according to the IPv6 Addressing Plan for Red SARA
- As far as MINETUR network is concerned, IPv6 addresses will be assigned according to the IPv6 Addressing Plan for MINETUR

For the first point, at present, a study to update such plan taking IPv6 into account is coming to an end, and a first draft of the Addressing Plan has been developed. The intended approach is based on Red SARA becoming a Local Internet Registry (LIR) and receiving a /26 to /24 block to distribute it among the entities connected to Red SARA.

German Pilot:

Citkomm operates with a subset of the central address space, claimed by the German government from RIPE NCC. From the view of a provider, this address space has to be handled as provider independent.

Based on the national address plan, Citkomm received a /48 network for its own infrastructure. The allocated subnet will be fully (i.e. as one block) announced to the Internet. Further address

spaces will be made usable later for the customer networks.

Turkish Pilot:

The 2a00:1d58::/32 IPv6 subnet has been allocated from RIPE NCC. The subnet 2a00:1d58::/36 is reserved for the eGovernment Gateway Network and is exposed to the Internet by means of the AS47524 autonomous system .

2.2.2 Planning (for the internal subnets)

Spanish Pilot:

To better understand the addressing plan for Red SARA, some diagrams of the network are provided below:

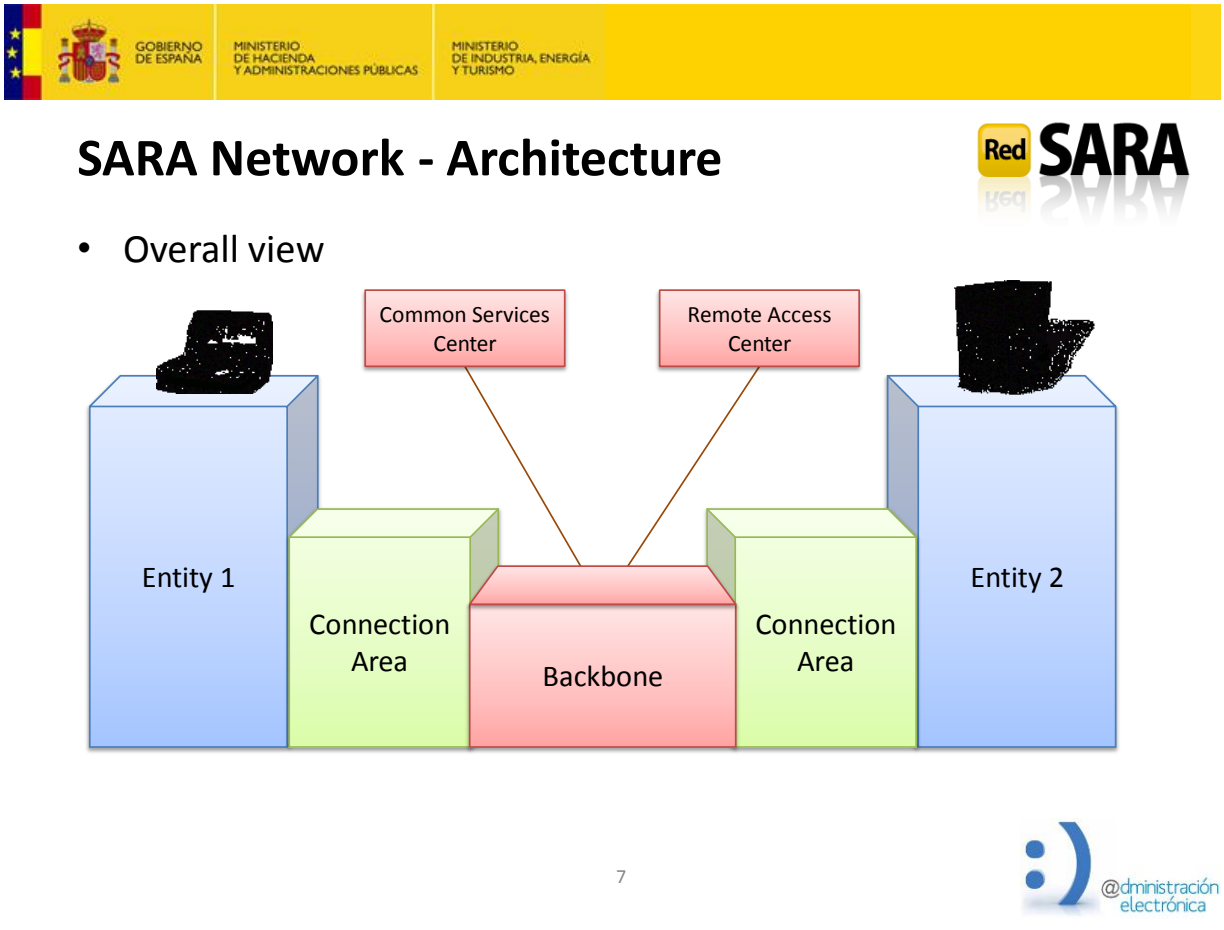

Figure 4 – Spanish Pilot: SARA Architecture #1

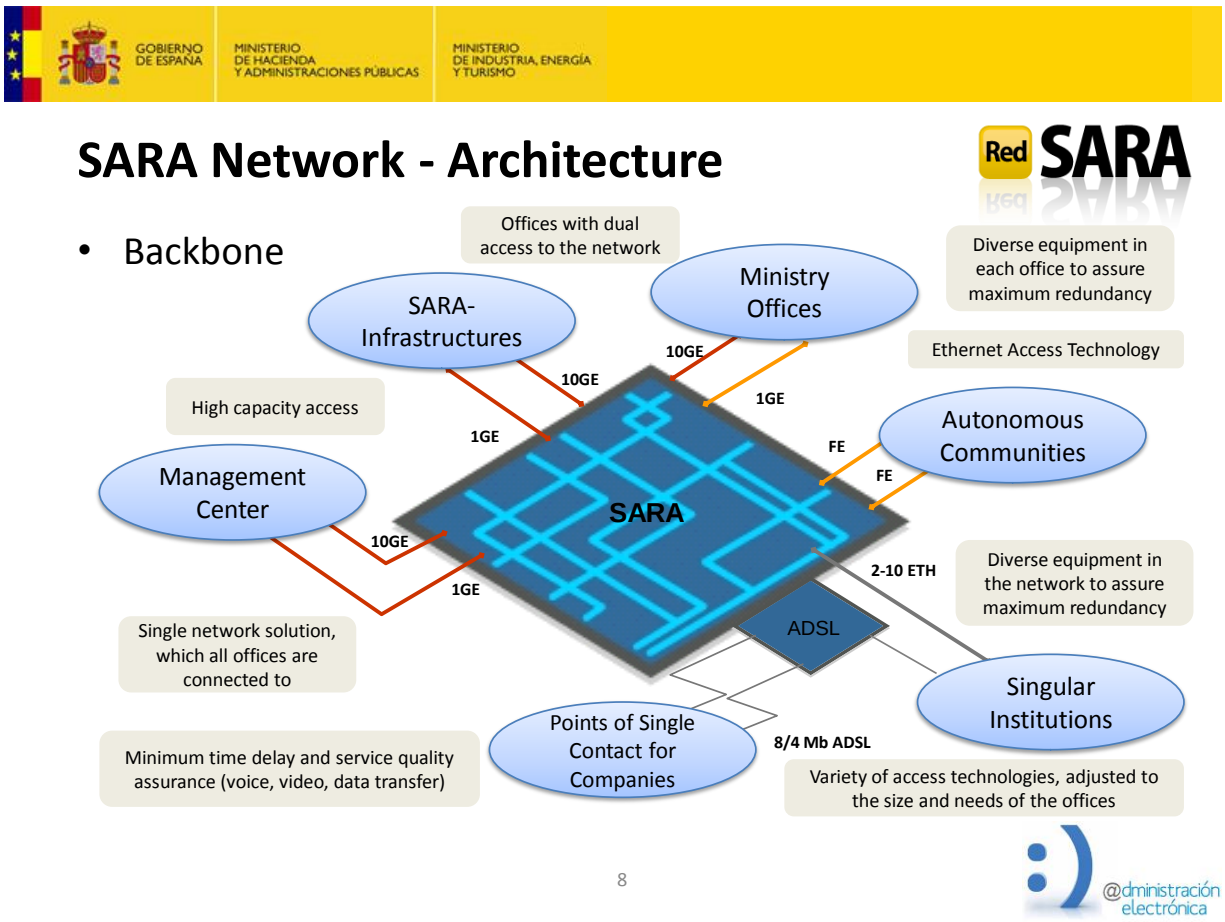

Figure 5 – Spanish Pilot: SARA Architecture #2

As can be seen from Figure 5, Red SARA is composed of a backbone network, which interconnects the networks of the different entities of the Spanish public administration linked to it, and a number of connection areas, which act as interfaces between the backbone and the entity network.

These connection areas are designed according to a DMZ outline, delimited by an external firewall (which connects with the rest of the Red SARA network) and an internal firewall (which connects with the entity). The first is supplied with the rest of the elements that compose the connection area, while the second is provided by the entity itself.

The elements of the connection area, apart from performing firewall functions, also host several basic services (proxy, mail relay, DNS, etc.), located in the service cluster, and security and monitoring services (IDS, data collection for statistics, etc.), located in the security cluster. This intermediate area (that is, this DMZ), can accommodate any equipment that the entity deems appropriate to be used for communication with the rest of organisms that make up the

Red SARA network.

A diagram of the connection area is shown below:

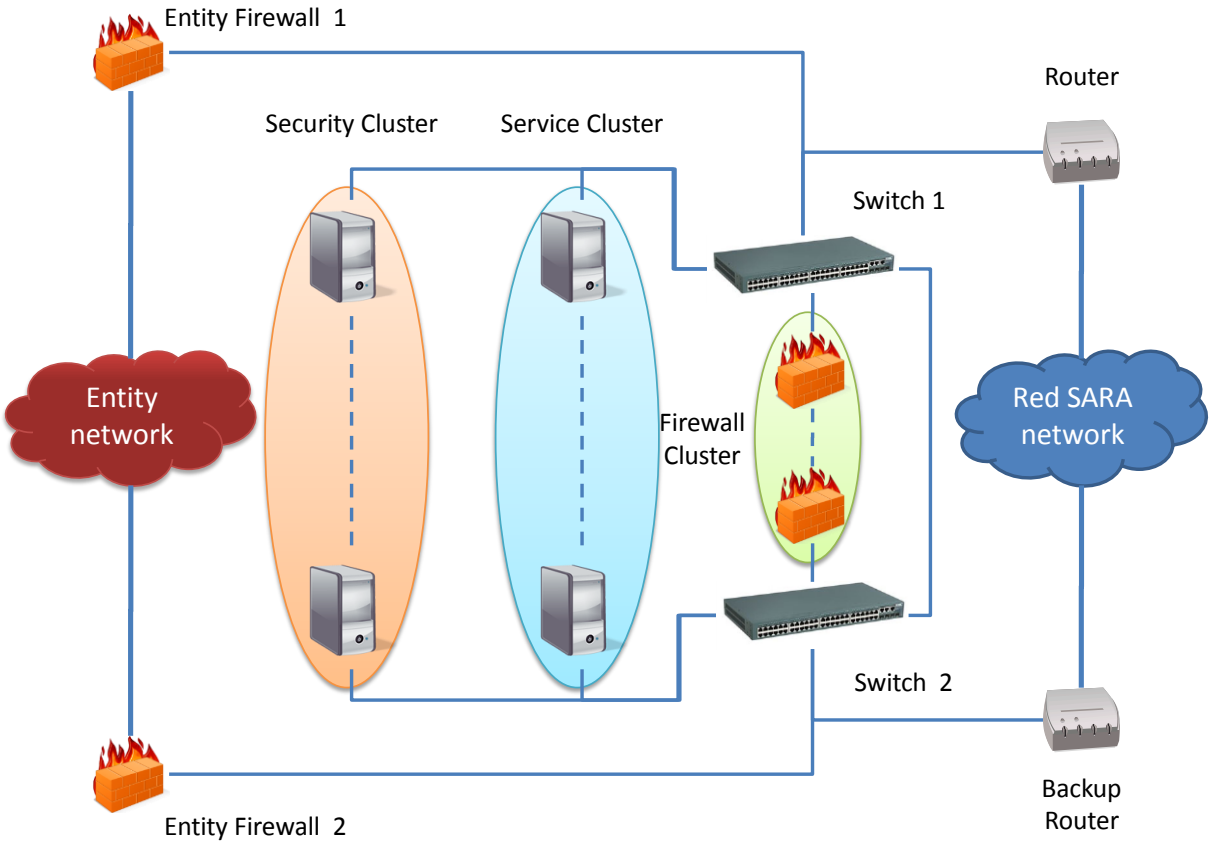

Figure 6 – Spanish Pilot: Connecting Area diagram

In this sense, and regarding the internal subnets of Red SARA, rules for addressing equipment in connection areas are being developed. For example, the IPv6 addressing for equipment required for IPv6 Internet connectivity is as follows:

Network	Number of hosts	1st Host	Last Host	Used for
2A00:2000:40A0:1::/64	18.446.744.073.709.500.000	2a00:2000:40a0:1:0:0:0:1	2a00:2000:40a0:1:ffff:ffff:ffff:ffff	DMZ
2A00:2000:40A0:FFFF::/64	18.446.744.073.709.500.000	2a00:2000:40a0:ffff:0:0:0:1	2a00:2000:40a0:ffff:ffff:ffff:ffff:ffff	Router-FW Segment

Table 1 – Spanish Pilot: IPv6 adressing for Red SARA

Inside the DMZ, the addressing assignment is as follows:

IP assignment	Equipment
.1	External FW,
.21	DNS,
.22	Mail Server,
.23	PROXY,
.24	REVERSE PROXY,
.30	Secondary DNS

Table 2 – Spanish Pilot: IP assignment for servers

Inside the Router-FW Segment, the addressing assignment is as follows:

IP assigment	Equipment
.1, .2, .3 .4	Router
.5	HSRP,
.6	FW iptable ipv6,
.7	NAT64,
.FF	Fw fortigate

Table 3 – Spanish Pilot: IP assignment for gateways

Regarding MINETUR internal subnets, MINHAP will provide to MINETUR a "./48" range of addresses offering MINETUR 65.536 networks to manage, according to the Spanish Public Administration Interconnection and Addressing Plan.

On the other hand, MINETUR keeps the option to use a private address range, in case of needing a confidential network without access to public networks for the internal management of the service.

The network masks that will be used to deliver IPv6 addresses in the infrastructure of the Ministry and Autonomous Bodies are as follows:

Network prefix	Number of Subnets
/48	65.536
/50	16.384
/51	8.192
/52	4.096
/54	1.024
/64	1

Table 4 – Number of subnets in IPv6 networks

The distribution of prefixes is made centrally from the Ministry to the dependent entities, even though this involves different sites. This is due to the fact that these entities need to go through the connection area of MINETUR to reach Red SARA, since this connection is unique for the whole Ministry.

MINETUR's initial addressing plan is going to be divided into 4 big address blocks:

1. The first /50 address block, will be devoted to links, DMZ and for delegation to MINETUR dependent Organisms, distributed as shown in the following table:

Network prefix	Description
/54	1.024 Networks for Links
/54	1.024 Networks for public DMZ
/54	1.024 Networks for protected DMZ
/54	1.024 Networks to deliver to Organizations
/52	4.096 Reserve Networks
/52	4.096 Reserve Networks
/52	4.096 Reserve Networks

Table 5 – Spanish Pilot: Use of differently-sized subnets

2. The Second /50 address block, will be devoted to the voice and data internal network of MINETUR's Central Services, distributed as shown in the following table:

Network prefix	Description
/51	8.192 Data Nets. To be elaborately developed when its need arises
/51	8.192 Voice Nets. To be elaborately developed when its need arises

Table 6 – Spanish Pilot: Data and voice IPv6 subnets

3. The Third /50 address block, will be devoted to the voice, data and specific applications internal network of the State Secretariat for Telecommunications and Information Society:

Network prefix	Description
/51	8.192 Data Networks. To be developed when needed
/51	8.192 Voice Nets. To be developed when needed

Table 7 – Spanish Pilot: Data and voice IPv6 subnets #2

4. The fourth /50 address block, will be devoted to data and voice services of MINETUR's organisms:

Network prefix	Description
/51	8.192 Data Networks. To be developed when needed
/51	8.192 Voice Networks. To be developed when needed

Table 8 – Spanish Pilot: Data and voice IPv6 subnets #3

The eITV national pilot will be accessible through the SARA network by using the protected DMZ address range.

The definitive IPv6 routes will be established when the IPv6 range requested to RIPE NCC will be delivered. This addressing plan is under review and may undergo changes as the project goes forward.

German Pilot:

Citkomm has started structuring the received address space of /48. Planning IPv6 addressed along existing network structures was not a viable approach.

The main reason is the need of several transfer networks. Due to the role of Citkomm, where the secure connection between several customer locations is a central service, there are numerous transfer networks between network components. Accepting the fact that also transfer networks with only two hosts need their own network with mask /64, the transfer networks claim an essential part of the whole usable address space.

Moreover, the structure of the server segments, based on the class C dimension in IPv4, can be restructured with an addressing capacity of 64 bits.

Turkish Pilot:

TURKSAT consists of four operating large network, namely:

- eGovernment Gateway
- Satellite Operations (VSAT, TV and radio streaming, etc.)
- TURKSAT Local Network Operations
- Cable TV and Internet

For the business level and the different Network Operation Centres, the IPv6 prefix has been divided into four /36 subnets:

1. for eGovernment Gateway Datacentre (2a00:1d58:0::/36)
2. for VSAT (2a00:1d58:2000::/36)
3. for TURKSAT Local Services (2a00:1d58:1000::/36)
4. for Cable TV and Internet (2a00:1d58:8000::/36)

2.2.3 Address configuration

Spanish Pilot:

Regarding the Spanish pilot, in the case of Red SARA, the network architecture is based on several connection areas, each of them with a different prefix, which includes a limited set of hosts running network services such as DNS, proxy, etc. Due to this, IPv6 addresses in Red SARA network will be assigned using manual/static configuration.

Therefore, at present, equipment using IPv6 in Red SARA, such as the one required to support the provision of IPv6 connectivity services to web portals, has been configured statically.

In the case of MINETUR's network, IPv6 addresses will be provided by Red SARA, according to the Spanish Public Administration Interconnection and Addressing Plan. Address assignment will be performed statically in two steps:

- Initial assignment using auto-configuration
- Final allocation with static IP address assigned in the previous step

German Pilot:

Mechanisms for the address configuration have not been approved in the pilot until now. All infrastructure components examined so far only need static addressing.

For the transition of the local networks, a testbed will soon be released to run first tests. At the moment, we expect to use dynamic IPv6 addresses based on the auto-configuration mechanism.

Turkish Pilot:

Static IPv6 addressing is used in the TURKSAT network rather than automatic addressing methods. Static addressing makes logging and management of IPv6 addresses feasible. Due to legislations in Turkey, IP addresses of hosts should be logged.

2.2.4 Address management

Spanish Pilot:

In Spanish Pilot, address management is performed according to the Spanish Public Administration Interconnection and Addressing Plan.

This plan will define a common addressing space for Public Administration entities that are connected through Red SARA, allocate different prefixes to the connected entities, and give some guidelines regarding address distribution.

German Pilot:

No tool has yet been planned for address management. The IPv4 addressing plan of the area of networks will be documented in Excel tables. The subnets themselves are documented in plans concerning one ore few subnets each.

Turkish Pilot:

There is no commonly defined address management scheme in Turkey for IPv6. In general, governmental institutions manage their IPv6 address blocks in parallel to their IPv4 address blocks. Also in this phase, institutions may consult with more experienced institutions such as ULAKBİM.

2.3 Network planning and/or (re-)design

Spanish Pilot:

Apart from addressing, new planning or re-designing, , has not been required in the Spanish pilot.

German Pilot:

At the WAN level, the transition to IPv6 will not force any redesigns. At the LAN and backbone area, the design concept can be varied, especially due to greater subnet dimension. Because this will affect further issues, especially security, we are currently considering subnet redesign.

Turkish Pilot:

No major network changes are needed since the network devices used in TURKSAT supports dual stack.

3 TRANSITION TO IPV6

This chapter documents the overall chosen high-level decisions concerning the introduction of IPv6 in each national pilot. Per pilot it will motivate the taken decision on how IPv6 will be introduced (e.g. in parallel, new networks, or inside existing ones), what are the steps taken to do so, from a top-down perspective and which aims have already been achieved (and how). In this part of the deliverable also the already found pitfalls in these works performed are documented.

3.1 Chosen approach

Spanish Pilot:

The Spanish pilot envisages three complementary lines of action with different approaches:

- The upgrade of Red SARA so that it can transport IPv6 natively, allowing therefore IPv6 communications between administrative units. This line is approached by means of dual-stack compatibility of elements in Red SARA.
- The implementation of a transition mechanism that allows Public Administrations to offer online services accessible by means of IPv6, based on a shared service approach. This line is being tackled by means of IPv6-to-IPv4 translation, using a Reverse Proxy and NAT64 equipment located in Red SARA's Internet access.
- The evolution of the MINETUR network so that it can provide native IPv6 services (eITV application) to be consumed by other administrative units (DGT, Directorate General for Traffic). This line is being approached by building an IPv6-native infrastructure.

In this way, 3 different approaches are being performed and expertise about all of them is being acquired.

Specifically, in the case of MINETUR's network the proposed solution consists of a dual stack system, allowing both IPv4 and IPv6 address publication.

In a first stage, native IPv6 will be produced, being accessible only through IPv6. This stage foresees an access only through the SARA network as an IPv4-only way of communication.

In a second stage, the architecture will be based on dual stack. It will allow access through both protocols and publish them to outside public networks. This will be a restricted access by way

of a failover system in case the DGT is not able to reach internally the IPv6 address through the SARA network.

The functional design achieves high availability and accessibility needs, key requirements demanded by MINETUR for a critical access system, with a high availability of 99.9999 % defined in the ANS of the service.

German Pilot:

Currently, all network components are based on dual stack. We expect this to be also the final solution, as most application servers are not available as cluster systems, which would open up the possibility to run some of them as IPv6 only systems. To avoid further effort separating or duplicating the systems on the application level, these servers are best running dual stack.

For the local networks dual stack is also the best choice, because it will not be possible to migrate all existing applications.

Turkish Pilot:

Through the TURKSAT network, network devices support both IPv4 and IPv6 at the same time. This leverages the deployment of dual stack networks. At this stage, no IPv6 only network is needed. This is valid for the connection between TURKSAT and the participating governmental agencies. There exists a connection between these points and through the pilot this connection will be made dual stack.

3.2 Planned order of changes due to transition

Spanish Pilot:

In the case of the Red SARA network, several network elements need to be examined:

- First, the backbone of the network, as well as the links connecting the institutions' sites to this backbone, must be upgraded to carry IPv6 traffic. During the pilot, and working together with the telecommunications provider, the network requirements to support this will be defined, and a piloting IPv6 infrastructure will be deployed through the backbone and through the links connecting MINETUR and MININT (Ministry of Home Affairs, which DGT belongs to) to the backbone.
- Second, the equipment located in the connection areas of MINETUR and MININT must be turned into dual-stack, so that it can handle both IPv4 traffic and the future IPv6

traffic that will be generated once the eITV service provided by MINETUR has been evolved to allow native IPv6 connections. Since all the connection areas follow a common architecture, the experience gained by the upgrading of these two connection areas can be easily replicated to the rest of the network?, allowing Red SARA to provide IPv6 connectivity to all the entities connected to it.

Additionally, Red SARA provides connectivity through? the s-TESTA network to the whole of the Spanish public administrations, by means of the s-TESTA connecting point located in the Remote Access Centre of Red SARA. Therefore, to support the cross border pilots envisaged in WP4, some actions, currently under study, have to be performed in the equipment responsible for managing the information exchange between Red SARA and s-TESTA. In this sense, MINETUR will also configure its network in order to reach s-TESTA through Red SARA using IPv6.

In the case of MINETUR's network, the changes to be made in large blocks are as follows:

Adaptations by the development team

1. Set up a complete IPv6 development environment.
2. Develop a new component of environment adaptation that allows the access to the service in a transparent way in any of both protocols IPv4 and IPv6. The development will be done using .NET.
3. Modify the access components to the Service through the component of environment adaptation.

Adaptations by the network team

4. Definition and installation of network devices for IPv6 access.
5. Define security policies for the IPv6 network perimeter.
6. Configure DNS.
7. Installing and configuring devices for high availability

Systems adaptation

8. Adapting end systems to IPv6.

German Pilot:

The pilot runs on a number of different network segments with individual approaches each. These segments are planned and migrated independently in the first phase of the pilot. After finalizing the activities in one segment, it can be connected with other areas already finished.

The different segment areas for the pilot are:

- Internet connection
- WAN gateways
- Local network – Linux servers
- Local network – Windows servers
- Backbone servers
- DMZ servers

The first phase focuses on the Internet connection and the WAN gateways. In Q4 2012 the work on all segments has started in parallel. In some areas the IPv6 transition is necessarily embedded in further transition projects.

Turkish Pilot:

There is no need to change hardware in the TURKSAT network. Layer 3 network devices, firewalls and load balancers are planned to be configured respectively. It is observed that a software update for load balancers is needed. Thus this update has been added to the plans. On the participating governmental agencies side, there are two different cases, namely: needs update and needs upgrade. For the pilot these agencies have prepared their own transition plans which both depend on a dual stack structure since the services should be provided both over IPv4 and IPv6.

3.3 First successfully moved components

Spanish Pilot:

A first version of the shared service platform for providing IPv6 connectivity to eGovernment Web Portals has been implemented.

Enabling IPv6 access is achieved by means of a Reverse Proxy (IPv6 clients connect to this proxy and the proxy acts as a gateway to IPv4 servers) or, in cases where the use of a Proxy is not possible due to the need of an electronic certificate validation, by using NAT64. In this solution, Squid is used as Reverse Proxy (more details in section 5.3), with the connection being split into two sections, as it is shown in the figure:

- In the first case, IPv6 traffic goes from the client to the Reverse Proxy.
- In the second one, IPv4 traffic goes from the Reverse Proxy to the web server to obtain the page demanded from the client.

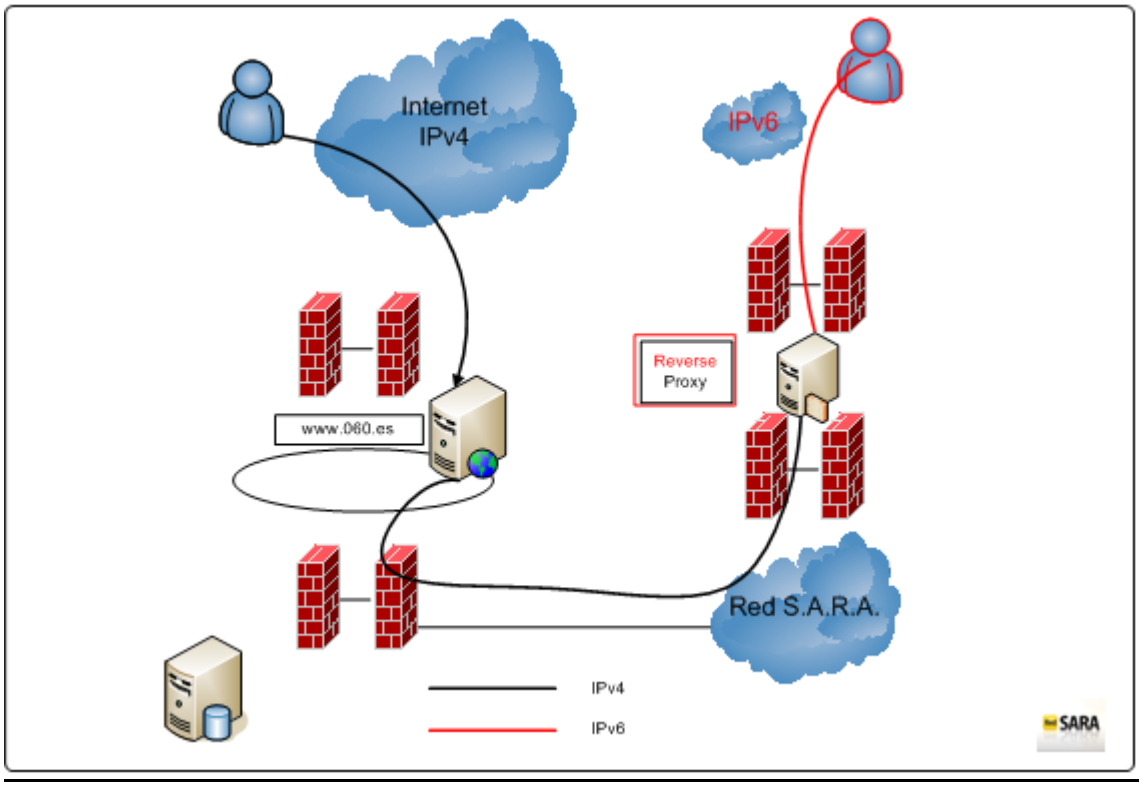

Figure 7 – Spanish Pilot: Reverse proxy approach for IPv6 enablement

As mentioned before, in areas that require user authentication using digital certificates, using a Reverse-Proxy is problematic. In such cases, NAT64 is used, mapping the IPv6 addresses requested by the client application to the IPv4 addresses which the web application is responding at.

Using this platform, in July 2012 two Web Portals from the MINHAP were IPv6 enabled:

- EGovernment Portal: www.administracionelectronica.gob.es
- A forge of the Technology Transfer Centre.

Other candidate portals from the MINHAP and other Ministries, to be added to the platform in the future, have been already identified (IGAE, Ministry of Health, Social Policy and Equality, Ministry of Justice).

Additionally, an inventory of IPv6 capabilities of elements connecting to the SARA network has been performed. There are 3 types of connection areas, depending on the entity in whose network they are deployed (Ministry Offices, Autonomous Communities and Singular Institutions). The elements in the connection area depend on the type of that connection except for switches and routers, which are all the same in all connection areas.

Regarding switches, they are Switch Cisco Catalyst 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.

Regarding routers, the connection to the backbone of the Virtual Private LAN Service (VPLS) network has not been configured in any router of the connection areas so far. Activities to test VPLS network IPv6 capability are on-going, so that the IPv6 transport through the backbone network can be supported. Since the backbone is a Layer 2 network, no problems regarding this are expected.

Information about servers and systems is detailed in section 4.

German Pilot:

As a first step, the Internet connection of Citkomm was enabled to route IPv6. This could be implemented as a pilot project even for the Internet network provider, who hadn't any operating IPv6 until then. Afterwards the Citkomm website www.citkomm.de was made available over IPv6 using a reverse proxy, based on the open source "nginx"[1]. The Citkomm web service went online in time for the IPv6 launch day in June 2012.

[1] Citkomm uses reverse proxy systems as strategic components for load balancing, caching and accounting and for saving resources in IPv4.

The WAN gateway components have been enabled for IPv6 connectivity. The most important gateways used in Citkomm networks are the iWAN gateways. These appliances are based on Linux open source modules. They implement several services, apart from the VPN connectivity over any IP transport platform. The ability for IPv6 has been successfully implemented both for the network interface and for the tunnel interface. At this point the pilot gateway implementation is able to support full network connectivity for IPv4 and IPv6. To check the functionality, one gateway was implemented in the IPv6 testbed of Fraunhofer FOKUS in Berlin. This gateway now keeps a permanent connection to a central gateway at Citkomm. Both connections use IPv6 as transport network.

For the Internet connection the transition to an autonomous system is in progress. The future topology for the components to design a high available infrastructure for the connection to the autonomous system uplinks has first been planned and tested for IPv4 only. After successful implementation and approval in a test area the real systems have been enabled with IPv6 too, operating in dual stack mode since then. The tests performed have been reproduced for the IPv6 functionality also. The validity of this concept could be confirmed finally as of Q4/2012. As a next step an external validation of the whole concept took place.

For the local network, all central servers were implemented using dual stack from the start. First tests did not show any significant problems in the test area.

The external connection to the German government backbone “Deutschland Online Infrastruktur – DOI” is planned to be enabled for IPv6 in Q3.

Turkish Pilot:

As the first achievement TURKSAT network has successfully updated the L3 network device configurations and updated the load balancer software in order to support IPv6. Following this step EGG Web portal has been IPv6 enabled.

3.4 Enabling IPv6 in components

3.4.1 Practical tests

Spanish Pilot:

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 will be delimited by two Cisco 2960S, level 2, systems.

A /64 prefix will be used. The IPs to be used are those obtained automatically when auto-configuring the equipment. Once the IP is obtained, it will be manually configured on the equipment.

This process will be exactly the same for the HSRP virtual IP's required for the Cisco equipment.

3 IPs will be used for each HSRP, 2 physical and 1 virtual.

In the perimeter security equipment, Palo Alto PA-5050, the same procedure will be used to obtain the IPs and the high availability system, allocating 3 IPv6 addresses, 2 physical and 1 virtual.

The configuration of the load balancing equipment, F5 3900, will use the same mechanism as in the previous equipment, with 3 IPs (2 physical and 1 virtual).

Two DNS servers will be used, dns4.mityc.es and dns5.mityc.es and they are using the same procedure to obtain their IP addresses.

This configuration will be the same as in the production environment, varying only the IPv6 provided by the SARA network.

German Pilot:

See section 3.3 above.

Turkish Pilot:

For the Turkish pilot, we built a test environment using the same configuration as the production environment. A new feature is first tested in this test environment and if it succeeds, it is ported to the production environment.

As a first step, performance and conformance tests have been run for the EGG Web Portal over IPv6 in the test environment. These tests include access and penetration tests over IPv6. After completing the tests successfully, the new configuration has been moved the production environment. Load balancer tests were critical for the Turkish pilot.

Further practical tests are being run on the backend of the pilot where the other governmental institutions will connect to TURKSAT over IPv6. The same procedure will be implemented in this

phase.

3.4.2 Experiences and pitfalls

Spanish Pilot:

As it was described, 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.

German Pilot:

For the transition of the Internet uplink it is necessary to contract the uplink provider, who supports IPv6. Citkomm has several uplink providers for Internet and MPLS. As a first step we asked all providers, whether they can provide IPv6 connectivity and additionally if they would support the routing of a /48 IPv6 subnet of the central address space allocated to the German government. The national network provider confirmed to be able to this. Unfortunately the Internet uplink provider who manages Citkomm's BGP-gateway router and one Internet uplink was not able to support IPv6. The DOKOM21 as a regional provider had no experience and even no concrete customer demands in implementing IPv6 in their network. Therefore one of the first steps was to talk to the provider to start a common pilot for this approach. After a relatively short time, the uplink router could be made available for IPv6. In the next step only the uplink to Deutsche Telekom was used for IPv6. Deutsche Telekom was able to implement IPv6 on the link within a few days, after the RIPE database was set up correctly. The delegation of the relevant IPv6 address space and the setup of the RIPE database was a further challenge, but primarily due to the fact that at this point the LIR for the German IPv6 address space and the Sub-LIR for Citkomm were not yet in operation at that point. This situation should be eliminated in further projects.

The technical implementation of IPv6 on the network components with static routing and the configuration of the reverse proxy were possible without any problems and could be executed

within a few days.

Concerning the WAN gateways, we concluded that the operating system and the modules used in the current version do not properly and reliably support IPv6. Therefore the whole system had to be re-implemented on current versions of the operating system as well as the modules. In fact, the iWAN gateway was re-implemented in a completely new version, instead of evolving the current one. This seemed unavoidable because otherwise the risk of system problems due to buggy IPv6 support in older software releases would have been uncontrollable.

Turkish Pilot:

Up to now, there are no IPv6 connectivity problems experienced in the Turkish pilot. ISP (Turk Telekom) provides native IPv6 connectivity, so by having IPv6 enabled devices institutions are able to connect to global IPv6 networks preferably using dual stack.

On the other hand, it is observed that network appliances may be problematic in terms of IPv6 deployment. There is no clear and common definition for “IPv6 enabled”.

4 AFFECTED NETWORK ELEMENTS

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 eGov 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 eGov services.

Spanish Pilot:

In the Spanish Pilot, concerning Red SARA, there are 3 types of connection areas, depending on the entity where they are deployed (Ministry Offices, Autonomous Communities and Singular Institutions). The elements existing in the connection area depend on the type of that area except for switches and routers, which are all the same in all connection areas. Those elements concerning the Ministry Offices (the ones inside the scope of the pilot) are the following:

Description	Name
Dell PowerEdge 2950 (1 x Quad Core)	STRABO
Dell PowerEdge 2950 (1 x Quad Core)	SAUNIO
Switch Cisco Cataliza 3750G *	AVIENO (stack 1)
Switch Cisco Cataliza 3750G *	AVIENO (stack 2)
Dell PowerEdge 2950 (1 x Quad Core)	SENECA
Dell PowerEdge 2950 (1 x Quad Core)	PORCIA
Dell PowerEdge 2950 (2 x Quad Core)	FIRMUS
Dell PowerEdge 2950 (2 x Quad Core)	FESTUS

Table 9 – Spanish Pilot: Used networking hardware

Service Name	HW related	Software	Versión	Dual-stack support
Web server	PORCIA/SENECA	Apache	2.2.3-11	Yes
Proxy	PORCIA/SENECA	Squid	3.1.8	Yes
DNS	PORCIA/SENECA	BIND	9.3.4-6	Yes
Email	PORCIA/SENECA	Sendmail	8.13.8-2	Yes
NTP	PORCIA/SENECA	NTPD	4.2.2p1-8	Yes
Log aggregator	SAUNIO/STRABO	Lógica		No
High Availability	PORCIA/SENECA	Heartbeat	2.1.3.3	Yes
High Availability	PORCIA/SENECA	Drbd	8.0.16-5	No
High Availability	PORCIA/SENECA	CMAN	2.0.84-2	No
Management	PORCIA/SENECA	DRAC	5	No
Firewall	FIRMUS/FESTUS	STONEGATE	5.3.3	Yes
Firewall	SAUNIO/STRABO	STONEGATE	5.3.3	Yes

Table 10 – Spanish Pilot: Basic services

4.1 Routers and Routing

Spanish Pilot:

Regarding Red SARA, at present, all Internet routers are capable to route IPv6 traffic. So far, those located in the back-up Data Center are already configured to do so. Since two links per Data Center are available, this allows ensuring high availability of the IPv6 connection to the Internet. The activities to make all routers IPv6-ready are ongoing, so this would lead to double redundancy in IPv6 Internet links (by means of redundancy in Data Centers and in links).

Regarding MINETUR's network, routers affected in the service consist of those to access the Ministry's secure network perimeter. These routers will be configured in redundancy using the HSRP protocol. 3 IPs will be used for each HSRP, two physical and one virtual.

German Pilot:

As part of the autonomous system implementation tests, all relevant routers have been enabled for IPv6. All relevant routers under control of Citkomm are implemented as Linux-based software routers. The provider edge routers are based on Cisco technology. The IPv6 implementation did not raise any significant problems. For the routing static and dynamic routing is implemented. For the dynamic routing OSPF is used.

Turkish Pilot:

Throughout the pilot process, the next step after the addressing plan has been configuring

routers with IPv6 support. Since routers in the TURKSAT network (as well as other L3 devices) have 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 OSPFv3 and static routing have been deployed where necessary. For instance, static routing has been deployed on the connection between TURKSAT and the participating governmental agencies.

4.2 Affected central IT systems

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.

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

German Pilot:

All central systems of the Citkomm network will affected by the project. Due to the fact that until now the focus of the project was on the network environment none of the following mentioned central systems have been transited productive until now.

Turkish Pilot:

DNS and logging are the main central IT systems that should be analysed for the Turkish pilot. These items are investigated and updates have been done as defined in the requirement analysis document.

4.2.1 E-Mail

Spanish Pilot:

Email servers in connection areas are IPv6 ready since the software they use, sendmail version 8.13.8-2, supports it; despite the fact that sendmail isn't IPv6-enabled on Linux by default, it is very easy to configure it to support IPv6 as well.

German Pilot:

E-mail based on postfix with IPv6 has still been investigated during tests with German national Backbone DOI. So basically it is expected to work proper. In productive area there is no connection available until now. For internet connectivity first the autonomous system must be finalized. The communication to governments over the national backbone could be enabled with IPv6 because the transition of the network gateway has been delayed for more than six month by the operator and is now scheduled for early 2013.

Turkish Pilot:

No changes are made in the e-mail systems for the Turkish pilot.

4.2.2 DNS

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.

DNS will be configured with entries in AAAA for IPv6. It will be detailed once the final address range is provided.

German Pilot:

Serving AAAA-Records was successful performed for the transition of first Web-Server. DNS with IPv6 network connection also has been investigated as part of the DOI IPv6 tests. The operation with current bind version lets the pilot expect no problems in transition in later steps of the pilot.

Turkish Pilot:

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

4.2.3 NTP

Spanish Pilot:

NTP service is provided by means of the Network Time Protocol daemon (ntpd) version 4.2.2p1-9, which is an operating system daemon program that maintains the system time in synchronization with time servers using the Network Time Protocol (NTP).

NTP is an application layer protocol and it has been proved to work properly over IPv6 as long as its implementation is IPv6 compatible, as this is the case for NTPD version 4.2.2p1-9.

German Pilot:

NTP services have not been investigated in detail until now.

Turkish Pilot:

No changes will be made for the NTP service. Same NTP servers (NTP version 4.2.6) are used in the Turkish pilot.

4.2.4 DHCP

Spanish Pilot:

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

German Pilot:

Most of the network areas and components affected are working with static IP addressing. DHCP will be relevant for the local networks. Testing networks for local networks have been installed and DHCP solution will be one of first investigation points to get these networks ready for operation.

Turkish Pilot:

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

4.2.5 Logging

Spanish Pilot:

Logging in connection areas is performed by means of logging aggregation software, called Lógica. This software reads log files from firewalls and Snort, consolidates them in a single log file and parses it in order to send it to other systems like CCN-Cert.

At present, Lógica does not support IPv6, so this software is being replaced with ArcSight, which is IPv6 compatible. This change is well underway, and currently it has taken place in several connection areas of Red SARA.

German Pilot:

There are no special logging environments in Citkomm network that have to be investigated. For each component logs will be generated based on the systems local ability. In iWAN network for some purpose central syslog servers are available. Special challenges dealing with IPv6 still have to be investigated.

Turkish Pilot:

All institutions in Turkey are obliged to log and sign their traffic for future forensics purposes. In TURKSAT logging has been already made for IPv4. For IPv6, the same logging solution has been used for the EGG Web portal in order to monitor the network traffic between this Web portal and its users. This solution should be deployed for the backend implementation of the Turkish pilot to log the network traffic between TURKSAT and other governmental institutions.

4.2.6 Others

Spanish Pilot:

Current high availability services (Heartbeat, DRDB and CMAN) do not support IPv6, and 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 eGovernment services in IPv6.

German Pilot:

There are several central systems in application backend that possibly may be affected by

transition activities. Citkomm tries to reduce the occurring possible disturbances trough strict network separation between dual stack areas and Ipv4 legacy areas.

Turkish Pilot:

No other central IT systems being affected.

4.3 Further affected systems/components

The following subsections describe other systems and components which are affected by the transition.

4.3.1 VPN

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 both in 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 and these firewalls are Stonegate version 5.3.3 and they support IPv6.

German Pilot:

The Citkomm WAN network uses VPN services as central infrastructure. So VPN is vital for the German pilot. The iWAN gateway components have been enabled for IPv6 connectivity. These appliances base on Linux open source modules and openVPN. The combination is performed by Citkomm in a kind useful for the special demands in the Citkomm wide area network and the connected customers. The ability for IPv6 has been successful implemented both for the network interface and for 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 implemented in the test filed of Fraunhofer FOKUS in Berlin. This gateway now keeps a permanent connection to a central gateway at Citkomm. Both connections base on IPv6 Internet access as transport

network.

Turkish Pilot:

A VPN connection has been deployed in the backend implementation of the Turkish pilot between TURKSAT and other governmental institutions. VPN connections will be finalized at the VPN box placed on the public institution side. NETAS CO. has been working on this box as an R&D project which will be finished in third quarter of 2013.

4.3.2 Load balancing

Spanish Pilot:

Regarding the Spanish pilot, in Red SARA load-balancers are not needed. In the case of IPv6 access to web portals of public administrations, the 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. 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 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 will be configured accordingly.

Turkish Pilot:

There exists a load balancing solution for the TURKSAT Web portal. Software has been required in order for this device to support IPv6. This update has been made successfully.

German Pilot:

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

4.3.3 Printers

Spanish Pilot:

No IPv6 communications with printer or faxes are considered within the scope of the Spanish

pilot.

German Pilot:

For LAN connectivity printers have to be investigated. Due to the fact that the IPv6 support for printer is not that far than for server and Client the transition of the printer has not been focused and will be deferred for later pilot phase.

Turkish Pilot:

Not applicable.

4.3.4 Monitoring

Spanish Pilot:

Generally speaking, it is required for all the systems and applications monitoring the networks involved in the Spanish pilot to be capable of dealing with information regarding IPv6 communications (such as exchanged traffic), as well as with IPv6 information elements (such as IPv6 addresses present in server logs).

In the Spanish pilot, it is intended that the solution provides the same information regarding IPv6 traffic that it is currently provided regarding IPv4 traffic. In particular, the following traffic statistics, broken down by entity connected to Red SARA, are needed:

- SMTP e-mail exchange
- Use of HTTP and HTTPS services
- TCP and UDP traffic

Due to the fact that 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 adapted yet. IPv6 traffic is being supervised, as a temporary means, using the IPv6 logging capabilities of the firewalls.

German Pilot:

Citkomm uses central monitoring services based in icinga. Icinga offers IPv6 support. The implemented services are not in a special monitoring for the IPv6 connectivity, so there are no

special experiences for monitoring so far.

Turkish Pilot:

TURKSAT has been monitoring IPv4 networks and services using different tools such as nagios and NfSen. These tools are 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.

4.3.5 Management

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 eGovernment services in IPv6.

German Pilot:

The management for Citkomm data centre operates as far as possible outband, 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.

Turkish Pilot:

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

4.3.6 SNMP

Spanish Pilot:

SNMP is currently used in Red SARA 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, it is intended to be performed during 2013, together with the upgrading of the backbone network and the connection areas equipment.

German Pilot:

SNMP is used only at few points for special monitoring solutions. None of this points has been affected so far, so no experiences with SNMP over IPv6 could be made until now.

Turkish Pilot:

SNMP has been used within TURKSAT network for monitoring IPv4 network. Similar process will be made for monitoring IPv6 network.

5 SECURITY ASPECTS OF USING IPV6

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

Spanish Pilot:

As far as Red SARA is concerned, regarding systems and components referred to in this section, 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, and it reports data to CCN-CERT through the logging aggregator. This new version is able to analyse IPv6 traffic.

German Pilot:

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

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. Also 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.

5.1 Firewalls

Spanish Pilot:

Firewalls of connection areas are Stonegate version 5.3.3 and they support IPv6.

German Pilot:

In Citkomm network firewalls are implemented on several points. In most cases Linux with IPtables is implemented. At this point it can be stated IPv6 is fully support in IPtables.

Turkish Pilot:

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

5.2 Application Layer Gateways (ALGs)

Spanish Pilot:

The use of ALGs is not intended in the Spanish pilot.

German Pilot:

As part of the network redesign / autonomous system the former ALG in Citkomm network will be set out of order. Network security will be implemented by tight IPtabels rulesets, not only for source and destination but also for packet and flow behaviour. ALG services near to the content will be transferred to services resp. the relevant servers.

Turkish Pilot:

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

5.3 Proxies

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, which supports IPv6.

Squid is also used as gateway for IPv6 clients to IPv4 world (see section 3.3). This software, among its capabilities, has the option to act as reverse proxy or accelerator, and it will be 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 eGovernment web portal servers.

In this way it will be able to act as bridge between IPv4 portal servers and IPv6 requests from citizens.

German Pilot:

For proxy service Squid is used. In reverse mode Squid is still used in IPv6 communication since IPv6 day in June 2012. Due to the experience there are no problems expected for using it in forward mode too.

Turkish Pilot:

Not applicable.

5.4 Use of secure protocols

Spanish Pilot:

For the Web Portals to be made IPv6 accessible, the use of IPsec is not required, nor is it required for the MINETUR eITV application.

German Pilot:

Secure protocol connections based on SSL have been successful investigated with the iWAN VPN solution. IPsec connections are only used with external partners outside the pilot, so there is no transition test planned for IPsec.

Turkish Pilot:

In the backend implementation, VPN has been deployed over IPv4. Through Turkish pilot, these connections will be made IPv6 enabled, and secure protocols such as IPsec over IPv6 will be deployed between TURKSAT and other institutions.

Also TLS is currently being used for EGG Web portal access. TLS is an application layer solution,

hence the underlying IP protocol is not related to this secure protocol.

5.5 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.

German Pilot:

It could be seen in some cases, that IPv4 traffic was strictly restricted on a gateway. At same time IPv6 was set with no filter rules, so IPv6 traffic was fully unrestricted and furthermore even uncontrolled. So as fundamental pint for network improvement and transition to IPv6 even for one ore few host must be a security check that all connected gateways definitively have a qualified ruleset regarding the filtering of IPv6.

Turkish Pilot:

There are no other security aspects to be mentioned at this phase.

6 LINK TO SYSTEM REQUIREMENTS

This section links the transition work documented in this document D3.6.1 to previous GEN6 deliverables which have listed the needed requirements to start such task in the first place.

6.1 Assessed basic technical requirements (so far)

Spanish Pilot:

As it has been mentioned before, a compatibility assessment is being performed regarding the IPv6 capability of the equipment involved in the pilot, whose preliminary results have been described in the corresponding paragraphs.

German Pilot:

Transition of network components to IPv6 will not raise special problems as far as current software releases are available. In the case operation systems or software modules may get a few years old the risk of running in failure grows rapid. So fundamental for any IPv6 transition is the premature focus of procurement on solutions with qualified IPv6 support.

Turkish Pilot:

An inventory of applications used or served by the eGovernment Gateway has been prepared for security controls. All the software components used by the eGovernment Gateway have been examined for IPv6 readiness. Some components have been replaced with IPv6 ready components, e.g. all application modules which have been developed by the eGovernment Gateway project team controlled by developers. Also, new modules are developed with respect to IPv6 requirements. An R&D project started for the XML Gateway Application, and it is planned to be IPv6 ready.

6.2 Assessed extended technical requirements (so far)

Spanish Pilot:

German Pilot:

No considerable point has been identified until now.

Turkish Pilot:

XML Gateway (Public Integration Box): This is a hardware and software integrated module which will be used by ministries. All network connections to the eGovernment Gateway will be secured by this module. Also this box has a connector module for XML web services published by the ministry or by the eGovernment Gateway. This project has begun on the first quarter of 2012 with NETAS CO. and this project is planned to be completed in the third quarter of 2013. The project will add IPv6 support to this module.

7 OUTLOOK

In 2013 and beyond, the GEN6 project's national pilots will further work on migration of additional parts of their infrastructure to IPv6. This section gives an outlook on the most prominent migration work ahead per each pilot.

7.1 Spanish Pilot

As it has been described previously, the Spanish pilot envisages three complementary action lines, all of them based on the role of Red SARA as the core network for the interconnection of the Spanish Public Administrations:

- The upgrade of Red SARA so that it can transport IPv6 natively, therefore allowing IPv6 communications between administrative units.
- The implementation of a transition mechanism that allows Public Administrations to offer online services accessible by means of IPv6, based on a shared service approach.
- The evolution of the MINETUR network so that it can provide native IPv6 services (eITV application) to be consumed by other administrative units (DGT, Directorate General for Traffic).

For 2013, the work foreseen in the Spanish pilot in each of these lines is the following:

- Upgrading of Red SARA to support IPv6 services provision between Public Administrations. In 2013, the actual upgrading of the backbone and of the infrastructure existing in the connection areas will be performed, as well as the training to the operation staff so that they can be prepared for the management of the IPv6 traffic.
- The interconnection via s-TESTA between the Spanish and the German pilots and the integration of IPv6 on the PEP component of SARA for evaluating the interoperability with IPv6 of the authentication services.
- IPv6 enablement of Public Administrations Web Portals through shared services. The

implementation plan for this activity is based on several iterative cycles, so that a set of web portals are made IPv6 available in each interaction. It is therefore intended that in 2013 more iterative cycles will take place, aiming to increase significantly the number of IPv6 enabled portals at the end of the year.

- Adaptation of MINETUR services to IPv6. In 2013, 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 Red SARA is upgraded, the IPv6 compatible version of eITV will be deployed and operated.

7.2 German Pilot

The IPv6 pilot at Citkomm will continue on the separated working points. The next steps are as follows

- Network
    - Transition of DOI (German government backbone) gateway to IPv6
    - Transition of E-Mail communication into DOI network to IPv6
    - Implementing of connectivity services between test networks (s. below)
    - Implementation of autonomous system with IPv6
    - Transition of further web server / url
    - Transition of infrastructure services like DNS, Proxy, E-Mail
- Local network – Windows
    - Enabling IPv6 connectivity as dual stack for server and client
- Local network – Linux
    - Investigate basic network services (DHCP, DNS, Proxy) in local network environment
    - Connectivity check for Win7-Clients

- Application backbone
    - Implementation of first basic services
    - Implementation of first application
    - Transition to IPv6 for implemented application

The following figure shows the whole system of test networks, gateways and corresponding productive networks.

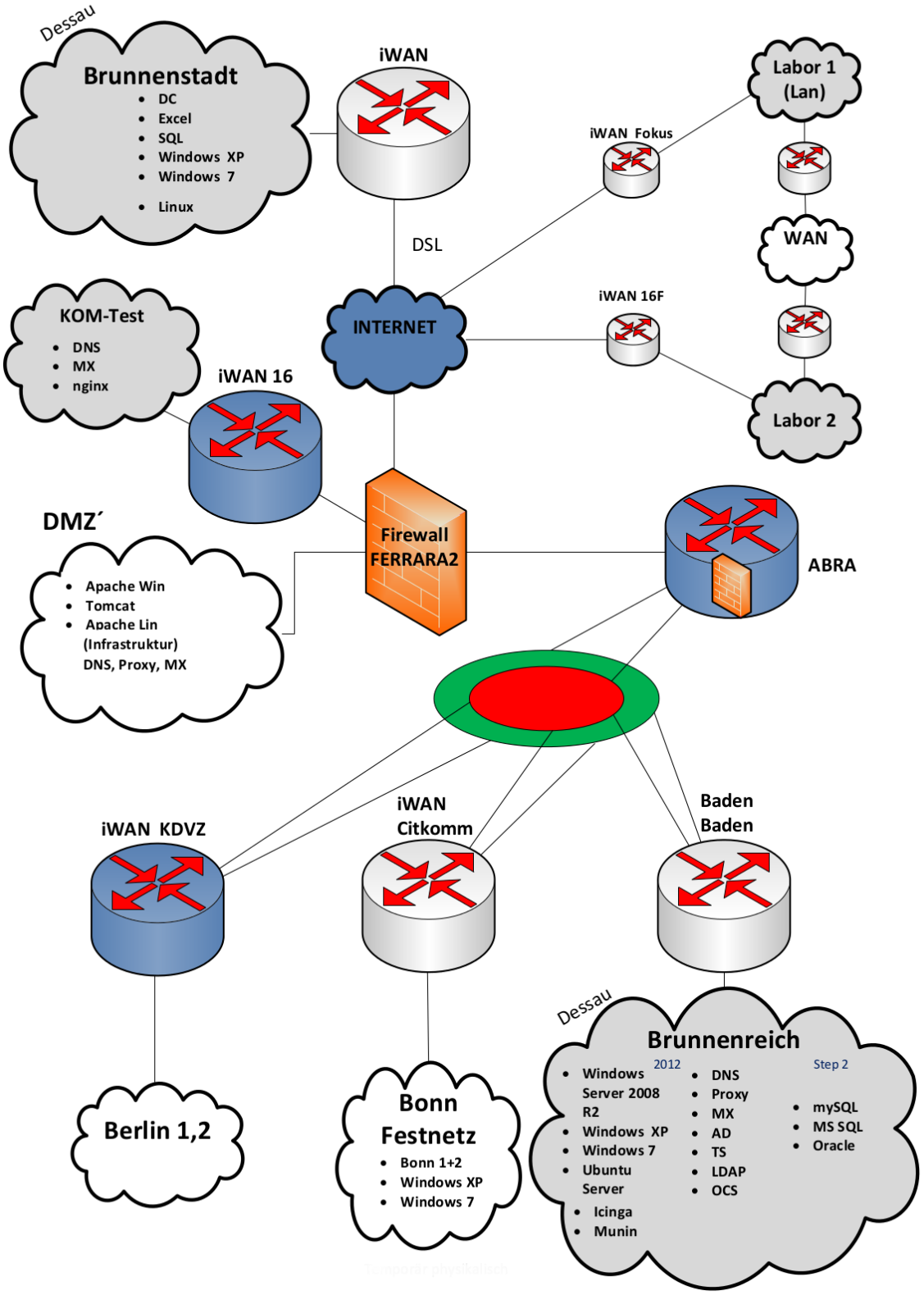

Figure 8 – German Pilot: test network infrastructure

7.3 Turkish Pilot

The Turkish pilot has successfully deployed IPv6 through TURKSAT and made the EGG Web portal IPv6 enabled. In other words, citizens are able to use the EGG Web portal either over IPv4 or over IPv6. In 2013, the backend of the EGG will be made IPv6 enabled. For this purposes, the connection between TURKSAT and other participating agencies will be made IPv6 enabled. In this process, bureaucratic procedures are on-going as well as technical issues. At the end of the project EGG is planned to be IPv6 enabled both for the backend and the frontend.

8 CONCLUSIONS

The three national pilots working inside the GEN6 project and located in Turkey, Spain and Germany are similar in their target: examining existing eGovernment Services currently based on IPv4 and building a pilot for selected services to ease the transition to IPv6. The environments in which the pilots are being implemented (technical and administrative responsibilities, existing infrastructures, pre-existing addressing plans, administrative level, etc.) are rather diverse. And so are the challenges encountered and possible solutions to examine.

Apart from the value of the individual experiences gained in the pilots, the summary of insights allows for a good overview of the broad range of tools, techniques and solutions available when moving eGoverment Services to IPv6. This range of possibilities will be further evaluated and described as the pilots make progress.