Title:	Document Version:
Deliverable D3.1 **Requirement Analysis for eGovernment Services with IPv6**	2.2

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

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/03/2012	02/10/2012	R – PU

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

Responsible and Editor/Author:	Organization:	Contributing WP:
Onur Bektaş	ULAKBIM	WP3

Authors (organisations):

Michiel Ettema (Alkmaar), Martin Krengel (Citkomm), Jan Severin (Citkomm), Gerold Gruber (Citkomm), Jordi Palet Martinez (Consulintel), Jens Tiemann (Fraunhofer), Joachim Kaeber (Fraunhofer), Carsten Schmoll (Fraunhofer), Julio Augusto Cogolludo Herranz (MINETUR), Carlos Gómez Muñoz (MPTYAP), Jorge Fabeiro Sanz (MPTYAP), María Ángeles Gonzalo García (MPTYAP), Arjen Holtzer (TNO), Kamil Seyhan (TURKSAT), Sami Yenice (TURKSAT), Foued MELAKESSOU (UL), Emre Yüce (ULAKBIM), Murat Soysal (ULAKBIM), Mojca Volk (ULFE), Janez Sterle (ULFE), Jan Zorz (ULFE), Antonio F. Skarmeta (UMU), Pedro Martinez Julia (UMU).

Abstract:

This deliverable presents the requirement analysis of four national pilot activities in the "IPv6 upgrade of eGovernment Network Infrastructures, e-Identification, Services and Applications" group, which will be accomplished by Germany, Spain, Netherlands and Turkey.

Keywords:

IPv6, Governments, eGovernment Services, requirements analysis.

Revision History

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

Revision	Date	Description	Author (Organization)
v1.0	12/03/2002	Document creation	Onur Bektaş (ULAKBIM)
v1.1	29/03/2012	Document merged with the new contributions	Emre Yüce (ULAKBİM)
v1.2	06/04/2012	Introduction and executive summary sections added.	Murat Soysal (ULAKBİM)
v1.3	06/04/2012	Requirement tables added, style checked.	Emre Yüce (ULAKBİM)
v1.4	09/04/2012	Wording and merging of sections.	Onur Bektaş (ULAKBİM), Murat Soysal (ULAKBİM), Emre Yüce (ULAKBİM)
v1.5	12/04/2012	Sections without requirements from any pilots are omitted. Content integrity among the sections is performed.	Onur Bektaş (ULAKBİM), Murat Soysal (ULAKBİM), Emre Yüce (ULAKBİM)
v1.6	13/04/2012	TURKSAT requirements checked and added missing requirements.	Kamil Seyhan (TURKSAT)
v1.7	14/04/2012	Citkomm requirements updated, 7.1.1 added, minor corrections all over the text	Gerold Gruber (Citkomm)
v1.8	16/04/2012	Overall review	Jordi Palet (Consulintel)
v1.9	19/04/2012	Minor changes according to Carlos Gómez Muñoz, Joachim Kaeber and Carsten Schmoll's comments.	Onur Bektaş (ULAKBİM), Emre Yüce (ULAKBİM)
v2.0	20/04/2012	Final review	Jordi Palet (Consulintel)
V2.1	14/09/2012	Revised with respect to the Technical Review Report	Michiel Ettema (Alkmaar), Kamil Seyhan (TURKSAT) Emre Yüce (ULAKBİM)
v2.2	20/09/2012	Final Review	Uwe Kaiser (Fraunhofer)

Disclaimer

[1] http://creativecommons.org/licenses/by-nc-nd/3.0/

Executive Summary

The national pilots of the GEN6 project in Germany, Spain, Netherlands and Turkey represent significant similarities and they are grouped under the “IPv6 upgrade of eGovernment Network Infrastructures, e-Identification, Services and Applications” topic. The efforts of these four pilots are expected to reveal common and different aspects of enabling IPv6-enablement, taking into account the different approaches to IPv6 in these pilots.

A major phase in implementing these pilots is the requirement analysis study. This study includes the identification of the needs for enabling IPv6 in each pilot with clear definitions and plans for future actions. The GEN6 consortium, to perform requirements analysis of these four pilots, followed a collaborative approach and this document summarizes it.

This deliverable includes a list of requirement categories, which were generated by GEN6 partners for the realization of the four pilots. A total of 73 topics were identified and these topics are clearly defined to represent a common understanding among the GEN6 members. Moreover, these topics are grouped under seven main categories: Network architecture requirements, network level requirements, network hardware requirements, business applications requirements, support applications requirements, management requirements and security.

Based on the list created, all four pilots are reviewed and specific needs of the pilots for each item on the lists are included in this deliverable. Therefore, this deliverable will provide not only a detailed work plan for the pilots but also a checklist for enabling IPv6. Finally, the inclusion of requirements of all pilots in “IPv6 upgrade of eGovernment Network Infrastructures, e-Identification, Services and Applications” grouped into a single deliverable enables the GEN6 consortium to compare the requirements of the pilots.

Table of Contents

Figure Index

Table Index

1. INTRODUCTION

GEN6 includes four different types of national examples (also called national pilots) to provide general guidelines for planning and realizing the steps in enabling IPv6. These pilots are:

- IPv6 upgrade of eGovernment Network Infrastructures, e-Identification, Services and Applications (Germany, Spain, Netherlands and Turkey).
- IPv6 upgrade of Secure Cloud Services (Luxembourg).
- IPv6 upgrade of Energy Efficiency in School Networks (Greece).
- IPv6 upgrade of Emergency Response Environments (Slovenia).

The goal of the first group of four pilots in four different EU countries is to experience the transition towards IPv6-enabled infrastructures under different approaches and to learn (and document) the best practices to do so during the process. This deliverable has a specific interest on the requirements of these four pilot activities within the eGovernment Network Infrastructures, e-Identification, Services and Applications group.

A requirement analysis is the initial step for identifying the needs of these pilots. Although they belong to the same group, all four pilots represent specific characteristics based on their network architectures and the features of the services included in the pilots. The GEN6 consortium followed a collaborative approach to present the requirements of these four pilots in a single document in a complementary manner to highlight the categories in common and the categories specific to one or more pilots.

During this collaborative action, first an inquiry was started among the pilot representatives to identify a list of categories to perform the analysis. A draft list circulated among the pilot attendees with a total 23 items grouped under 6 categories. Following the discussion and contributions of all work package members the final list of categories for the requirement analysis was composed with a total of 73 items grouped under seven main categories. These categories are network architecture requirements, network level requirements, network hardware requirements, business applications requirements, support applications requirements, management requirements and security.

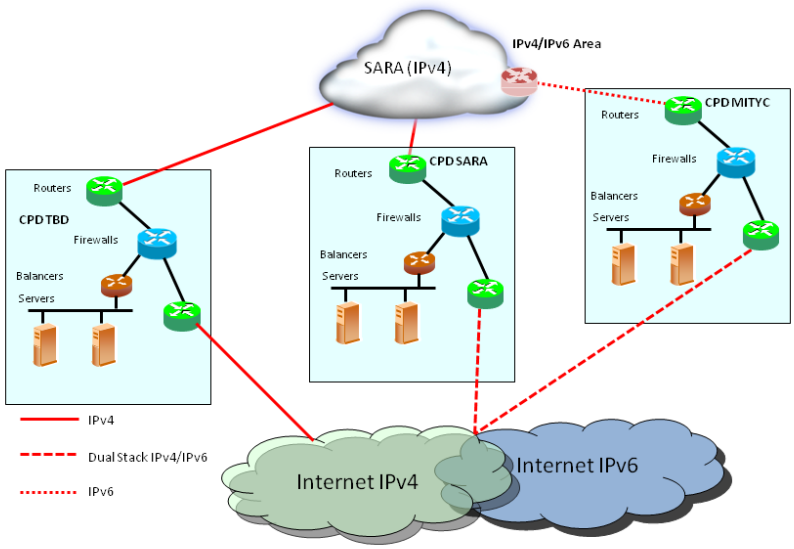
Before passing to the analysis of requirements of each pilot for these 73 items, the team members were assigned to provide one paragraph of definition for items in the list. The main aim in this action was to generate a common understanding among the partners about the categories. Following each partner's contribution, a full list of requirement analysis topics including definitions of the items in the list was composed.

Each pilot performed the final step individually and the requirements of pilots for each item in the list were provided as inputs for this deliverable. In the following section, all of these inputs are represented following the same procedure in collecting the inputs. The requirement analysis items are included with a definition representing the common understanding of the project and followed by special sections for each pilot's own requirements on that item. In case an item is not specified for a pilot, the sub-section for that pilot under the specific item is explicitly marked as "No requirements specified".

This deliverable will guide each pilot in enabling IPv6 since it includes the requirements of the pilot in a categorized format. Each pilot will follow the items in the document and use it as a checklist to complete the required steps for enabling IPv6. Moreover, the list will help to define the detailed work plan of each pilot.

2. NETWORK ARCHITECTURE REQUIREMENTS

In order to complete the pilots successfully, the network architectures should be analysed carefully. This analysis should include requirements on the subjects such as external connectivity, infrastructure and geographical structure that are presented in this section accordingly.

A 3.1	Germany	• IP-addressing plan, will use the national government address range allocated by RIPE NCC
A 3.2	Spain	Two participant network are involved: • Red SARA, managed by MINHAP (formerly MPTYAP), acting as the network that interconnects Spanish Public Administrations and provides a platform for IPv6 connectivity to the Internet. • MINETUR (formerly MITYC) network, acting as the provider of IPv6 capable service oriented business applications to be consumed by other administrative units outside the Ministry. Figure 2-1 shows the overall view of the pilot and relationship between the two networks.  **Figure 2-1: Overall View of the Spanish Pilot**
A 3.3	Netherlands	Figure 2-2 shows the architecture of the Netherlands pilot. The aim is to enable the entire architecture (except for all components of the Internet) to IPv6, but the main focus lies on the Alkmaar and Inter Access networks and services. Note that one of the activities in the Netherlands pilot involves motivating third parties to introduce IPv6.

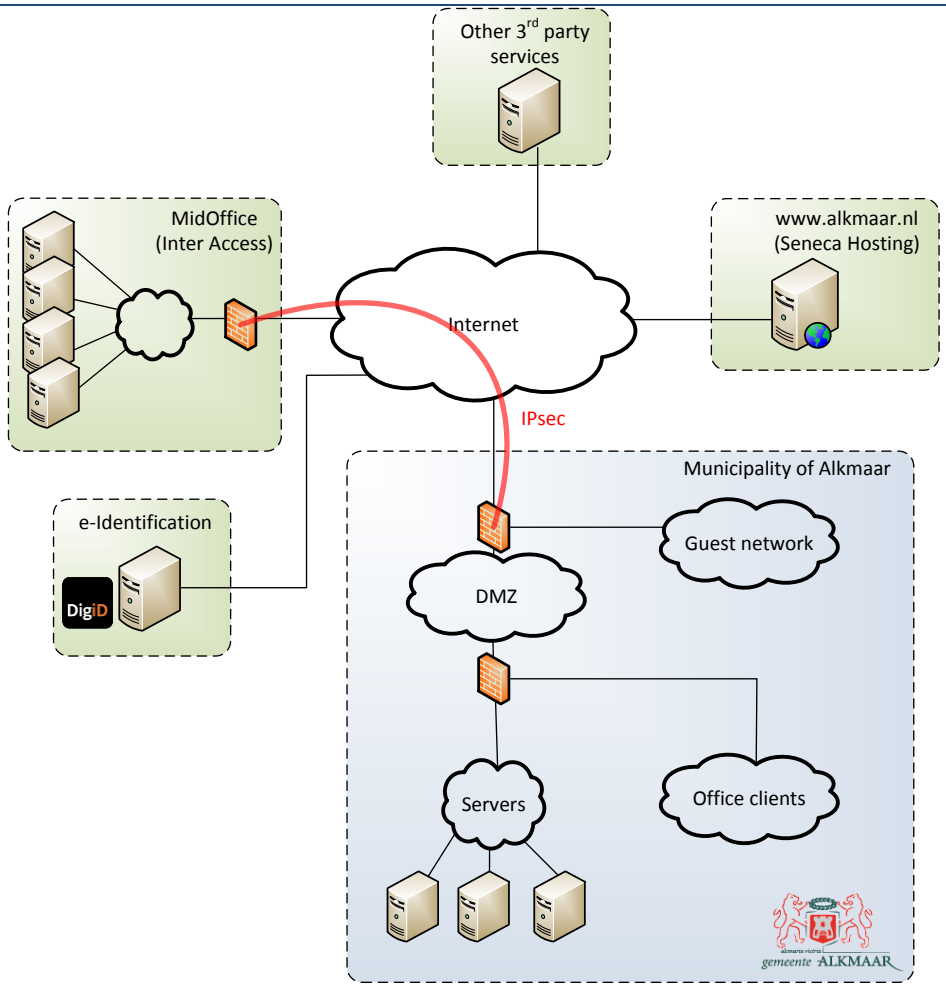


Figure 2-2: Overall View of the Netherlands Pilot

A 3.4	Turkey	Currently eGovernment Gateway Web portal is giving several services to the citizens over IPv4. Pilot aims giving these services over IPv6 at the same time. On the backend connections will be made between TURKSAT and the collaborating governmental institutions (SGK, PTT and ULAKBİM).

Table 2-1: Network Architecture Requirements

2.1 External Connectivity Required

This section refers to the requirements regarding to the connectivity between the network of the participants in the pilot, the Internet and the network of other organizations.

A 3.1	Germany	The Citkomm network needs external connectivity: • Uplinks to the Internet • Connections to other governmental, federal and municipal institutions via the national government backbone (called DOI) • Connections towards the customers through several provider networks based on MPLS
A 3.2	Spain	Red SARA external connectivity requirements are: • The connection to the Internet • The connection to the MINETUR network • The connections to the network of the administrative units that are the "clients" of the MINETUR services • The connections to the network of the administrative units that want to make their Web Portals and/or other services accessible through Red SARA over IPv6 MINETUR network external connectivity requirements are exclusively related to the need of connection to Red SARA.
A 3.3	Netherlands	The Alkmaar network needs external connectivity to: • The Internet • Mid office environment via IPsec tunnel The mid office environment, the hosting provider and e-identification services need to be connected to the internet.
A 3.4	Turkey	TURKSAT has the following external connectivity requirements: • Connection to Internet, i.e. citizens to use services. • Connection to institutions that are giving services over eGovernment system.

Table 2-2: External Connectivity Required

2.1.1 IPv6-Capable Network Ingress and Egress Points

The organization network may be connected to many other networks where some are IPv6 enabled and some not. The requirements mentioned in this section refer to the specific connection points, which must be IPv6 enabled.

A 3.1	Germany	The following connections need IPv6 connectivity as a component of the pilot: • The Uplinks to the Internet • The connection to DOI (national government backbone)
A 3.2	Spain	There will be two connection points that must be IPv6 capable: • The connection point between the Internet and Red SARA • The connection point between Red SARA and MINETUR network
A 3.3	Netherlands	All connections to the internet, as indicated in Figure 2.2, should be IPv6 enabled.
A 3.4	Turkey	TURKSAT external connectivity and the connection between TURKSAT and the governmental institutions should be IPv6 enabled.

Table 2-3: IPv6-Capable Network Ingress and Egress Points

2.2 Geography: Number and Location of Sites

This section refers to the number and the location of the sites that will be connected through the participant organization network during the pilots. These sites should include the locations where the technical works oriented to the IPv6 transition will take place.

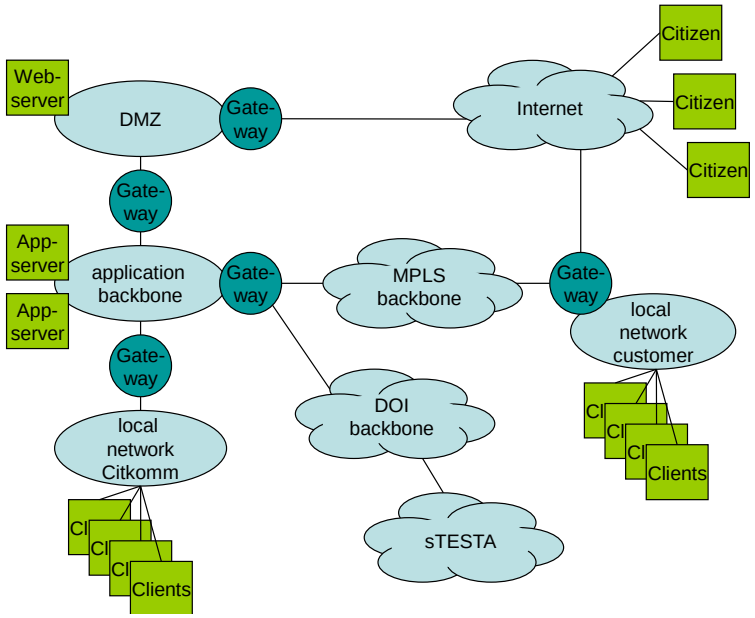
A 3.1	Germany	The relevant network segments are illustrated in following figure.  **Figure 2-3: Relevant network segments in the German Pilot**
A 3.2	Spain	The sites involved are the following: • Red SARA Data Centre, located in Madrid, which houses the connection area to the Internet. • MINETUR Data Centre, located in Madrid, which houses the servers that provide the business applications to be used by means of IPv6, as well as the connection area to Red SARA. • MINETUR's clients Data Centres. Even though the specific clients are still to be determined, they will be probably located also in Madrid, since the city hosts the majority of the institutions of the Spanish National Administration. • The Data Centres of the institutions that want to make their Web Portal accessible through Red SARA using IPv6 protocol. These institutions are also to be determined.
A 3.3	Netherlands	The sites involved are the following: • DMZ and primary server farm of the Municipality of Alkmaar, located in the City office in Alkmaar • Secondary server farm of the Municipality of Alkmaar, located in Datahouse hosting facility in Alkmaar. • Mid office environment, located in Inter Access data centre, in Hilversum
A 3.4	Turkey	The sites involved are the following: • TURKSAT Data Centre Located in Ankara, which houses the servers of eGovernment Gateway and the connection area to the Internet. • PTT (General Directorate of Posts and Telegraph Organization) Data Centre, located in Ankara, which houses the servers that provide the registration of citizens to e-Government Gateway. • The Data Centres of the public institutions that want to make their business applications accessible through eGovernment Gateway using IPv6. These public institutions are also to be determined.

Table 2-4: Geography: Number and Location of Sites

2.3 Ownership: In-House/Outsourced

These requirements are related to the sourcing approach chosen by the participants for the

provision of network services, considering different types of resources involved such as network equipment, links, software and human resources.

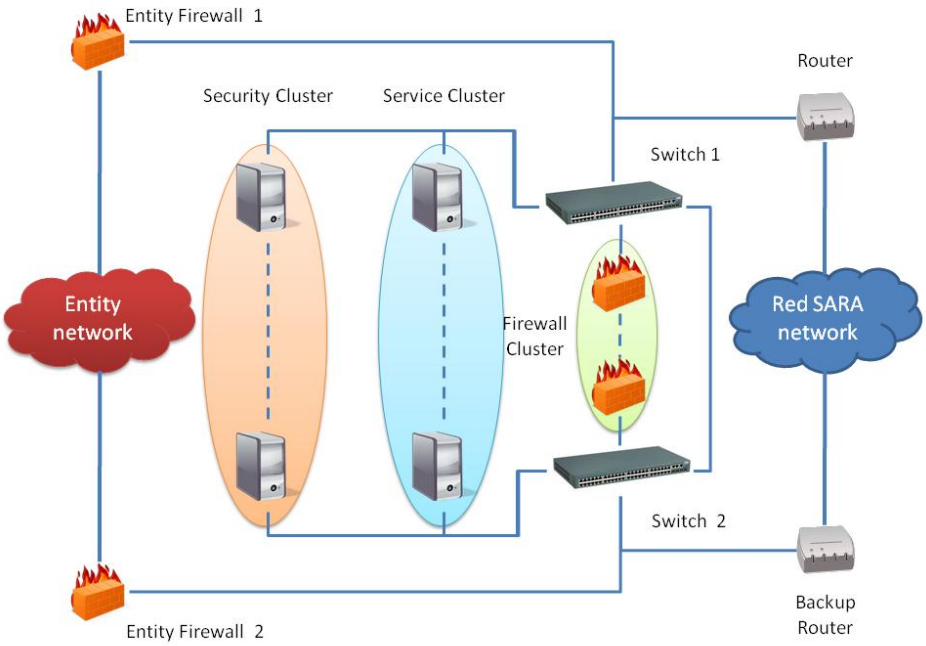
A 3.1	Germany	Citkomm itself operates most relevant components. Dependencies to external partners exist for the network: • Internet-connectivity via two physical uplinks with different providers • An external provider operates the DOI (national government backbone) • Several providers operate MPLS infrastructures
A 3.2	Spain	A distinction has to be made between Red SARA and MINETUR network: • Red SARA sourcing approach is based on a model in which: ○ A telecommunications operator owns and manages, according to demanding Service Level Agreements and under the close supervision of Red SARA staff, the network backbone that interconnects all the institutions connected to Red SARA, as well as the links between the backbone and the institutions' sites. ○ MINHAP owns and manages the equipment located in the connection area between the institution network and Red SARA access links. ○ The institutions provide the infrastructure (housing, power supply, refrigeration, etc.) needed to support the connection area. • MINETUR network sourcing approach is in-house Figure 2-2 shows an overall view of the before mentioned connection areas, whose role is the key in the IPv6 transition of Red SARA.  Figure 2-4: Overall View of the Connection Areas in Red SARA
A 3.3	Netherlands	Alkmaar operates their own networks and servers and initiates changes on networks and servers themselves, expect for continuity assurance, including monitoring. Other parts of the pilot are outsourced as indicated in Figure 2-2.
A 3.4	Turkey	TURKSAT has the Internet-connectivity via two physical uplinks provided from Turk Telekom. The governmental institutions are responsible for their own connectivity and network equipment in order to establish the connection to the eGovernment infrastructure.

Table 2-5: Ownership: In-House/Outsourced

2.4 Infrastructure: Shared/Dedicated

This section refers to the specific requirements regarding the infrastructure of the participating pilots.

A 3.1	Germany	The network segments operated by Citkomm are always dedicated for the offered service portfolio. Connected network platforms like MPLS or DOI are based on shared infrastructures, but operated by external providers.
A 3.2	Spain	In the case of Red SARA infrastructure, two different situations occur: • The network backbone, provided by the telecommunications operator, is physically shared among many organizations, but logically partitioned using MPLS technology. The operator offers Red SARA a Virtual Private LAN Service (VPLS) that allows setting up different VPNs, which guarantee the confidentiality of the communication between the organizations linked to Red SARA. • The access links, as well as the infrastructure of the connection areas, are fully dedicated to provide connectivity between the institutions and Red SARA with encrypted communication and between Red SARA and the Internet. In the case of MINETUR, the infrastructure is fully dedicated.
A 3.3	Netherlands	The Alkmaar network infrastructure, including the uplinks to the transit provider, is fully dedicated to Alkmaar. The Mid-office infrastructure is shared with many other municipalities, who are also customers of Inter Access.
A 3.4	Turkey	There exist two types of infrastructure for Turkish Pilot. Firstly connection to TURKSAT web portal in order to use governmental services is shared. Secondly on the backend the infrastructure used to connect to the institutions to exchange information is dedicated.

Table 2-6: Infrastructure: Shared/Dedicated

2.5 Multi-homing

Multi-homing is a technique used to increase the reliability of the Internet connection for an IP network. It is generally based on the use of multiple links, provided by one (typically with different geographically located paths) or several Internet Service Providers, connecting a site with a single IP address space. Additionally, multi-homing may be based on single link/multiple IP address spaces or multiple links/multiple IP address spaces.

A 3.1	Germany	Multi-homing exists for several provider connections in different flavours: • Multi-homed Citkomm-owned autonomous system for Internet access • Backup-scenarios for DOI and MPLS access Multi-homing in the context of using different IP ranges for connection to the targets has to be discussed to evaluate the only use of PI de.government addresses versus additional use of PA addresses (or in the Citkomm case additional IPv6 address space for our own AS) for general Internet connectivity.
A 3.2	Spain	Multi-homing is provided by means of multiple links to the same ISP, connected to two different Internet Points of Presences through different access nodes. The reliability goals regarding the Internet connectivity are approached by means of redundant links and first class Service Level Agreements.
A 3.3	Netherlands	Alkmaar is multi-homed using two different POPs of the same ISP, namely A2B Internet.
A 3.4	Turkey	TURKSAT is multi-homing using two different POPs of the same ISP, namely Turk Telekom. For the pilot phase this infrastructure will be used.

Table 2-7: Multi-homing

2.6 IPv6 Service Requirements for the Telecommunication Operators

This section refers to the specific requirements regarding IPv6 services provided by the telecommunications operators considering Internet connectivity services, Virtual Private Networks connectivity services among sites, as well as other services such as DNS, e-mail, VoIP, etc.

A 3.1	Germany	• IPv6 must be fully supported, not only a few features • Routing of PI address space from de.government RIPE NCC allocation should be possible, even in small subnets down to /48 • Both uplink providers of each autonomous system must support IPv6 • MPLS backbone should support IPv6 native • DOI backbone should support IPv6 native • IPv6 must be in stable use by the provider, being part of operational products; no solution on only experimental infrastructure.
A 3.2	Spain	Regarding Internet connectivity services, the following features are required: • The operator must guarantee a reliable and robust connection to the Internet both through IPv6 and IPv4, via the same physical links. • Tunnels should be avoided inside the operator network. • The operator must have a reliable IPv4 and IPv6 upstream structure. • The operator must provide mechanisms to guarantee high availability. • The operator must provide visibility and therefore, transit and peering (directly and indirectly) of the whole global routing table, both in IPv6 and IPv4. Regarding VPN services in the Spanish pilot, the following features are required: • The operator must guarantee a reliable and robust connection between sites both through IPv6 and IPv4. • The operator must provide static and dynamic routing mechanisms. In both cases, the network performance (latency, packet loss, bandwidth, etc.) must be independent from the protocol (IPv6/IPv4) being used.
A 3.3	Netherlands	Gemeente Alkmaar requires dual stacked network connections with the same service levels for both IPv4 and IPv6 from operators. The requirements are stated in availability, bandwidth, packet loss, latency and visibility in the global routing table.
A 3.4	Turkey	TURKSAT has SLA with the telecommunications operator Turk Telekom. The operator should satisfy the items specified in the SLA such as packet loss rate, throughput, etc. For the Turkish pilot phase, the same SLA will be used and the same items should be valid for the connections between TURKSAT and the other participant institutions of Turkish pilot.

Table 2-8: IPv6 Service Requirements for the Telecommunications Operators

2.7 IPv6-Capable Platforms

Computer platforms typically refer to the combination of hardware architecture and a software framework that allows other application software to run. This section provides information and requirements about the platforms that will be used in the pilots.

A 3.1	Germany	Several server OS platforms will be used during the pilot. Main focus will be given to: • Linux – Ubuntu • Linux – Debian • Linux – CentOS • Linux – SLES • Windows Server 2003 • Windows Server 2008 • Windows Server 2008R2 • VMware The focus for clients will be on: • Windows XP • Windows 7
A 3.2	Spain	The IPv6 capability is required for the following platforms. Red SARA: • Linux – CentOS 5.2 running on Intel Quad-Core Xeon processors • Linux – CentOS 5.4 running on Intel Quad-Core Xeon processors • StoneGate 5.3.3 running on Intel Quad-Core Xeon processors • Cisco IOS 12.2 • Red Hat Enterprise 5.5 Linux running on Intel Quad-Core Xeon processors • Red Hat Enterprise 5.5 Linux running on Intel Xeon processors MINETUR network: • Firewalls (PA5050) • DNS servers – Windows 2008 Servers R2 • Load-balancers (F5) • Web Servers IIS7 – Windows 2008 Servers R2
A 3.3	Netherlands	The Netherlands pilot uses the following OSes and systems: • VMWare ESXi • Windows Server 2003 • Windows Server 2008 • Windows Server 2008 R2 • HP-UX • Junos 11.4 • Checkpoint UTM1 R75 • Blue Coat SGOS 6.x • Citrix XenApp • Citrix NetScaler
A 3.4	Turkey	The platforms that will be deployed during the pilot are listed below. The IPv6 readiness of these platforms should be checked. • Cisco IOS 12.2 • Load-balancers (F5 BIG-IP 10.2.1 Build 297.0 Final) • Red Hat Enterprise 5.3 Linux running on Intel Qual-Core Xeon processors • Ubuntu 10.0.4 • Cisco FWSM 4.1(7) • Client-side: Windows XP, Window 7

Table 2-9: IPv6-Capable Platforms

3. NETWORK LEVEL REQUIREMENTS

3.1 Dual-Stack Connectivity

Dual-stack is a technique by which components that take part in IP-based data communication can make use of Internet protocol (IP) version 4 or version 6, because both are present and available. Native dual-stack support means that a component (e.g. a host) is connected to a data network in which IPv4 and IPv6 are available directly, i.e. without use of any transition technique (e.g. IPv6 in IPv4 tunnels). Since IPv4 and IPv6 are incompatible IP protocols, each direct IP communication has to take part between compatible end systems (i.e. IPv4-to-IPv4 or IPv6-to-IPv6). For supporting IPv6 end-to-end communication many infrastructure components need to support IPv6, such as routers, clients, servers, firewalls, infrastructure services for instance DNS and DHCP, and to some extent switches too.

A 3.1	Germany	Existing infrastructure is based on IPv4. For several reasons it is to expect, that some applications are unable to transition to IPv6. For these applications the remaining of IPv4 in the network will be vital. So a fully functional dual-stack implementation will be a key feature for the whole German pilot.
A 3.2	Spain	The goal is allowing IPv4 and IPv6 connectivity using the same infrastructure, so the coexistence of both protocols is required. Although the intended approach is to use dual-stack whenever is possible, there are not initially specific requirements about dual-stack connectivity, since in the Spanish pilot the choice of the transition mechanism (dual-stack, tunnelling or translation) will be made after the IPv6 compatibility assessment for the current infrastructure has been completed.
A 3.3	Netherlands	The Netherlands pilot aims to run dual stack in all networks and systems in the pilot. As far as third parties are concerned, it will depend on their architecture, and hardware and software implementation, whether a full native dual stack implementation can be achieved.
A 3.4	Turkey	In the final quarter of 2009 Turk Telekom has started providing IPv6 connectivity to its customers. After IPv6 subnet has been allocated to TURKSAT by RIPE NCC in the 3rd quarter of 2010, the dual-stack connectivity between TURKSAT and Turk Telekom has been established using 1 Gbps Metro Ethernet Interface. On the other hand, this connection is not in use practically since then. In other words, there is no IPv6 traffic flow over this link. It is assumed that ISPs lacks best practices for IPv6 troubleshooting. Therefore, ULAKBIM and TURKSAT immediately should start some connectivity tests via IPv6 and verify Turk Telekom meets the SLA parameters of this link such as capacity, delay and packet loss.

Table 3-1: Dual-Stack Connectivity

3.2 Addressing Plan

It is crucial to setup and maintain a well-organised addressing scheme independently from the address family used in a network. With the much increased size of address space in IPv6, it is now possible to plan the addressing scheme considering new features embedding semantic information into the address itself, e.g. what type of subnet (DMZ, servers, clients) this address belongs to, etc. This is being studied in WP2.

A 3.1	Germany	For the German governmental institutions, RIPE NCC has allocated a common address space. A part of this address space will be used for the relevant IPv6 address planning. For the segmentation of the expected /48 range into the local networks a detailed address plan has to be developed. Furthermore, regarding the general Internet connectivity it has to be discussed, whether the same address range can be used or if PA address space should be used. This depends among others on the results of current discussions of the German IPv6 address concept.
A 3.2	Spain	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 assigns 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.
A 3.3	Netherlands	Since all concerned parties in the pilot are connected to the internet, they will select their own IPv6 address space (PA or PI space). For example, Seneca Hosting (www.alkmaar.nl), uses PA space from the data centre in which their servers are located. Alkmaar has its own /32 PA space as a LIR and applies zoning of the IPv6 address space in blocks of /48 among different network functionalities, for example client networks, server networks and DMZ networks. Within each functionality group, specific /64 networks are assigned to segments (or LANs), for example a /64 for all Windows servers and a /64 for all XenApp servers.
A 3.4	Turkey	TURKSAT consists of 4 network operations namely: • eGovernment Gateway • Satellite Operations (VSAT, TV and radio streaming, etc.) • TURKSAT Local Network Operations • Cable TV and Internet Due to this business level and different Network Operation Centre, IPv6 prefix has to be divided to /36 subnets: • /36 for eGovernment Gateway Datacentre (2a00:1d58:0::/36) • /36 for VSAT (2a00:1d58:2000::/36) • /36 for TURKSAT Local Services (2a00:1d58:1000::/36) • /36 for Cable TV and Internet (2a00:1d58:8000::/36)

Table 3-2: Addressing Plan

3.3 Address Allocations and Assignments

IPv6 prefixes are allocated or assigned to organisations on request following similar procedures as in the IPv4 case. In Europe and Middle East, the RIPE NCC, in its function of Regional Internet Registry (RIR), performs the IPv6 prefix allocations to Local Internet Registries (LIR), which in turn redistribute parts of their allocated address space to its customers. Organisations get allocated their IPv6 address space from a LIR, which is usually the Internet Service Provider (ISP) of that organisation. Address assignment procedure starts with an application of the organisation, which should clearly indicate the requirements of address space and a possible address distribution plan over the departments/subnets of the organisation. Another option for an organisation is to directly apply to a RIR and become a LIR or an end-user in the case of PI (Provider Independent) addressing needs.

A 3.1	Germany	German government has become a LIR by itself and maintains control over the address space allocated for use by the IT infrastructure of all German public bodies. In Germany each federal state becomes a “sub-LIR”, so it gets control over a part of the German IPv6 address space and can assign prefixes (usually /48 or /56) to federal and communal public bodies. For north Rhine Westphalia the municipalities build up an own “sub-LIR”. This “sub-LIR” is located at Citkomm.
A 3.2	Spain	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. Address assignment procedures must be compliant with the policies stated in the Spanish Public Administration Interconnection and Addressing Plan, and must respect the prefixes allocated to the organization in that Addressing Plan.
A 3.3	Netherlands	The Municipality of Alkmaar is a LIR with RIPE NCC and has been allocated the address block 2a02:2738::/32. This is being announced on AS51088 to the Internet.
A 3.4	Turkey	2a00:1d58::/32 has been allocated from RIPE NCC. 2a00:1d58::/36 is reserved for eGovernment Gateway Network and is being announced with AS47524 to the Internet.

Table 3-3: Address Allocations and Assignments

3.4 Address Configuration

IP address deployment is concerned with the configuration of IP addresses to interfaces of nodes inside an organization, more concretely with the technical process of configuring IP addresses inside each network segment. For IPv4 networks, this is commonly done with either static configuration or by using the dynamic host configuration protocol (DHCP). In IPv6, the address deployment can be performed either by static configuration or auto configuration methods (e.g. Stateless Address Autoconfiguration – SLAAC – and Stateful Address Autoconfiguration). Static configuration is strongly recommended for configuration of server interfaces: A fix IPv6 address is configured directly on the networked device. Here it is worth noting that an interface may use multiple IPv6 address at the same time.

A 3.1	Germany	For the address deployment the needs of the different network segments have to be kept in mind. For server segments a static address deployment will be a useful way. For the local networks with several client systems an automatic system must be build definitively, to reduce the manual configuration expenses to a necessary minimum.
A 3.2	Spain	In the case of Red SARA, the network architecture is based on several connection areas, each of them with a different prefix, which host a limited set of hosts running the network services such as DNS, proxy, etc. Due to this, IPv6 addresses in Red SARA network will be assigned using manual/static configuration. In the case of MINETUR network, Red SARA, according to the Spanish Public Administration Interconnection and Addressing Plan, will provide IPv6 addresses. Address assignment will be performed statically in two steps: • Previous assignment using autoconfiguration • Final allocation with static IP address assigned in the previous step
A 3.3	Netherlands	Concerning Alkmaar: network elements (routers, firewalls, etc.) will be manually configured using static IPv6 addresses. Servers and end-user devices are configured with a combination of SLAAC, for the IPv6 address and router discovery, and stateless DHCPv6 for DNS configuration. Address configuration by third parties is to be determined by those parties themselves.
A 3.4	Turkey	A medium scale address deployment, which will allow static IPv6 addressing, is necessary for eGovernment Gateway. Hence static IPv6 address deployment will be used rather than autoconfiguration methods in order to make monitoring and logging easier.

Table 3-4: Address Configuration

3.5 Enabling IPv6 in Layer-3 Devices

The IPv6 specification RFC2460[2] starts with a terminology section, which says that hosts and routers are summarized under the term node – a device that implements IPv6. The IPv6 node requirements are summarized in RFC6434[3]. In the light of these two RFCs, the requirements for a generic node can be grouped as: Communication of the IPv6-node, network management and link-specific requirements. The former is the focus of this section while the second and third group will be included in other sections of this document.

The requirements for the communication of a node include all protocols and mechanisms that are needed for the interworking of nodes and that are not specific for a dedicated device. For instance, host and router need to share the same view on protocol headers and semantic of addresses.

[2] http://tools.ietf.org/rfc/rfc2460.txt

[3] http://tools.ietf.org/rfc/rfc6434.txt

A 3.1	Germany	All backbone Layer-3 components must support IPv6 in dual-stack mode. Access routers must even support IPv6, if they are used for connection to other networks. Most used equipment bases on Linux software routers, so it is to expect that IPv6 support will be available. Some elder equipment will not be IPv6 ready. In these cases components have to be changed.
A 3.2	Spain	It is required IPv6 enablement (understood as the capability to route IPv6 traffic as well as IPv4, whatever the underlying transition mechanism) in the routers located in the connection area between Red SARA and Internet, and in the connection area between Red SARA and MINETUR's network.
A 3.3	Netherlands	Alkmaar obeys the comply-or-explain principle mandated by the Dutch Ministry of Interior Affairs, which states IPv6-support is required in all tenders issued by Dutch governments. Most equipment acquired in this way is IPv6 ready with regard to communications.
A 3.4	Turkey	TURKSAT has already been purchasing IPv6 Ready network equipment and licenses since 2008. All necessary IOS, JunOS and software upgrades will be finished in the middle of 2012.

Table 3-5: Enabling IPv6 in Layer-3 Devices

3.6 Enabling IPv6 in Management for Layer-2 Devices

Since most of the Layer-2 devices need IP addresses for management purposes, these devices should be IPv6 capable especially in pure IPv6 networks.

A 3.1	Germany	As the focus of the pilot is on enabling end user application connectivity with IPv6 the management of devices is not critical for the success. Therefore there are no specific requirements.
A 3.2	Spain	There are no specific requirements for IPv6 management of Layer-2 devices, since the use of IPv6 for managing devices is out of the intended scope of the Spanish pilot, because the network will keep dual-stack capabilities, so management can still be achieved by means of IPv4.In the future, it may be considered management achieved by means of IPv6-only, in preparation for the future removal of IPv4 in the network.
A 3.3	Netherlands	No special effort is directed at migrating network management to IPv6. Also Gemeente Alkmaar only has very limited layer-2 devices since the entire LAN is equipped with Layer-3 switches.
A 3.4	Turkey	There exist no special requirements for enabling IPv6 in management for Layer-2 devices are foreseen. The network is supposed to be working dual stack, so management of Layer 2 devices may be done over IPv4.

Table 3-6: Enabling IPv6 in Management for Layer-2 Devices

3.7 Enabling IPv6 Specific Functionalities for Layer-2 Devices

IPv6 hosts can be transparently attached to Layer-2 devices since they do not process IP headers directly. Hence, transport of IPv6 over Layer-2 devices does not need significant changes. However, in order to use some IPv6 functionality such as MLD snooping, IPv6 capabilities of these devices is important. Additionally, blocking rogue Router Advertisement messages on specific ports is a security feature that definitely should be acquired by the Layer-2 switches.

MLDv2 Snooping[4], DHCPv6 Snooping[5], Duplicate Address Detection[6], Rogue-RA Mitigation

[4] http://www.ietf.org/rfc/rfc4541.txt

[5] http://www.ietf.org/rfc/rfc3315.txt

support of the Layer-2 devices should be checked for relevant functionalities.

A 3.1	Germany	No such capabilities are used in the relevant network segments, so there are no requirements specified.
A 3.2	Spain	There are initially no IPv6 specific functionalities required for Layer-2 devices in the Spanish pilot, considering that auto-configuration will not be used. However functionalities such as Rogue-RA Mitigation may be considered, as part of the security measures. Other functionalities that may be required will be: • MLD Snooping. • IPv6 support for Telnet, SSH, HTTP, FTP, TFTP, SNMP and related MIBs.
A 3.3	Netherlands	Gemeente Alkmaar only has a very limited number of layer-2 devices since the entire LAN is equipped with Layer-3 switches which do support the features named or have support planned.
A 3.4	Turkey	There are no specific requirements since such IPv6 functionality is out of scope of the Turkish Pilot.

Table 3-7: Enabling IPv6 Specific Functionalities for Layer-2 Devices

3.8 Routing Configuration

Routing is the process of selecting path in a network along which to send network traffic. Routing in IPv6 is not very different from that in IPv4. IPv6 routers determine best paths to destinations based on metrics and administrative distances, and like in IPv4, IPv6 routers still use the longest prefix match routing algorithm to forward a packet to its destination. The main difference is that the IPv6 routers are looking at 128 bits when making a routing decision instead of 32 bits. Routers can build their IPv6 routing tables using the information manually entered by network administrator (static routing) or using appropriate algorithm to compute the best route (dynamic routing). Although default parameters may vary from one vendor to another, usually IPv6 traffic forwarding is disabled on routers. Therefore in order to use IPv6 on a router, first IPv6 address should be assigned to the related interfaces and IPv6 unicast routing should be enabled in the router.

[6] http://www.ietf.org/rfc/rfc4429.txt

A 3.1	Germany	The Citkomm network uses static routing in the WAN area. In the data centre internal backbone OSPF is used. Both solutions must be enabled for IPv6 end to end.
A 3.2	Spain	Regarding Red SARA infrastructure, routing configuration is the responsibility of the telecommunications operators that provide Internet and VPN connectivity services. Therefore, there are no IPv6 specific requirements regarding routing configuration, apart from the requirements derived from those imposed on the connectivity services mentioned previously.
A 3.3	Netherlands	Gemeente Alkmaar uses dynamic routing wherever possible and feasible. For IPv4 the only part of the network that uses static routing is the DMZ configuration. For IPv6 the same approach is favoured.
A 3.4	Turkey	2A01:0358:4F00:0002::/64 has been allocated from Turk Telekom for Interface connectivity and BGP configuration. BGP connectivity established and 2A00:1D58:0::/36 has been announced to Internet. Following requirement analysis on addressing plan, the BGP configurations should be updated if any change occurs in the current plan.

Table 3-8: Routing Configuration

3.9 Routing Protocols

Routing protocols operates between the routers through exchange of information related to topology and to the state of the network. Routers that are controlled and administrated by the same authority are grouped in Autonomous Systems (AS). Routers belonging to the same AS exchange routing information through an Interior Gateway Protocol, whereas routers belonging to different AS are using an Exterior Gateway Protocol. Internal Gateway Protocols having IPv6 support are RIPng[7], IS-IS[8], OSPFv3[9] and EIGRP. BGP[10] is worldwide used external gateway protocol and it has IPv6 support.

Dynamic routing protocols require router-id, which is a 32 bits integer. When IPv4 is used, the router-id can be auto-generated from configured IP addresses. However, if only IPv6 routing is enabled, router-id needs to be manually configured. Therefore, if dynamic routing is used, most of the organizations prefer dual-stack implementations for IPv6.

A 3.1	Germany	OSPF must be enabled for the backbone area. BGP is used for the Internet connection. Because of these components are operated by an external provider he must enable IPv6 connectivity over BGP routing.
A 3.2	Spain	In the sourcing approach for connectivity services, it is the telecommunications operator's choice to use the appropriate routing protocols to provide the demanded service. Therefore, there are no IPv6 specific requirements regarding routing protocols, apart from the requirements derived from those imposed on the connectivity services.
A 3.3	Netherlands	Gemeente Alkmaar uses OSPF for internal IPv4 routing. There is a strong desire to use OSPFv3 for internal IPv6 routing. However due to licensing issues it remains to be seen if this is economically feasible. If this is not feasible static routing for internal IPv6 will be used. For external routing BGP is used which is managed by an external party.
A 3.4	Turkey	BGP is used for external connectivity. BGP announces is being made to the ISP. For the connection between TURKSAT and the governemntal institutions there will be a P2P connection

[7] http://www.ietf.org/rfc/rfc2080.txt

[8] http://www.ietf.org/rfc/rfc5308.txt

[9] http://www.ietf.org/rfc/rfc5340.txt

[10] http://www.ietf.org/rfc/rfc2545.txt

		so static routing will be used instead of routing protocol.

Table 3-9: Routing Protocols

3.10 Load-Balancing

A load-balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of servers. Load-balancers are used to increase capacity (concurrent connections) and reliability of applications. They improve the overall performance of applications by decreasing the burden on servers associated with managing and maintaining application and network sessions, as well as by performing application-specific tasks.

Load-balancers are generally grouped into two categories: Layer-4 and Layer-7. Layer-4 load-balancers act upon data found in network and transport layer protocols (IP, TCP, FTP and UDP). Layer-7 load-balancers distribute requests based upon data found in application layer protocols such as HTTP.

A 3.1	Germany	At Citkomm network no load-balancers on network level are in use.
A 3.2	Spain	In Red SARA load-balancers are not needed. Load-balancing function is performed by the firewalls located in the DMZ of the connection between red SARA and 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, considering reassessing it once the IPv6 traffic through Red SARA becomes increasingly significant. In the case of MINETUR, load-balancers are needed to send IPv6 traffic to the servers' farm and to act as IPv6/IPv4 gateway to the backend servers inside the internal network.
A 3.3	Netherlands	Gemeente Alkmaar uses load balancers for high availability. These load balancers will be required to operate in dual stack mode.
A 3.4	Turkey	Purchasing process for the IPv6 licenses has been started and software upgrades will be finished after licenses are purchased. At the 2nd quarter of 2012 necessary configurations (Virtual IP Addresses, server pools, iRules) will be made as an additional service. After completing configurations, security and load tests will be made. TURKSAT Local Information Security group and an external Information Security company will perform the testing. Handling the dual-stack traffic, performance and security will be evaluated. For the TURKSAT local side tests, IPv6 will be implemented to test platform and servers.

Table 3-10: Load-Balancing

3.11 Virtual Private Network (VPN)

A Virtual Private Network (VPN) allows the use of a secure channel between remote locations (e.g. office) or a remotely operating co-worker (road warrior, teleworker) and an organisation's network over public communications infrastructure like the Internet. So the remote unit can get access to the local network and use its resources, e.g. file services, printers, mail systems, internal Web services, in general all servers and services of the internal network. This document refers only to ISO/OSI Layer 3 VPNs.

The remote site, the organisation's home network and the transition network between these

two locations are the three main members of a VPN. All these three components should be considered in enabling IPv6. The IPv6 configurations in remote site (or the client software in case of a single remote user), the IPv6 support of the transition network (IPv4-only, IPv6-only and dual-stack) and the IPv6 configurations of the VPN gateway in organisation's home network are the main consideration in this process.

A 3.1	Germany	Citkomm and its customers use almost all flavours of VPN e.g. site-to-site, remote user to home network via conventional or mobile networks. The VPN handles only IPv4 traffic today. IP assignment is done in a centralized manner i.e. the central VPN gateway provides IP addresses for all connecting gateways and clients and the remote components accept the routing information from the central too. As remote connecting devices we handle our own Linux based gateway appliances (iWAN) and software based solutions for home and mobile workers. Further detailed information regarding these devices is given in VPN Points of Entry/Exit section.
A 3.2	Spain	Red SARA hosts a set of different VPN. Among them, only the VPN that connects Ministries (National Government), Autonomous Communities (regional Governments) and singular entities (constitutional bodies and such) are 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. Additionally, the VPN will use IPsec as the mechanism to secure VPN connections in the connection areas of Red SARA, making sure that all communication in the network is encrypted.
A 3.3	Netherlands	Communication between the back office servers of Gemeente Alkmaar and the mid-office which is hosted by Inter Access is done over an IPSec VPN connection over internet. This is to ensure confidentiality of transmitted data. However due to RFC1918 address space conflicts this IPSec connection makes heavy use of NAT which complicates management and troubleshooting. In the pilot the aim is to run a dual stack IPSec VPN tunnel and migrate communication to IPv6.
A 3.4	Turkey	Currently TURKSAT and governmental institutions are establishing their communication using VPN over IPv4 if the connection is not established over dedicated lines. In the pilot this communication will be done using VPN over IPv6 if the line is not dedicated.

Table 3-11: Virtual Private Network (VPN)

3.12 Application Level Gateway (ALG)

Application Level Gateway operates at application layer of the ISO/OSI model. An ALG is positioned at the border between an untrustworthy network (e.g. the Internet) and a trusted LAN. Typically, the ALG appears to the outside world as an end point application server, but in fact, the ALG inspects each incoming packet or request and dynamically change the contents of a packet or request.

Application Level Gateways can also be used as an addition to translation mechanisms that are used for communication between IPv4-only nodes and IPv6-only nodes. ICMP ALG performs translation between ICMPv4 and ICMPv6 (e.g. IPv4 ping is translated to IPv6 ping). DNS ALG performs translation between DNSv4 and DNSv6 (e.g. when IPv4 host does a DNS query for a device with only IPv6 connectivity, then the DNSv4 request is translated to DNSv6 request). The use of ALGs for IPv4 to IPv6 translation is defined in Network Address Translation – Protocol

Translation (NAT-PT)[11], is now deprecated due to its limitations, all of which are documented in "Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic status"[12].

A 3.1	Germany	Application level gateways and Firewall components are used at several points in the Citkomm network. Commercial solutions are in use for exposed locations like DMZ. These components must be evaluated for IPv6 in special manner. The further firewall systems must be enabled for IPv6, too. In the latter case the management of the IPv6 rules and their centralised distribution needs special attention.
A 3.2	Spain	One of the goals of the Spanish pilot is to test the interoperability between administrative units in different IPv6 readiness stages. In that sense, it is expected that an administrative unit that has not initiated the transition to IPv6 will be able to access, using IPv4, services offered in IPv6. Therefore, in the design of the proposed solution it is required a transition mechanism to allow users that have only IPv4 capabilities access to IPv6-ready applications.
A 3.3	Netherlands	Gemeente Alkmaar uses several application level gateways. These gateways are primarily used for security and auditing purposes. They can also provide translation services from IPv4 to IPv6 and vice versa . These translation features can be used during transitioning of services but are not planned as the aim is to provide native dual stack services.
A 3.4	Turkey	ALGs are used at some points in TURKSAT network for auditing purposes. Although the main purposes is not to use ALGs in Turkish pilot, if necessary ALGs may be deployed to audit the traffic or make IPv4-IPv6 transition possible where there is no other eligible solution.

Table 3-12: Application Level Gateway (ALG)

3.13 IPv6 to IPv4 Access: IPv6-Only Systems

This functionality uses address family translation, which is applicable in cases where servers or hosts exist in IPv4-only network and want to communicate with IPv6-only hosts. An example could be when existing or new content providers decide to offer services to IPv4-only and IPv6-only users while servers stay in IPv4-only network environment.

The main address family translation methods are NAT-PT and NAT64. NAT-PT is deprecated and must not be used; in addition has the problem that it requires ALGs for DNS translations while NAT64 does not require this facility. The current situation with NAT-PT is summarized in the previous section.

NAT64 can be implemented using stateless or stateful translations. Stateless NAT64 is defined in IP/ICMP Translation Algorithm[13] and it uses translation algorithm for mapping IPv6 addresses to IPv4 addresses and vice versa. While performing translation, it does not maintain any bindings or session state, which is the case with classic NAT44. Stateful NAT64 is defined in Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers[14] and uses stateful

[11] http://www.ietf.org/rfc/rfc2766.txt

[12] http://www.ietf.org/rfc/rfc4966.txt

[13] http://www.ietf.org/rfc/rfc6145.txt

[14] http://www.ietf.org/rfc/rfc6146.txt

translation mechanism for translating IPv6 addresses to IPv4 addresses and vice versa. Like classic NAT44, the mechanism is stateful because it creates bindings or session state while performing translation. Mapping can be dynamic or static (manually defined). Stateful NAT64 can handle UDP, TCP and ICMP packets.

A 3.1	Germany	Currently there is no need for NAT64 as a network infrastructure component expected. There will be gateways to enable IPv6-only to IPv4-only communication and vice versa, but they are intended to be implemented as proxy systems, working on the upper ISO/OSI levels.
A 3.2	Spain	It is expected that users outside Public Administrations (citizens, companies, etc.) will be able to access, using IPv6-only access, Public Administration Web Portals that are offered only in IPv4. Thus, a mechanism to assure IPv6 access to IPv4 applications is required.
A 3.3	Netherlands	Gemeente Alkmaar does not plan on using NAT-PT nor NAT64. If translation is required this will be implemented in the existing ALG's.
A 3.4	Turkey	EGovernment services are planned to be made available both over IPv4 and IPv6 at the end of the pilot. Also connection between TURKSAT and the governmental institutions is available over IPv4 and will be working dual stack at the end of the project. Hence there are no expected problems for IPv6-only systems to use these services.

Table 3-13: IPv6 to IPv4 Access: IPv6-Only Systems

4. NETWORK HARDWARE REQUIREMENTS

4.1 Routers/Switches

Routers are special purpose Layer-3 devices that mainly perform two actions: Path selection and switching. Furthermore, they have to implement one or more routing protocols suitable for routing IPv6 packets. Depending on where the router is placed in the network, this can be IS-IS[15], BGP[16] or RIPng[17]. In addition, routers might also act as DHCP relays, so the respective RFCs have to be studied as well.

Switches connect network segments/devices and process/forward data at Layer-2. Although Layer-2 devices seem not to be effected with the change of the Layer-3 protocol, there are some points that should be considered. Firstly, switches used in enterprise settings are usually configured and monitored centrally, so they will have to implement management protocols to an extent similar to routers. Secondly, IPv6 heavily relies on multicast based mechanisms e.g. neighbour discovery. So switches will have to implement the respective RFCs to recognize and handle multicast messages. Switches should also filter malformed packets, which might adversely affect global networking. This includes inspection of Router Advertisement (RA), Neighbour Solicitation/Advertisement or Duplicate Address Detection (DAD) messages. Erroneous packets should not be made available on other switch interfaces. Additionally, most modern switches can work at Layer-3, so Layer-3 requirements should be checked for these switches.

A 3.1	Germany	Router functionality will be a must for IPv6 as outlined under “Network Level Requirements”. All used equipment has to be checked for IPv6 compatibility and interoperability with the other routing components used in the Citkomm network, including the provider operated uplink routers. Switching infrastructure in the Citkomm network is just used for Layer-2 switching. Further features, especially Layer-3 functions, are not available or turned off to keep a clear structure of the network. Therefore for the pilot less risk is expected from these components. Nevertheless at the end for each used switch platform it has to be proofed that it operates really transparent to the Layer-3 protocol.
A 3.2	Spain	IPv6 compatibility is required in means of the capability to switch, forward and route IPv6 traffic in the routers and switches located in the following connection areas of Red SARA: • The connection area between Red SARA and Internet. • The connection area between Red SARA and MINETUR network. Additionally, IPv6 compatibility is required in the routers and switches of MINETUR network that link the connection area with Red SARA to the hosts where the business applications offered over IPv6 are running.
A 3.3	Netherlands	Support for IPv6 is required for all network elements in the network of Gemeente Alkmaar

[15] http://www.ietf.org/rfc/rfc5120.txt

[16] http://www.ietf.org/rfc/rfc4271.txt

[17] http://www.ietf.org/rfc/rfc2080.txt

		operating at layer 3 or higher. The leading method of attaining this has been the comply-or-explain principle mandated by the Dutch Ministry of Interior Affairs, which states IPv6-support is required in all tenders issued by Dutch governments. This principle also includes specifications to which equipment must adhere and refersto RIPE-554.
A 3.4	Turkey	IPv6-support, for all the equipments purchased, is mandated by a circular published by the Turkish Government in 2010. Obeying this circular, there is no expected problems for IPv6-support of the network equipment either in TURKSAT or in the other governmental institutions.

Table 4-1: Routers/Switches

4.2 Entry/Exit Points of VPN's

A general description and requirements for the central VPN gateway are given in Virtual Private Network section. This section provides requirements regarding the VPN gateways that will be deployed throughout the pilots where necessary.

A 3.1	Germany	The central VPN gateways are Linux based routers. They are connected to a distribution network and they deploy dynamic routing. They are managed centrally and provide configuration information to the connecting clients, mobile users as well as site-to-site connections. Firewall rules are applied on the VPN gateways. The used VPN software is OpenVPN. Requirements: • The underlying OS must be fully IPv6 capable. • The used routing protocols and the software packages must support IPv6. • The firewall and its administration interface must support IPv6. • The address assignment and its admin interface must support IPv6. • Encryption must meet the requirements (standards, laws, etc.). • Certificate based authentication must be supported. Site-to-site gateways are Linux based appliances called iWAN. Since they are managed centrally, VPN related requirements include: • The underlying OS must be fully IPv6 capable. • Should be able to work behind NAT (e.g. connection to central VPN gateway). • Static IPv4 and IPv6 routing is deployed, no dynamic routing protocol requirement. • Must cooperate with central VPN gateway (i.e. certificate based authentication). Home Office VPN gateway is a pure software solution, based on OpenVPN. Here the requirements are: • The underlying OS (Windows XP, Windows 7) must be fully IPv6 capable. • Must able to work behind NAT (e.g. connection to central VPN gateway). • Must accept central given configuration (i.e. routing information). • Admin tools, by means of which preconfigured packages are built, must support IPv6. • Must support certificate-based authentication. Requirements for mobile VPN gateway: • IPv6 support from underlying OS (iOS, Android). • Must able to work behind NAT (e.g. connection to central VPN gateway). • Must support certificate-based authentication. • Must accept central given configuration (i.e. routing information). • Admin tools, by means of which preconfigured packages are built, must support IPv6.
A 3.2	Spain	The entry/exit points of the VPN that will be established through Red SARA will be created by the external security subsystem located in the connection areas between Red SARA and the organizations linked to it.
A 3.3	Netherlands	The entry and exit points of the VPN between Gemeente Alkmaar and Inter Access are dedicated to this VPN connection. If it turns out that IPv6 is not supported on these devices they can be replaced with minimal impact and cost.
A 3.4	Turkey	VPN connections will be established between TURKSAT and the governmental institutions wherever a shared line is used. The equipments at these points will be checked for IPv6 and VPN capabilities and will be replaced where necessary. IPv6-support is expected to exist in most of the devices according to the circular on the IPv6-support of the purchased devices.

Table 4-2: Entry/Exit Points of VPN's

4.3 Security Servers and Services

Security servers and services provide actions such as, intrusion detection/prevention, packet filtering and deep packet inspection in a network.

A 3.1	Germany	Security services are mostly integrated features in used ALG/firewall systems. Therefore only few specific requirements exist besides the necessary enabling of some software based network probes for IPv6.
A 3.2	Spain	The security servers within the scope of the Spanish pilot are those located in the connection area between Red SARA and the Internet and in the connection area between Red SARA and MINETUR network. These servers offer the following security services: • Intrusion detection and prevention • Firewall record management The requirements for these security services are detailed in the items referring to IDS, IPS and Firewalls.
A 3.3	Netherlands	Gemeente Alkmaar does not use specific security servers. Security services are integrated in the firewalls and application level gateways. The requirements for these will be described in the respective items.
A 3.4	Turkey	All the security servers and services should be checked for IPv6 support. Related servers and services (firewalls, IPs/IDSs etc.) are investigated in the upcoming sections in details. Also governmental institutions which will be connected to TURKSAT should be informed about these requirements to be applied on their side.

Table 4-3: Security Servers and Services

5. BUSINESS APPLICATIONS REQUIREMENTS

5.1 List of Relevant Applications

This section covers the list of applications relevant to the pilot projects. Obtaining a comprehensive list of all applications and services running inside an IT infrastructure can be a complex task. The easiness of this procedure depends on the state of documentation of the network, complexity and variety of the IT infrastructure elements and offered services, the clarity of responsibilities etc.

A 3.1	Germany	Citkomm operates a wide bandwidth of applications in its backbone. So for the transition of these applications the pilot needs to cooperate with several application developers. Due to the structure of the application market for local administrations most of these companies are small ones with widely varying competences regarding innovations on the network level. Furthermore it is not unusual that such products are based on legacy technologies or at least use some functions or components of older technology in the depths of their code. In this case the enabling for an IPv6 environment might present special challenges in dual-stack implementation. So alternative solutions of enabling the applications for IPv6 or other kinds of workarounds will have to be found. A specific challenge bases on the fact, that the operational applications are developed by a variety of companies with individual focuses on used technologies and implementation strategies. Application families compliant to a unique base technology are expected be found only in rare cases. So there will be a need to have a questionnaire about IPv6 readiness of their products among the application makers. A list of checked applications and components and the results of their evaluation for IPv6 transition will be updated continuously.
A 3.2	Spain	The relevant applications 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 chosen application in the pilot for demonstrating IPv6 enablement of eGovernment services is eITV. eITV service replaces the existing paper-based ITV card (the card used to register the technical inspections required by law made on motor vehicles) by an electronic card, as well as all the face-to-face procedures by other electronic procedures. Before eITV, to register a vehicle in Spain a manufacturer had to rely on an ITV paper card. For purchasing this ITV card, vehicle manufacturers had to provide in person to MINETUR with several documents that, once reviewed by MINETUR, allowed the manufacture to obtain the card on paper. Since the data from this card has to be supplied by vehicle manufacturers, the manufacturers had to print several copies of the same card with the data of the vehicle they want to register and send them to the stakeholders involved in the process: Directorate General for Traffic (DGT), financial institutions, car dealers, regional governments. With the new ITV service the old cards on paper have an electronic format. Hence, all face-to-face control procedures prior to the purchasing approval become electronic processes that do not require the presence of vehicle manufacturers in MINETUR and that allow vehicle manufacturers to have information at any time of the status of their request. Besides sending the ITV card to the different stakeholders is carried out in an electronic way, avoiding the costs associated with moving paper. Additionally, DGT can consult electronically MINETUR the status of the card with the purpose of a subsequent registration of the vehicle, what it was not possible when using a paper-based procedure. Regarding security measures, eITV cards incorporate electronic signature and transmission is made using a secure communication channel, thus ensuring the integrity, confidentiality and authenticity of the data.
A 3.3	Netherlands	The Alkmaar pilot focuses on enabling IPv6 on multiple services in their online digital service portal. Here the services are listed that require e-identification:

		• Request, modify or discontinue direct debit agreement • Request passport • Request drivers license • Request digital customer file • Request dutch nationality • Request dutch identity card • Request marriage / registered partnership • Request registration new born child • Request newborn child parental recognition • Request extract of civil status • Request extract of administrative record • Request disposal of electronic devices • Request disposal of bulky household waste • Request disposal of pruning Waste • Request Citypass Alkmaar • Request remittal • Request school transportation • Request permit for use of municipal land • Request felling permit • Filing Objections • Register dogs • Consult Cadastral information • Monitor delivery time of travel documents
A 3.4	Turkey	In Turkish Pilot, Turkish eGovernment Gateway portal, used by over 13 million citizens, will be made available over IPv6. Using this portal citizens have access to their records regarding to several services such as military services, health services or social security services. Also IPv6 connection will be established between TURKSAT and the chosen governmental institutions.

Table 5-1: List of Relevant Applications

5.2 Types of Access to the Applications: Internal/External

The applications can be grouped with respect to their network usage patterns as the following:

- Network connections from user/client to server/datacentre, client components (e.g. dedicated client, pure Web browser, terminal server session, etc.).
- Connections can use just the LAN (with high bandwidth and low latencies), any kind of corporate network including VPN or they could pass the public Internet with its whole set of possibilities of connectivity (IPv4-only, dual-stack, maybe IPv6-only, IPv4 with private addresses and local or carrier grade NAT).
- Network connections of the server/central components: Front systems (load-balancer, reverse proxies, etc.), middleware components (single sign on, SOAP, RPC, etc.), backend connections (databases, archive systems, storage systems/file services, backup systems, etc.) and base system components (cluster, virtualization systems, etc.).
- Last but not least there are data exchange connections for import and export of datasets, which operate offline or time triggered. It should be possible to consider those

connections separately, i.e. to enable them for IPv6 independently from the other data connections.

It is generally assumed that external connections are initiated from the outside of the corporate network. In this manner, internal connections are the ones that are initiated within the scope of the corporate network. However, the definition of internal/external connection may change depending on the infrastructure.

A 3.1	Germany	Due to the network segments chosen for the pilot externally as well as internally accessed applications are in the scope of the pilot. Applications with external accesses are concentrated in the DMZ segment. Internal access is typically directed from a Client network to a backbone segment. But for backed communications also other communication relationships may occur.
A 3.2	Spain	Regarding the Web Portals, both internal and external access is required. Internal access is here referred to the access from the networks of any of the organizations connected to Red SARA, whereas external access is referred to the access from users outside the Public Administrations through Internet. Regarding business applications provided by MINETUR, the access would be external to the MINETUR (by other administrative unit outside the Ministry), but internal to the Red SARA, that is, with no access through Internet.
A 3.3	Netherlands	The focus of the Netherlands pilot is services offered to citizens. As such, most access will be from external users. The services are mainly provided via HTTP/HTTPS over the internet. The aim is to make these services available to IPv4-only users, dual stack users and IPv6-only users. Data exchange is performed over a VPN connection. The organisation of Gemeente Alkmaar also uses the mid-office services directly via HTTP/HTTPS.
A 3.4	Turkey	The main application is the EGG portal which is used by citizens. The access is established over HTTPS. On the backend there will be connections established between TURKSAT and the governmental institutions over IPv6.

Table 5-2: Type of Access to the Application: Internal/External

5.3 Protocol Support Required: IPv4/IPv6/Both

As IPv4 is the legacy protocol, it is supported by today's applications. During the transition, IPv6 support of the applications is required; however it is not mandatory and depends on the transition mechanism. Most applications will require dual-stack support but it will be possible to identify applications where a Web client can connect via IPv6 to an application level gateway or a reverse proxy, from which the server can be reached via pure IPv4. Other backend connection of the server, where data is exchanged with third parties, has to be considered separately and can operate with different network connections than the frontend does.

A 3.1	Germany	Dual-stack implementation is the aspired solution for all end user connection. To reduce the pilot's complexity the backend communication of applications will be subordinated the client access. This is feasible because of backend communication is limited to local networks in the data centre in almost all cases, whilst client communication needs WAN connectivity.
A 3.2	Spain	Both IPv4 and IPv6 support is required for the relevant applications mentioned previously.
A 3.3	Netherlands	Since no assumption can be made as to which protocol a user will support, dual stack is required for all relevant services offered to citizens. For the IPSec VPN tunnel, migration to IPv6-only is to be studied after dual stack is implemented.
A 3.4	Turkey	For TURKSAT and the pilot phase, current infrastructure is working over IPv4. At the end of the project the services will be provided over IPv6. Therefore services require support for both protocols.

Table 5-3: Protocol Support Required: IPv4/IPv6/Both

5.4 Need of Globally Routable Addresses

In the "early" IP-based (post-DARPA) Internet all nodes that were connected via this global network had unique, globally routable IPv4 addresses. This fact became one of the success factors of the Internet, known as the "end-to-end communication principle". With the ever more increasing number of IP-connected devices IPv4 world ran into a shortage of available unique addresses. Therefore IPv4 address reuse has been in place for many years now in the form of IP network address translation (NAT)[18] together with (non-unique) private IPv4 addresses[19]. However NAT has the disadvantage of breaking the end-to-end connections creating many troubles to applications.

For these reasons IPv6 was designed without any NAT functionality in mind. The immense address space of IPv6 means that again, each and every IP-capable device can get one or several globally unique IP address (per interface) and that no IPv6 address translation is needed. If desired, protection mechanisms that disallow incoming connections, at least to certain ports, can be achieved also without NAT[20].

For today's communication patterns this principle is extremely valuable, as it allows the use of applications with direct connections, without complicated and error-prone NAT-workaround solutions. Applications which most benefit from unique, globally routable IPv6 addresses are those for Voice over IP (VoIP), media and cloud data access, access to home servers and home automation systems and any peer-to-peer mechanisms, for example a distributed file storage.

[18] http://www.ietf.org/rfc/rfc1631.txt

[19] http://www.ietf.org/rfc/rfc1918.txt

[20] http://www.ietf.org/rfc/rfc4864.txt

A 3.1	Germany	Global routable addresses from the central address allocation for the German government 'de.government' will be used for the project.
A 3.2	Spain	For the Web Portals within the scope of the Spanish pilot, globally routable addresses are required, since they will be accessed through Internet. For the business applications provided by MINETUR within the scope of the pilot, globally routable addresses are not required, since they only will be accessed through the internal network (Red SARA). However for management simplicity it is not expected to use ULAs, so Global Unicast Addresses (GUAs, and consequently globally routable), will be the default configuration for the entire network.
A 3.3	Netherlands	For services presented via the Internet, globally routable addresses will be required. For internal services on IPv4, RFC1918 address space is used. Internal services on IPv6 will use globally routable addresses to ease management and troubleshooting.
A 3.4	Turkey	EGG servers use globally routable addresses to be reachable over the Internet. On the other hand, connections between TURKSAT and governmental institutions deploy globally routable addresses.

Table 5-4: Need of Globally Routable Addresses

5.5 IP Address Management by the Application and Use of Literal Addresses

This section refers to the format of literal IPv6 Addresses used in URIs and URLs for use in web browsers to identify services that have access through an IPv6 network. Literal addressing syntax for an URL containing a literal IPv6 address must enclose the IPv6 address in "[ ]", as defined on the RFC2732[21]. The RFC indicates that this format is compatible with Microsoft Internet Explorer, Mozilla and Lynx.

A 3.1	Germany	All application addressing in the Citkomm network is based on DNS addressing. In rare cases, there occurred limitations for this approach so literal addressing is in use. It is expected that such applications are still focused on IPv4 and therefore a transition to IPv6 will not be possible for this components.
A 3.2	Spain	In the case of Web Portals IPv6 accessible through Red SARA, due to the web architecture of the system, the Web server which hosts the Portal, by means of configuration files, performs the IP address management. It is therefore required for this Web server to be able to manage IPv6 addresses as well as IPv4. All the applications will use DNS and literal addresses are not expected and moreover, considered harmful in order to facilitate the transition. In particular, two dual-stack DNS servers will be required within the DMZ of MINETUR to handle the DNS requests related to the pilot. They will be accessed by both IPv4/IPv6 protocols and will resolve addresses regardless of the protocol used in requests.
A 3.3	Netherlands	Literal addresses are discouraged in the network of Gemeente Alkmaar. They are only used in firewall configurations and a few legacy applications which are outside the scope of the pilot.
A 3.4	Turkey	Literal addresses are not planned to be used throughout the pilot. All applications will be accessible using DNS records.

Table 5-5: IP Address Management by the Application and Use of Literal Addresses

5.6 Web Applications

This section provides requirements regarding the Web applications that will be deployed

[21] http://www.ietf.org/rfc/rfc2732.txt

among the national pilots such as Web portals.

A 3.1	Germany	In the Citkomm network several web applications are operated. Using consequent design patterns of web applications in most cases the applications should not be affected by a transition of the IP protocol version. Due to the actual mismatch of some implementation to the pure design guideline the ability for transition has to be checked for each single application responding application component.
A 3.2	Spain	Web applications relevant to the Spanish pilot are the following: • Web Portals operated by Spanish Public Administrations to be made IPv6 accessible through Red SARA. • Web services provided by MINETUR to be consumed by other administrative units outside the Ministry, related to the eITV application on which the pilot is based. The eITV pilot will be based then on a service-oriented architecture (SOA) over an open and interoperable solution due to the large number of stakeholders that are participating in the eITV process: • On one hand it will be developed as a Web application for vehicle manufacturers in order to apply for a card authorization to MINETUR. Manufacturers will be able to know at any time the status of their requests. • Another Web application for internal management will be developed, from which MINETUR managers will be able to carry out all the tasks relating to the processing of requests. Both Web applications use ASP.NET technology, since the eITV pilot will be supported on a Microsoft Framework.
A 3.3	Netherlands	The eGovernment services which are the centre of attention in the Netherlands pilot are all web applications. The use of IP addresses in these applications remains to be verified. Also of interest is the interworking between the web services and the consolidated government authentication platform for citizens, Digid.
A 3.4	Turkey	eGovernment Gateway includes various Web applications. These applications will be checked for IPv6 support and will be modified accordingly.

Table 5-6: Web Applications

5.6.1 Web Server

A Web server aims at delivering Web pages. Any computer can be turned into a Web server by installing HTTP server software and connecting the machine to the Internet. HTTP servers treat and serve requests that follow the client/server communication, using HTTP developed for the World Wide Web.

A 3.1	Germany	Citkomm operates several web servers, even for external or internal access. They base on different platforms, like Typo3, other Linux based content management systems. The production bases on:
		• Common web server implementations
		  ○ apache
		  ○ Windows IIS
		• For connectivity reverse proxy systems are used as
		  ○ squid
		  ○ nginx

A 3.2	Spain	Red SARA offers to the entities linked to it a web content publishing service. This service is provided by means of Apache servers located in the connection areas, so that the connected entities can host in those servers the contents that they want to be accessible by other entities internally through Red SARA. This way, security is increased, since the internal network of the

		organization is not accessed. It is intended to enable IPv6 connections only in those Web servers involved in the provision of the services within the scope of the pilot, that is, Public Administration Web Portals and business applications offered by MINETUR. Depending on the final solution, this may imply enabling IPv6: • In the Web servers located in the connection areas between Red SARA and the entities owners of the Portals to be made IPv6 accessible, in the case that Red SARA access to the contents of the Portal is achieved by means of these servers. • In the Web servers of the connection area between Red SARA and MINETUR, if the access to the business applications is made through them. Additionally, IPv6 is required for the Web servers in MINETUR servers' farm that will be hosting the Web applications used by vehicle manufacturers to access the information on ITV cards.
A 3.3	Netherlands	Gemeente Alkmaar uses Microsoft Internet Information Server and Apache for web servers. The mid-office services are run on Oracle Application Server 11g. All these HTTP servers are certified for IPv6. However for the Oracle environment all plug-ins that are used will have to be identified and checked for IPv6 readiness.
A 3.4	Turkey	Web servers running in the EGG server farm consists of Apache servers. These servers are known to have IPv6 support.

Table 5-7: Web Server

5.6.2 Virtual Hosts

Multiple domain names can be hosted on a single IP address. This condition leads the fact that a unique server can share its resources to deliver basic services to multiple websites. All the customers of the virtual host can share the Web services and the server resources.

Two types of virtual hosts can be distinguished respectively name-based and IP-based. Name-based virtual hosting is based on the host name presented by the client. In that case a single IP address can be used for several websites. With Web servers that support HTTP/1.1, users send the hostname from the URL typed in the address bar of their browser. Afterwards the server can use the Host header required in all HTTP/1.1 requests, to determine which website the user has requested. In the other case, IP-based virtual hosts use a distinct IP address for each host name associated to a domain name. In other words, each site is associated to a unique IP address. In that case, the Web server is configured with multiple physical and/or virtual network interfaces or also multiple IP addresses on one interface.

A 3.1	Germany	Virtual hosts are used excessively for web services in the Citkomm network. Therefore the transition process must take special attention to an operational solution for these existing implementations.
A 3.2	Spain	Red SARA Apache Web servers mentioned above can offer virtual hosting if it is needed by the organization in whose connection area they are hosted. Depending on the final solution, it may be required using virtual hosts in the Web servers that are intended to accept IPv6 connections, in which case these virtual hosts should support IPv6. In the case of MINETUR Web servers, the pilot will be deployed over virtual hosts with the following functionalities: • A Web service on a virtual host that allows applying for the issuing of the eITV card. • A Web service on a virtual host that allows the vehicle manufacturers to know the state of their requests. • A Web service on a virtual host that allows the vehicle manufactures to send the eITV cards. These cards include advanced electronic signature.

		• A Web service on a virtual host that allows the vehicle manufactures to cancel the eITV cards sent. • A Web service on a virtual host that allows the vehicle manufactures to modify the eITV cards sent. • A Web service on a virtual host that allows the vehicle manufactures and DGT to know the eITV cards sent.
A 3.3	Netherlands	Name based virtual hosts are not widely used for externally accessible web services of Gemeente Alkmaar because these are secured with TLS. However multiple web services for communication between mid-office an back-office are frequently run on a single server. If transitioning the IPSec VPN tunnel for this communication from IPv4 with IPSec and NAT to IPv6 and IPSec is to be successful all these services will have to be IPv6 enabled.
A 3.4	Turkey	Virtual hosts are deployed in the current infrastructure in TURKSAT. Web servers' IPv6 support should be checked for the used web server applications. For the Turkish Pilot case virtual hosts created using Apache has IPv6 support.

Table 5-8: Virtual Hosts

5.6.3 Application Servers

Application servers support all application operations between users and organization's backend business applications or databases. Application servers offer a complete execution context for real stand-alone applications, applets and other components. They provide software applications combined with services such as security, data services, transaction support, load-balancing and management of large distributed systems. They are often referenced to Web servers that support the Java Platform, Enterprise Edition. In fact, Java EE defines the core set of API and features of Java Application Servers. An application server handles high-end needs, so it is often based on redundancy, monitoring and high-performance distributed application services that support complex database access.

A 3.1	Germany	Several application servers are in use for Citkomm web services. The following systems are in use with different software releases: • Tomcat • Glassfish • JBoss • Oracle IAS
A 3.2	Spain	In the case of Red SARA, there are no application servers belonging to its network, so these requirements are not applicable. Application servers used by the Web Portals that will be IPv6 accessible through Red SARA are hosted and managed by the Portal owner organization, so their transition to IPv6 is out of the scope of the pilot. In case of MINETUR, the application server will be deployed on Microsoft Internet Information Server.
A 3.3	Netherlands	Gemeente Alkmaar uses Oracle Application server in the mid-office and Apache Tomcat for web services which connect the mid-office to the back-office. These will all have to be IPv6 enabled to provide the e-government service over IPv6.
A 3.4	Turkey	Application servers will be deployed through the pilot. For some application servers IPv6 support should be checked (e.g. Glassfish).

Table 5-9 Application Servers

5.7 Application Level

5.7.1 User Front-End

The user front-end is the interface that the user is interacting with. Therefore, it is important that it has IPv6 support, as there could appear IPv6-only clients in the public Internet in a near future. During the IPv6 support of the User Front-End components, non-PC front-ends should be taken into account, i.e. public Web front-ends should be tested using current mobile devices over IPv6.

A 3.1	Germany	Many applications within the Citkomm network are based on Client Server architecture. Therefore the transition of the client component will be one essential for a successful transition for the application. Due to the individual implementations of the different applications the possible problems will be very individual for each application. For applications based on centralised systems like web applications, the transition is expected more lissom, because of more standardisation in basic technology can be assumed.
A 3.2	Spain	In the case of the Web Portals belonging to Public Administrations that will be IPv6 accessible through Red SARA, user front-end will be the Web browser that the citizen is using to interact with them. In order to make possible the foreseen scenario in which the user accesses the Web Portal using IPv6, it is required that the Web browser, as well as the underlying operating system, supports IPv6. However, since user equipment is out of the control of the organizations participant in the pilot, these requirements can be only demanded to the equipment used to perform the tests to verify the appropriateness of the implemented solution. In the case of MINETUR application, the front-end solution will be based on Microsoft Internet Information Server.
A 3.3	Netherlands	The e-Government services which are the primary target of the Netherlands pilot are provided over HTTP. As such, the front end used by citizens is a web browser and beyond control of Gemeente Alkmaar.
A 3.4	Turkey	There are no major modifications planned on the user interface. In order to raise public awareness, a notification icon or a tiny banner may be displayed, if connection is established on IPv6.

Table 5-10: User Front-End

5.7.2 Middleware Connection

The ability of middleware components to talk IPv6 can, but must not necessarily influence the operation of the application from the customers or users point of view. It will depend on the architecture of application, server and network landscape, how much IPv6 must or can be spoken in the setup.

A 3.1	Germany	Middleware differs significantly in architecture, compared to the client infrastructure. In several cases the middleware component is even part of the application front-end communication, not only for backend communication. The transition of those components is necessary for a successful application transition. This point has to be worked out for each relevant application in detail.
A 3.2	Spain	Regarding Web Portals IPv6 accessible through Red SARA, some middleware connected to the Portal may exist in order to make possible the provision of the services offered to the citizens by the Portal. However, this middleware is managed by the organization that owns the Portal, so their transition to IPv6 is out of the scope of the pilot. In the case of MINETUR eITV application, middleware will be integrated in application servers and balancers described previously, offering performance, availability, scalability, security and supporting the collaborative management in use.
A 3.3	Netherlands	For transitioning the VPN connection between mid- and back-office to IPv6 all middleware is required to support IPv6.
A 3.4	Turkey	Current middleware system that is used in eGovernment Gateway is compatible with IPv6. After configuration, it will work seamlessly with IPv6 operations.

Table 5-11: Middleware Connection

5.7.3 Backend Services and Interfaces to Other Applications

Backend connections can often be viewed independently from the frontend ones. Their IPv6 support is not as crucial as the user front-end since they are not communicating with the users directly. How much power should be invested in making backend connections run over IPv6 will depend on the actual situation.

A 3.1	Germany	Backend communication will be enabled for IPv6, if it is possible without dealing with heavy challenges. Due to the focus of the pilot on the front-end communications in all other cases the backend transition will only be driven subordinated.
A 3.2	Spain	In the case of MINETUR eITV application, the backend database will be implemented using IPv4 protocol, with the load-balancers managing the translation between IPv6 to IPv4.
A 3.3	Netherlands	The connection between the middle ware of the back-office and the back end systems is not a direct part of the Netherlands pilot.
A 3.4	Turkey	On the backend side there will be connections between TURKSAT and the chosen governmental institutions established over IPv6.

Table 5-12: Backend Services and Interfaces to Other Applications

5.8 Application Security

Application security deals with preventing exceptions in the security policy of an application or the underlying system (vulnerabilities), which may cause from flaws in the design, development, deployment, upgrade, or maintenance of the application.

A 3.1	Germany	Security aspects are part of the design guidelines for Citkomm self-developed applications. These guidelines will have to be reviewed regarding the IPv6 requirements and specifics. Citkomm checks its operated applications for vulnerabilities on network and application level at initial release or activation, major release changes and periodically. As part of the necessary quality inspection of the transition relevant applications need to be subject to an adequate check, to reduce risks.

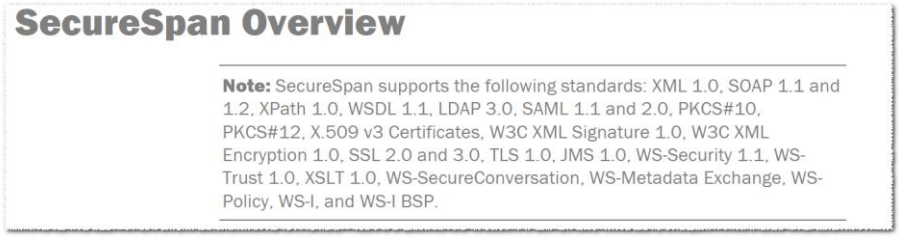
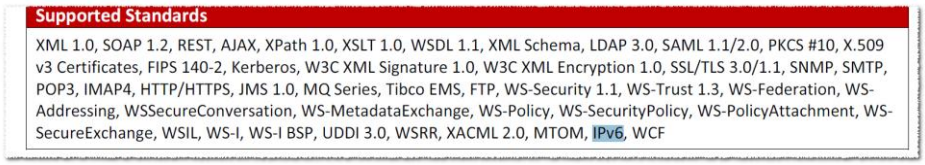
A 3.2	Spain	No requirements specified
A 3.3	Netherlands	No changes in the existing policies for application security are foreseen. The current application security policies do not specify networking protocols.
A 3.4	Turkey	First of all, an inventory of applications that is used or served by eGovernment Gateway, will be prepared for security controls. All applications used by eGovernment Gateway will be examined for IPv6 readiness and necessary upgrades or renewals will be done. Developers or tools for automated assessment of application source code will control all application codes developed by eGovernment Gateway project team, for IPv4/IPv6 calls. As an example, Layer 7 XML Gateway is used by eGovernment Gateway. Current version is not supporting IPv6.  Figure 5-1: Current SecureSpan Version But the latest version of Gateway software (6.1.5) already supports IPv6.  Figure 5-2: SecureSpan version 6.1.5 During the IPv6 transition the XML gateway application will be renewed or upgraded to support IPv6.

Table 5-13: Application Security

5.8.1 Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec)[22] is the protocol suite to secure IP packets by implementing cryptographic algorithms. IPsec uses IP headers, namely Authentication Header (AH)[23] and Encapsulating Security Payload (ESP)[24] to provide authentication, confidentiality and integrity for IP packets. IPsec may be used in host-host, network-network or host-network scenarios. IPv6 implementation mandates inclusion of IPsec, so it has often stated that IPv6 is more secure than IPv4. This is not a true statement since the same problems like key management or implementation bugs are valid for both of the protocols. In addition, usage of IPsec provides security in the IP layer; however this does not provide security against upper layer attacks such as SQL injection.

[22] http://www.ietf.org/rfc/rfc2401.txt

[23] http://www.ietf.org/rfc/rfc2402.txt

[24] http://www.ietf.org/rfc/rfc2406.txt

A 3.1	Germany	No requirement specified, because IPsec is not used in relevant scenarios for the pilot.
A 3.2	Spain	To make sure confidentiality in communications, IPsec tunnels must be established between the two connection areas of the entities that are transferring data through Red SARA. In the case of Web Portals to be made IPv6 accessible, the use of IPsec is not required, or is required in the case of MINETUR eITV application.
A 3.3	Netherlands	IPSec is used between the mid-office located in Hilversum and the Back-office located in Alkmaar. This VPN is transported over the public internet and encryption is used to safeguard confidentiality. At this time NAT for IPv4 is used to prevent conflicts between the RFC1918 addressing used by Inter Access and Gemeente Alkmaar. To easy administration and troubleshooting migration to IPSec on IPv6 is part of the pilot.
A 3.4	Turkey	Current IPsec/VPN firewalls do not support IPv6 connectivity. The acquirement of new firewall process has been started.

Table 5-14: Internet Protocol Security (IPsec)

5.8.2 Transport Layer Security/Secure Socket Layer

Transport Layer Security (TLS)[25] and its predecessor Secure Socket Layer (SSL)[26] are security protocols used to provide network security for the segments of network connections above transport layer. Asymmetric encryption schemas are used for key exchange and symmetric ones for encryption of the transmitted data. Since TLS/SSL is not working in the IP layer, no changes are expected in TLS/SSL usage for IPv6. Software should support IPv6 for the proper usage of TLS/SSL in IPv6 networks.

A 3.1	Germany	TLS/SSL is used in several scenarios, for web servers as well as for VPN mechanism. As outlined above no greater influence on the transition activities is expected. Nevertheless all used implementations of TLS/SSL have to be checked on fully operational compatibility.
A 3.2	Spain	In the case of Web Portals to be made IPv6 available through Red SARA, TLS/SSL connections are required to secure the data interchange when the user is accessing a functionality that requires identity verification by means of electronic certificates. In the case of MINETUR eITV application, TLS/SSL connections are required, since all Web services will be accessed using https.
A 3.3	Netherlands	All e-Government services provided by Gemeente Alkmaar except the public web page are secured with TLS. When the services are provided over IPv6, TLS is required too since the data that are exchanged are privacy sensitive.
A 3.4	Turkey	EGG portal is published through HTTPS over IPv4 for the time being. It will also be published using TLS/SSL over IPv6 since the portal serves critical citizenship data.

Table 5-15: Transport Layer Security/Secure Socket Layer

5.8.3 Legal Considerations

During the design or implementation of any system, legal considerations should be taken into account beside the technical considerations. This is especially important when dealing with the

[25] http://www.ietf.org/rfc/rfc5246.txt

[26] http://www.ietf.org/rfc/rfc6101.txt

government infrastructures.

A 3.1	Germany	As the pilot aims the transition to a dual-stack infrastructure in most cases no variation of the basic use of (legal relevant) data will occur. Anyhow, for technical reasons in the implementation of used tools and application components the data handling may differ, so that legal impacts can take place. Therefore every implementation has to be checked for those kinds of variation, esp. regarding data protection regulations. Relevant issues will be documented.
A 3.2	Spain	The security of the applications must be compliant with the requirements derived from the relevant Spanish legal framework: • Personal data protection security measures, according to Organic Law 15/1999 of 13 December on the Protection of Personal Data and to Royal Decree 1720/2007, of 21 December, which approves the regulation implementing Organic Law 15/1999. • Security measures, according to the three groups of measures (organizational, operational and protective) stated in the Royal Decree 3/2010, of January 8th, which regulates the National Security Framework within the eGovernment scope.
A 3.3	Netherlands	Gemeente Alkmaar has to comply with laws for securing personal information of citizens as drawn up in the “wet bescherming persoonsgegevens” and the “wet gemeentelijke basisadministratie persoonsgegevens”. While networking protocols are not specified in these laws existing policies for IPv4 will have to be translated to IPv6 when IPv6 is deployed.
A 3.4	Turkey	eGovernment Gateway is subject to: • Circular 2010/25, which was issued on 12 December 2010. (IPv6 Transition Plan for Public Institutions). • Law number 5651 (Regulation of Internet Publications, Fighting Crime Committed By These Publications).

Table 5-16: Legal Considerations

6. SUPPORT APPLICATIONS REQUIREMENTS

6.1 Support applications

6.1.1 Virus Scanner

Antivirus or virus scanner software is used to prevent, detect and remove malware, including but not limited to computer viruses, computer worms, Trojan horses, spyware and adware. Virus scanner software can be run on the servers, network devices (i.e. SMTP servers, firewalls) or client machines (i.e. PC, mobile devices).

A 3.1	Germany	Several virus scanners are used to secure a large number of client machines and servers. The management and update of virus-signatures should be possible via IPv6 especially for the clients to reduce IPv4 traffic from the end users site to a minimum.
A 3.2	Spain	As far as Red SARA is concerned, virus-scanning applications are installed in the services clusters of the connection areas and their mission is to analyse and filter the e-mail messages processed by the e-mail relay system. It is required for these virus-scanning applications to be able to analyse and filter IPv6 e-mail messages, providing the same security level in IPv6 as in IPv4.
A 3.3	Netherlands	Gemeente Alkmaar uses on-access virus scanners which have no interaction with the network besides management and updates. An updated version of the virusscanner used does support IPv6.
A 3.4	Turkey	Several virus scanner applications are deployed in server and client machines. There is no specific requirement regarding to these applications since they are not directly related to the network protocol on which they are running.

Table 6-1: Virus Scanner

6.1.2 E-mail

Electronic mail, commonly known as email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. E-mail uses the Simple Mail Transfer Protocol (SMTP), which is initially defined in RFC821[27].

A 3.1	Germany	For Citkomm and its customers SMTP communication as a very basic one must be enabled for IPv6. IMAP-traffic must also be possible via IPv6 in the local networks. Furthermore E-mail communication is used embedded in groupware communication. Different applications can be found in the pilots coverage, namely: • Microsoft Exchange/Outlook • OpenExchange • eGroupware These groupware solutions should support IPv6 as part of the pilot.
A 3.2	Spain	In order to act as a platform for providing Web Portals of Public Administrations with IPv6 connectivity to Internet, an IPv6 compatible e-mail relay system is required to be deployed in Red SARA. The job of this e-mail relay system is to route the IPv6 e-mail traffic generated by the users of the Web Portals to the appropriate e-mail servers that will effectively handle the

[27] http://www.ietf.org/rfc/rfc821.txt

		requests.
A 3.3	Netherlands	Gemeente Alkmaar uses Microsoft Exchange for internal email. External access to email is provided by the Outlook Web access and Outlook Mobile Access component of Exchange which are published via reverse proxies. External email communication is provided by SMTP relay servers running Postfix.
A 3.4	Turkey	There is no specific requirement for Turkish Pilot regarding to the e-mail system as the system does not use smtp in any of its components.

Table 6-2: E-mail

6.1.3 Network Time Protocol (NTP)

The Network Time Protocol (NTP)[28] denotes a protocol and implementation by which hosts that are connected to a packet-based communication network can obtain quite accurately the current time of day. NTP is used to exchange the current time, usually UTC time, between a host and an NTP Server system. It automatically adjusts accommodation for the network transmission delay in order to get a highly accurate local time stamp.

An accurate local time is essential for the correct operation of many IT systems such as file servers, domain controllers, crypto boxes or BGP routing daemons. It is also highly recommended for other IT Systems such as monitoring systems, log systems (syslog servers, etc.) and even normal client systems.

A 3.1	Germany	Citkomm operates NTP-servers for their LAN, backbone and DMZ networks. On the WAN-Gateways NTP-service is offered to the customer-networks.
A 3.2	Spain	Red SARA provides a NTP service that allows synchronizing all the devices connected to it, and that serves as a reliable time source for the different linked entities, since it uses as a reference the legal hour in Spain. IPv6 NTP communication is not expected within the scope of the pilot, so there are no specific requirements regarding this topic.
A 3.3	Netherlands	The NTP services provided by Gemeente Alkmaar are integrated in the layer 3 network core- and access switches except for the stratum-1 servers. When IPv6 is enabled on the network equipment NTP will automatically also be available over IPv6. The stratum-1 servers will be IPv6 enabled.
A 3.4	Turkey	TURKSAT will deploy new NTP servers for transition to IPv6. After the security, performance and stability tests dual-stack configuration will be deployed.

Table 6-3: Use of Network Time Protocol (NTP) service in the pilots

6.2 Middleware Requirements

This section refers to the systems and devices that allow the applications to work properly without knowing the architecture of the lower layers. The middleware shall provide the interoperability and functionality of the systems and improve the phases of the development due to the independence of lower layers.

[28] http://www.ietf.org/rfc/rfc5905.txt

Middleware is the software that provides the way to recognize two remote applications from each other that allow transferring information and data between them. Adapting the middleware to IPv6 includes aspects such as configuration of IPv6 capabilities and network access mode with the aim to use the new features of IPv6 for each element that composes the middleware software.

6.2.1 Operating Systems

This section refers to a set of services that interacts with the hardware resources of the system, offering a base platform, services and functions that allow running applications on that hardware. Most existing operating systems offer IPv6 in its services list.

A 3.1	Germany	IPv6 has to be supported on all servers, especially the iWAN-gateways. They are running currently: • Ubuntu Hardy Heron LTS Server • The upcoming new generation will be based on the next Ubuntu LTS release Precise Pangolin. The Firewalls running: • Secure Platform R62 NGX Application servers are running: • Ubuntu Lucid Lynx LTS Server • Debian Linux squeeze • Centos 5 (Up to date Version) • Centos 6 (Up to date Version) • SLES 10 • SLES 11 • Windows Server 2003 • Windows Server 2003R2 • Windows Server 2008 • Windows Server 2008 R2 A couple of servers offer virtualisation services. They run: • VMware ESXi 4.1 • VMware ESXi 5.0 • VMware ESX 4.1 For the transition of the local area networks IPv6-support is also needed for the client operating systems. These are: • Windows XP • Windows 7
A 3.2	Spain	In the case of Red SARA, IPv6 support is required for all the operating systems that are running in the different hosts located in the connection areas through which IPv6 traffic is intended to go. These operating systems are: • Linux – CentOS 5.2 • Linux – CentOS 5.4 • StoneGate 5.3.3 • Cisco IOS 12.2 • Red Hat Enterprise 5.5 In the case of MINETUR, IPv6 support is required for: • Microsoft Windows Servers 2008 • Load-balancers F5 operating system

		• Palo Alto networks, PAN-OS
A 3.3	Netherlands	All operating systems on servers participating in the pilot will need to support IPv6. Legacy servers running on old operating systems will be IPv6 enabled after updates or replacement The following Operating systems are in use: • Windows XP SP3 on the desktop • Windows Server 2003 • Windows Server 2008 • Windows Server 2008 R2 • Debian Linux squeeze • Oracle Enterprise Linux 5.3 • Oracle Enterprise Linux 5.6 • HP-UX 11
A 3.4	Turkey	For TURKSAT the following operating systems are required to have IPv6 support: • Load-balancers F5 BIG-IP 10.2.1 Build 297.0 Final • Red Hat Enterprise 5.3 Linux running on Intel Quad-Core Xeon processors • Ubuntu 10.0.4 For the other participants of the pilot such as PTT, the operating systems that should be checked.

Table 6-4: Operating Systems

6.2.2 Databases

A database is defined as a collection of data arranged in a system that are accessed individually through networks, in this case over IPv6.

A 3.1	Germany	As complete networks have to be enabled, all databases have to support IPv6. Currently the following database software is used: • MySQL 4 • MySQL 5 • MSSQL 2000 • MSSQL 2005 • MSSQL 2008 • MSSQL 2008 R2 • Oracle 10g • PostgreSQL 8 • PostgreSQL 9 • DB2
A 3.2	Spain	In the Spanish pilot, as far as Red SARA infrastructure is concerned, there is no database software, so these requirements are not applicable. In the case of MINETUR, the backend database will be implemented on IPv4, with the F5 load-balancers translating IPv6 to IPv4.
A 3.3	Netherlands	The following databases are in use at Gemeente Alkmaar. If direct access from the mid-office to the database is needed for the E-government services the will need support IPv6 • Oracle 10g • Oracle 11g • MS-SQL Server 2005 • MS-SQL server 2008
A 3.4	Turkey	PostgreSQL database servers are deployed for EGG portal. All of them are up-to-date and known to have IPv6 support.

Table 6-5: Databases

6.2.3 Application Servers

This section describes the transactional platform requirements and business logic. It refers to the compatibility to adapt the application server to IPv6 networks, defining the set of transactional process will be executed over IPv6.

A 3.1	Germany	Several application servers are used in the Citkomm networks: • Tomcat • JBoss • Glassfish • MS .NET Framework 4.0 • MS .NET Framework 3.0 • MS .NET Framework 2.0 They are used for different applications. To offer those applications the possibility of IPv6 communication, the application servers must support IPv6.
A 3.2	Spain	In the case of Red SARA, the infrastructure dedicated to support the pilot does not include any application servers, so these requirements are not applicable. In the case of MINETUR, IPv6 support is required for the application servers hosting the eITV application, which will be based on Microsoft Framework 4.0 and Internet Information Server 7.
A 3.3	Netherlands	Besides the webservices middleware the main application server is the Alfresco Document Management system. This will have to support IPv6 for communication to the mid-office.
A 3.4	Turkey	Application servers will be deployed through the pilot. For some application servers IPv6 support should be checked (e.g. Glassfish).

Table 6-6: Application Servers

6.2.4 Proxy

A proxy server acts as an intermediary between client and the Internet. It can be used to perform main functions such as connecting local users to corporate network, making indirect network connections to other network services, providing content filtering or caching the most frequently accessed Web content to reduce network traffic.

A proxy server sits between a client application, such as a Web browser and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. Otherwise it forwards the request to the real server.

A 3.1	Germany	To allow virus scanning and caching of network communication, each network is equipped with a proxy. This is squid 3.0 on the WAN-gateways of the customer premises and on the proxy servers for LAN-, backbone- and DMZ-networks as well. Furthermore a reverse proxy is used to provide content to the Internet. This is an nginx cluster. Both software packages have to be able to communicate via IPv6 to the Internet as well as to the internal networks.
A 3.2	Spain	Red SARA provides proxy services to the institutions that are connected to its network. To achieve this, there are proxy servers running in the services cluster located in the connection areas between the institution and Red SARA, which can act both as direct and as reverse proxies. It is required that proxy servers in Red SARA can offer direct and reverse proxy services both to IPv4 and IPv6 connections.
A 3.3	Netherlands	Gemeente Alkmaar uses Blue Coat proxies in explicit mode with authentication for web access from the office network. For the client networks this is the only connection to the internet that is allowed. The rationale behind this is that the proxies provide virus scanning, access control and audit trail generation. This is to protect the client network and to make it possible to track malware activity. The proxies are required to be IPv6 enabled both on the internal side which the clients connect to as the external side with which the proxy retrieves object from the internet. The Blue Coat proxies are also used in reverse mode to publish internal web servers like webmail and intranet on the internet for use by employees.
A 3.4	Turkey	There are no proxies deployed in TURKSAT network. Hence there are no requirements for this topic.

Table 6-7: Proxies

6.3 Network Operations Software Requirements

6.3.1 Domain Name System

The Domain Name System (DNS) is one of the Internet's fundamental building blocks. It is the global, hierarchical and distributed host information database that is responsible for translating names into addresses and vice versa.

A 3.1	Germany	General server or client communication ability with IPv6 enabled requires a working IPv6 aware DNS. Per concept every Citkomm network attached device has to be given a DNS name. Furthermore some applications rely on specific names to get the correct server. For instance every Citkomm customer system can find his proxy with the same DNS name. When those applications are to be enabled for IPv6 communication, these names must be available per IPv6. To accomplish this, the BIND9 configurations must be adjusted.
A 3.2	Spain	DNS service is one of the foundations of Red SARA, key to properly route the traffic through Internet or through the internal links. It allows to present users internally other users' services that are usually accessed through Internet, as well as to present services that are exclusively intended for internal use. To achieve this, Red SARA DNS system is composed by DNS servers located in each of the connection areas between the linked organizations and Red SARA network, and a central DNS server located in the Common Services Centre, which acts as the repository of the addressing tables of the other DNS servers of the system.
A 3.3	Netherlands	No requirements specified
A 3.4	Turkey	All applications running should have their DNS names recorded in the DNS servers. Current DNS servers can answer A and AAAA requests over IPv4. Even though this is enough for the pilot, the DNS servers is planned to be made IPv6 enabled to answer requests over IPv6.

Table 6-8: Domain Name System

6.3.1.1 Current DNS Servers (Dual-Stack)

A 3.1	Germany	Several groups of DNS servers will have to be considered, among thempublic available ones, the specific ones for Citkomm customer network and backbone, those on the customer premise WAN gateways and last but not least the internal Citkomm LAN systems. All of those will have to speak Dual-stack IPv4 and IPv6 fluent in an early state of the pilot project.
A 3.2	Spain	In order to make possible the scenarios envisaged in the Spanish pilot, it is required that the DNS servers involved in the routing of IPv6 traffic through Red SARA can manage both IPv6 and IPv4 addresses. These DNS servers are the ones located in the connection areas between Red SARA and Internet, between Red SARA and MINETUR's network, and between Red SARA and the unit, which will consume the services offered by MINETUR in IPv6. In the case of MINETUR's internal DNS, it will be running on Windows Server 2008 R2 DNS Servers, and will resolve addresses in dual-stack for IPv4 and IPv6.
A 3.3	Netherlands	No requirements specified
A 3.4	Turkey	TURKSAT will deploy new DNS servers for transition to IPv6. After the security, performance and stability tests dual-stack configuration will be deployed.

Table 6-9: DNS Servers (Dual-Stack)

6.3.1.2 Operating Systems

This section describes requirements on operating systems in which the DNS server application is running.

A 3.1	Germany	DNS servers run on Linux systems and as part of Microsoft AD on Windows servers. For a list of flavours of Operating systems see above.
A 3.2	Spain	To achieve the required compatibility with IPv6, the operating systems on top of which DNS servers are running must be able to provide the capabilities to interact with both, IPv6 and IPv4 protocols, as well as an Application Programming Interface that allows applications to make use of those capabilities.
A 3.3	Netherlands	No requirements specified
A 3.4	Turkey	There is no requirement for the DNS server operating system since it is known to have IPv6 support.

Table 6-10: Operating Systems

6.3.1.3 Network Information Centre (NIC) Support

Network Information Centre (NIC) is an organisation that manages the registration of domain names within the top-level domains for which it is responsible, controls the policies of domain name allocation and technically operates its top-level domain.

A 3.1	Germany	Citkomm operates its DNS servers itself. For delegations and NS records DENIC is involved. For new reverse delegations RIPE NCC or the de.government LIR will be involved.
A 3.2	Spain	No specific NIC support, apart from the current support, is initially required in the Spanish pilot, since no specific IPv6 domain names are expected to be used (i.e. public services accessible through Red SARA using IPv6 will be reached by means of the same names used currently for accessing in IPv4). Moreover, the Spanish ccTLD, NIC.ES, responsible of .es, which is the 1st level domain being used for all the DNS services, has been already updated to support IPv6 natively.
A 3.3	Netherlands	Gemeente Alkmaar uses domains in the .nl top level domain. SIDN who manages this domain supports IPv6 with AAAA and necessary PTR and glue records.
A 3.4	Turkey	NIC.TR is the responsible institution for .tr country code top-level domain registrations. IPv6 DNS (AAAA) and IPv6 reverse DNS records are supported and they can be submitted using the graphical web interface provided by NIC.TR.

Table 6-11: Network Information Centre (NIC) Support

6.3.1.4 Registration of IPv6 DNS Servers to Relevant TLDs (for Public Services Only)

A 3.1	Germany	Records for the IPv6 enabled DNS zones will have to be updated in the relevant NIC database.
A 3.2	Spain	In order to act as a platform for providing Web Portals of Public Administrations with IPv6 connectivity to Internet, an IPv6 DNS, managed by Red SARA, is required to be registered to red.es (host of NIC.ES), the entity that manages the Spanish ccTLD .es domain to which the Public Administration Web Portals are associated.
A 3.3	Netherlands	The DNS servers of gemeente Alkmaar need to be IPv6 enabled and their IPv6 addresses will need to be registered with SIDN
A 3.4	Turkey	When the deployment of dual-stack DNS server is completed, it will be registered to NIC.TR.

Table 6-12: Registration of IPv6 DNS Servers to Relevant TLDs (for Public Services Only)

6.3.1.5 Reverse Delegation

The Domain Name System (DNS) provides name-to-number (forward) and number-to-name (reverse) translations, using defined client-server and server-server protocols. Reverse DNS delegations allow applications to map to a domain name from an IP address. Reverse delegation is achieved by the use of the special domain names in-addr.arpa (IPv4) and ip6.arpa (IPv6).

A 3.1	Germany	Database entries for IPv6 reverse delegations will have to be made.
A 3.2	Spain	Red SARA DNS system does not use currently reverse delegation. However, it is intended to implement it during the pilot, in order to reinforce the security of the solution.
A 3.3	Netherlands	Database entries for IPv6 reverse delegations will be requested with RIPE NCC.
A 3.4	Turkey	PTR records will be configured on the IPv6 DNS and rDNS registration to RIPE NCC will be made.

Table 6-13: Reverse Delegation

6.3.2 Enterprise Network Server Applications

A 3.1	Germany	No requirements specified
A 3.2	Spain	The requirements for these applications are restricted to the capability of dealing properly with information regarding IPv6 attributes, since using IPv6 as transport protocol for network management is not expected, at the time being, within the scope of the pilot.
A 3.3	Netherlands	No requirements specified
A 3.4	Turkey	No requirements specified

Table 6-14: Enterprise Network Server Applications

6.3.3 High Availability Software for Nodes

High availability is a system design approach to ensure a high uptime by ensuring redundant path, hardware and protocol availability.

A 3.1	Germany	Citkomm uses high availability functions for a number of solutions and systems. These HA systems always use separate communication paths for the interchange of state information between involved nodes. Therefore this is a kind of backend communication and in most cases IPv6 transition for HA functions needs no priority for the pilot. High availability in the flavour of load-balancing was considered in the sections related to Load-Balancing and Proxy.
A 3.2	Spain	In the case of Red SARA infrastructure, connection areas are designed to operate in high availability mode. This is achieved by means of redundancy in the case of routers and switches, and by means of cluster configurations in the case of servers. Within the scope of the pilot, cluster management it is not expected to be performed by means of IPv6, so there are initially no specific requirements about high availability software. In the case of MINETUR infrastructure, high availability is offered through an IIS7 server farm and F5 load-balancers.
A 3.3	Netherlands	No requirements specified
A 3.4	Turkey	High availability is achieved using load balancers located through the critical points of the network. Details are shared in the load balancers section.

Table 6-15: High Availability Software for Nodes

7. MANAGEMENT REQUIREMENTS

7.1 Network Management Procedures

Network management procedures define how to sustain administration and maintenance of network systems. The ISO Telecommunications Management Network model defines the appropriate management tasks under the five categories Fault, Configuration, Accounting, Performance and Security (FCAPS). For a professionally managed network, the procedures and tasks from these five categories should be well defined. Enabling IPv6 in such a network requires not only the update of the existing procedures for its management but also the definition of new procedures where needed. For example, identification of any unplanned network outage is one of the tasks under the Fault category. Procedures defining e.g. basic ping tests to the IPv4 address of the next hop routers should be updated with addition of IPv6 ping tests accordingly in the IPv6 deployment phase. On the other hand, a new security procedure should be defined for Stateless Address Autoconfiguration, since such a mechanism (and a security procedure) does not exist in IPv4-only networks.

A 3.1	Germany	Network management includes the Linux based Firewall and Routing appliances Citkomm uses for the operation of its network. Those appliances as core components must be enabled for IPv6. But besides making these boxes capable of dealing with all the requirements of IPv6 traffic all the procedures for their management have to be adopted: • The automated installation procedure for these systems has to become IPv6 enabled. • The management tool monitoring configuration changes on the systems must be adopted. • The centralised management must be IPv6 enabled (firewall rule maintenance and distribution, proxy configuration, VPN configuration management ...). • Customer management interfaces on the boxes must be IPv6 enabled. Operators must be trained for dealing with an IPv6-enabled network.
A 3.2	Spain	Regarding the Spanish pilot, as it has been mentioned before, the only expected impact of IPv6 transition regarding network management will be the need to deal properly with IPv6 attributes, since the initial approach for the pilot is to keep IPv4 as transport protocol for network management. Therefore, no new network management procedures are required, beyond their adaptation to take into account IPv6 attributes as well as current IPv4 attributes. Another issue to consider is the fact that, due to the high number of available addresses, it will not be possible to scan the network using brute force, so inventory procedures must be reviewed and changed in the case they are based in network scanning.
A 3.3	Netherlands	Network management procedures will need to be updated as current procedures are based on IPv4. The main points of interest are the fault isolation worksheets and availability and performance monitoring tools.
A 3.4	Turkey	MRTG has been used for traffic monitoring through IPv4. For the IPv6 case, the same method will be applied. Applications that will be used for collecting and analysing the traffic should support IPv6.

Table 7-1: Network Management Procedures

7.1.1 Management Network

A separate out of band management network can be used to provide a secure access to management interfaces of different devices. Those interfaces often allow very basic control of the devices, up to powering them off and on.

A 3.1	Germany	For the view of this pilot project the management network will not be affected.
A 3.2	Spain	No requirements specified
A 3.3	Netherlands	IPv6 enabling of the management networks is not included in the scope of the Netherlands pilot.
A 3.4	Turkey	Management network is out of scope for the Turkish Pilot case. Hence there is no specific requirement for this topic.

Table 7-2: Management Network

7.2 Monitoring

7.2.1 Traffic Monitoring

Network traffic monitoring includes analysis of the data flowing through a network for management purposes such as identification of faults, verification of routing configurations, accounting of the customers, analysis of link performances and detection of security incidents. Monitoring can occur at different levels such as checking the IP headers of the packets or sniffing the payloads depending on the purpose of the monitoring, technical requirements and legislations. While the analysis of headers is enough to keep accounting of the customers, payload inspection could be required to identify signatures of certain attack types for security purposes. Regarding the technical requirements, lower layer analysis will be more preferable for high capacity links such as backbone connections while the later will be a more common monitoring type in the edges. And finally, user data privacy and legislations on that could bring limitations on monitoring levels, especially for the payload inspections. During IPv6 deployment, existing monitoring tools should be checked for IPv6 support. For example, NetFlow, which provides information on IP traffic aggregated from the headers, can only give information for IPv6 in version 9. Therefore, network-monitoring tools based on previous version of NetFlow (e.g. v5) should be updated or upgraded. Similarly, a wide spread payload inspection tool Snort can perform analysis on IPv6 traffic with “Snort 2.8.0” and later versions.

A 3.1	Germany	The used monitoring system for the network and the services has to become enabled for dealing with IPv6. Performance data acquirement, processing and presentation must be IPv6 enabled. It has to be made sure the bandwidth recording does not only cover IPv4 but also IPv6 traffic. Monitoring tools like Munin and MRTG/RRD tool have to be checked updated if necessary. Snort has to be updated.
A 3.2	Spain	It is required 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
A 3.3	Netherlands	Gemeente Alkmaar has implemented traffic monitoring in several distinct systems. Some of these systems already make a distinction between IPv4 and IPv6 like the firewall and proxy audit logs. Some systems are protocol agnostic and do not need changes like connection capacity and throughput monitoring and alerting. A few systems will need change to enable the monitoring of IPv6 uptake. These are mainly the log analysis of the public website and mid-office.
A 3.4	Turkey	Same requirements apply as stated in Network Management section.

Table 7-3: Traffic Monitoring

7.2.2 SNMP Support

Simple Network Management Protocol (SNMP) is an application protocol and uses the main Internet Protocol (IP) stack for managing and monitoring IP devices. SNMP supporting devices include routers, switches, modems, servers or other network-attached devices like printers. SNMP provides a common view of the management data by all members (management stations and the managed devices) through the Management Information Base (MIB) objects. Data stored in a MIB can be read, changed or deleted by management station via SNMP queries. IPv6 deployment brings two issues with SNMP. The first one is performing SNMP queries over IPv6 to manage IPv6-only devices. SNMP as a protocol support IPv6 so this issue only requires enabling IPv6 in management stations of a network and addition of IPv6-only devices to the managed devices lists. The second issue is the IPv6 related MIB objects which mainly include the counters for IPv6 traffic such as bytes and packets. IPv6 enabled devices should also have MIB objects for IPv6 traffic and these object should provide consistent data for monitoring purposes. The existence and consistence of the IPv6 related MIB objects in network devices should be verified.

A 3.1	Germany	SNMP daemons of routers and servers have to be checked for providing IPv6 related information. Gathering of that information over IPv6 is not intended primarily. All Switches at Citkomm work on layer-2 only so their management can be done over IPv4 without affecting the pilot's success.
A 3.2	Spain	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.
A 3.3	Netherlands	SNMP is only used in the management network of Gemeente Alkmaar which is outside the scope of this pilot. As such SNMP over IPv6 is not directly required. IPv6 MIB objects are required to be supported by network equipment that has IPv6 configured to enable availability monitoring.
A 3.4	Turkey	SNMP is currently used in TURKSAT to monitor the network and therefore all the nodes in TURKSAT network support SNMP. Within the scope of the Turkish 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.

Table 7-4: SNMP Support for used Hardware

7.2.3 Monitoring Server IPv6 Support

A monitoring server may be used in a network to analyse the network traffic. Results may be used for forensics or behavioural analysis and will help to see any misuse or illegal activity. This device should be capable of identifying IPv6 traffic and tunnel traffic as there may exist nodes using IPv6 in IPv4 (or vice versa) tunnelling methods.

It is expected that monitoring activities will go on being performed using IPv4 in the near future, because of the needs of adapting a considerable number of elements and due to the fact that monitoring is an internally focused activity which does not require to communicate with external networks. Therefore, within the scope of the pilot, it is not required for the monitoring server to communicate with the monitored nodes using IPv6. However, the monitoring server must be able to deal with information elements containing IPv6 attributes.

Besides of monitoring the network traffic itself a monitoring server is usually used to observe the availability, operation, health and performance of servers and other devices, services and finally even whole business processes.

And with this scope the monitoring of IPv6 services will have a major impact on the monitoring system, using the monitoring to even check availability of some services even via IPv6.

A 3.1	Germany	The monitoring system (icinga) has to become IPv6 enabled (configuration of the monitored systems and of tests). The availability of tests for non-basic or non-standard IPv6 services can turn out as an interesting challenge. So it is expected that due to the nature of the used Open Source solution a number of tests will have to be extended, overworked or rewritten.
A 3.2	Spain	It is expected that monitoring activities will go on being performed using IPv4 in the near future, because of the needs of adapting a considerable number of elements and due to the fact that monitoring is an internally focused activity which does not require to communicate with external networks. Therefore, within the scope of the pilot, it is not required for the monitoring server to communicate with the monitored nodes using IPv6. However, the monitoring server must be able to deal with information elements containing IPv6 attributes
A 3.3	Netherlands	The configuration of the existing HP Openview NNM monitoring system used by Gemeente Alkmaar will need to be adapted to include IPv6 functionality.
A 3.4	Turkey	TURKSAT is planning to use the same monitoring devices due to recurring costs.

Table 7-5: Monitoring Server IPv6 Support

7.2.4 DNS Statistics on IPv6

DNS server is one of the main building blocks of a network. DNS statistics should include the statistics about AAAA queries. In addition if the DNS server is IPv6-enabled then statistics should include queries made over IPv6.

A 3.1	Germany	DNS statistics are in the first run a more informational issue for Citkomm. But finally the tools for analysing DNS logs will have to be checked and updated if necessary.
A 3.2	Spain	DNS servers must be able to provide DNS statistics regarding IPv6 use that are at least equivalent to those that are currently provided regarding IPv4 use.
A 3.3	Netherlands	The statistics gathered by the BIND DNS servers used by Gemeente Alkmaar already include information on IPv6. However this information will need to be processed for reporting.
A 3.4	Turkey	Current monitoring service does not support IPv6 DNS statistics. Thus, required module will be rewritten.

Table 7-6: DNS Statistics on IPv6

7.2.5 Logging Support

Logging enables administrators to maintain the network in case of a problem or to detect a misuse in the network. IPv6 enabled services should save logs about the nodes accessing the services.

A 3.1	Germany	Currently used central syslog servers have to be enabled for IPv6 transport. Analysing the log files (regardless of the information contained within was transported over the network or not) is a completely different point. A number of self-written log file analysers will have to be adopted, as far as this is not done in conjunction with the monitoring system. Commercial/3rd party log file analysing components can show up during the work with the pilot.
A 3.2	Spain	It is required that the solution provides the same level of detail for logging when dealing with IPv6 connections as it is currently providing when dealing with IPv4 connections.
A 3.3	Netherlands	Firewall logging and proxy logging already include IPv6 information. These logs are not processed to reports except when an audit is requested. In that case the raw data is provided to the auditing party for processing. Auditing parties will need to adapt their tooling to provide for IPv6 information. The existing syslog server is part of the management network and IPv6 enablement for this server is outside the scope of the pilot.
A 3.4	Turkey	SyslogNG has been configured for logging and timestamp through IPv4. Load-balancer will send IPv6 traffic to syslogNG server through IPv4. New parsers for IPv6 traffic data will be written for monitoring.

Table 7-7: Logging Support

7.2.6 Performance and Conformance Tests

Testing is one of the key phases in network technology deployment cycle. Once the decision on which technology is to be implemented is made, the testing procedures should take place.

Performance testing is used to determine the performance of a certain device (Device under Test - DUT), network or a system (System under Test - SUT). Typically, the performance tests at a L2/L3 level of ISO/OSI model evaluate how DUT/SUT perform under different traffic and load conditions and this is achieved by measuring network parameters such as latency, jitter, throughput and packet loss. Conformance testing is testing to determine if a DUT/SUT meets standards that are specified for certain network technology or protocol. The conformance testing typically consists of traffic generation and traffic analysis.

For IPv6 DUT/SUT possible performance and conformance test procedures are parameter performance testing (latency, jitter, throughput and packet loss), Benchmarking Methodology for Network Interconnect Devices, IPv6 Benchmarking Methodology for Network Interconnect Devices and IPv6 Testing Address Allocation.

A 3.1	Germany	Performance tests will go beyond the performance monitoring from “Monitoring Server IPv6 Support ”. Because during this pilot existing services and systems will become IPv6-enabled, all existing performance test suites need to be adapted with IPv4/6 dual-stack operations. This refers in the first run mostly to already heavily loaded systems but may be extended to the investigation of DoS behaviour on publicly available systems.
A 3.2	Spain	For the Spanish pilot it is not intended to perform conformance tests in order to verify how a device complies with specific protocol standards, but to rely on the results of tests made by other organizations, since the equipment involved in the pilot is widely used and there exists enough information to assess its IPv6 compatibility. However, it is intended to carry out performance tests, once the IPv6 solution is deployed, to verify the behaviour of the equipment in the actual environment in which it is going to operate, under the premise that the performance using IPv6 must be at least as good as it is currently using IPv4.
A 3.3	Netherlands	No performance and conformance tests on network equipment are planned for the

		Netherlands pilot. There will be performance and availability tests in normal operation which will identify misbehaving equipment.
A 3.4	Turkey	Information Security group will plan performance, conformance and security tests after the conclusion of transition configurations.

Table 7-8: Performance and Conformance Tests

7.3 Quality of Service Procedures

A 3.1	Germany	QoS documents will have to be overworked to reflect the IPv6 awareness. The whole chain of performance data acquisition and analysis, monitoring and reporting will have to be checked and adopted.
A 3.2	Spain	It is required that after the successful implementation of the pilot, the involved systems will provide at least the same level of performance and reliability with IPv6 as it is provided currently with IPv4. Hence, the procedures to guarantee the quality of service must be adjusted in order to include indicators regarding IPv6 communications as well as IPv4 communications.
A 3.3	Netherlands	No requirements specified
A 3.4	Turkey	QoS is not in the scope of Turkish Pilot.

Table 7-9: Quality of Service Procedures

7.4 Security Procedures

A 3.1	Germany	The basic security rules will remain in force. It is intended to migrate to a new version of the firewall management tool with the IPv6 enabling. This reason will be used for a review of the whole security policy. Basic security checklists will have to be updated. Especially the control, usually the disabling of unwanted tunnel connectivity will come into focus. Other IPv6 specifics as necessary ICMPv6 traffic and protection against unwanted router announcements will have to be worked out.
A 3.2	Spain	In the Spanish pilot, security policy is not intended to change due to the transition to IPv6, so basically security procedures will stay the same. It is required therefore that all the current deployed security measures are operating both in communications using IPv4 and IPv6 (filters, access lists, firewall rules, etc.). IPv6 access to devices must be then properly secured, preventing any unauthorized access. However, some specific features of IPv6 make necessary to introduce some changes in the way security is implemented: • Some multicast and ICMP communications, usually blocked in IPv4, must be allowed in IPv6 due to the fact that they are essential for its operation. • Since IPv6 tunnelling is supported by default in many operating systems, this capability should be disabled when it is not needed, to prevent the risk of not being detected by the security devices. • In early stages, information about security incidents with IPv6 can be scarce, so the risk of lack of information must be considered. • Manufacturers' support for IPv6 can be initially weak and the frequency of IPv6 functionalities update releases can be initially low, what makes more difficult to be protected against the newest threats.
A 3.3	Netherlands	The standard Request for Change form regarding security policies will need to be changed to add specific fields for IPv6.
A 3.4	Turkey	Current security procedures will be checked if any changes are necessary regarding the IPv6 support for eGovernment Gateway.

Table 7-10: Security Procedures

7.5 Training

Enabling IPv6 in the four pilots will require training of the IT personnel of GEN6 partners. In addition to main transition techniques, the training requirements maybe on IPv6 address configurations, IPv6 support on services (DNS, HTTP), security, network management and etc.

A 3.1	Germany	A training plan will be initiated. It will cover the needs for system administrators and operators as well. The qualification of the operators will accompany the introduction of IPv6 enabled system in production state. Then the in house software developers and the staff responsible for the process Citkomm provides to its customers have to be IPv6 enabled. As soon as customer networks or systems come into focus the technical personnel of the customers has to be included in the training courses.
A 3.2	Spain	In the Spanish pilot, a training plan will be designed in order to assure that the people responsible for the implementation and operation of the pilot has the required skills for these tasks. This training plan will include classroom training and online training, will cover both generic topics regarding IPv6 transition and specific topics derived from the actual implementation in the pilot and will be customized according to the different roles of the audience during the pilot: • Technicians and network managers from Red SARA • MINETUR's technicians and network managers responsible for the connection area with Red SARA • MINETUR's technicians and developers involved in the adaptation of business applications. • Technicians and other people not involved directly in the pilot but with relevant interest in it (e.g. network managers from other Ministries than MINETUR that are planning to offer IPv6 services through SARA).
A 3.3	Netherlands	Training of Gemeente Alkmaar staff will be done in house and on the job. No specific training programs are envisioned. External parties will be responsible for training their own staff.
A 3.4	Turkey	IT staff from TURKSAT and governmental agencies may face some difficulties regarding the new concepts introduced by IPv6. This situation will be resolved by giving IPv6 Transition Training course to the related personnel. This training should be done as soon as possible in order to keep up with the deadlines in the proposed work plan. To increase efficiency, training should be in Turkish since some participants (especially the ones from the governmental agencies) have problems in foreign languages. Since ULAKBIM has "IPv6 Transition Training" programme for governmental agencies with hands-on exercises, a special class for all Turkish pilot participants should be opened in M3.

Table 7-11: Training

7.6 Documentation

This item refers to the potential requirements imposed on the documentation prepared within the scope of the pilot.

7.6.1 Application of Standards

This item refers to the documentation requirements arisen from the compliance of the organization with standards and frameworks in the fields related to the scope of the pilot, such

as quality (e.g. ISO 9001, EFQM), ICT management (ITIL, COBIT, etc.) or information security (ISO/IEC 27001).

A 3.1	Germany	The work during the GEN6 pilot will have to keep several standards like ITIL in mind, but no specific papers in relation to standard documents will be produced.
A 3.2	Spain	No requirements specified
A 3.3	Netherlands	No requirements specified
A 3.4	Turkey	The standards of ISO 27001 all the documentations and standard procedures will be revised.

Table 7-12: Applied Standards

7.6.2 List of Internal Documentation

This item refers to other internal documentation requirements apart from those stated previously as derived from the standards and frameworks adopted by the organization.

A 3.1	Germany	Systems and processes are documented in an in house wiki primarily. This will have to be made IPv6 aware in the sense that it can provide IPv6 addresses and specifics. Further documents like release and approval documents will have to be reworked.

A 3.2	Spain	The required internal documents are organized around three main lines of activity:
		• IPv6 enablement of Public Administrations Web Portals.
		  ○ Solution design
		  ○ Identification of candidate Web Portals and Implementation plan
		  ○ Testing documentation
		  ○ Deployment and operation guide
		• Upgrading of SARA to support IPv6 services provision between Public Administrations.
		  ○ Transition strategy
		  ○ Updating of the current Public Administration Interconnection and Addressing Plan, to include the prefix allocation and address assignment procedures associated to the introduction of IPv6 in Red SARA
		  ○ Compatibility Assessment
		  ○ Transition technologies and Solution design.
		  ○ Implementation plan
		  ○ Training plan
		  ○ Training materials
		  ○ Testing documentation
		  ○ Deployment and operation guide
		• Adaptation of MINETUR services to IPv6
		  ○ Solution design
		  ○ Implementation plan
		  ○ Training plan
		  ○ Training materials
		  ○ Testing documentation
		  ○ Deployment and operation guide

A 3.3	Netherlands	Internal documentation will be amended during the implementation of needed requirements. This is inline with the normal production of internal as-build documentation during implementation of systems.
A 3.4	Turkey	After revising the necessary documentations, TURKSAT will list and update them.

Table 7-13: Available internal Documentation

8. SECURITY

8.1 Firewall

Firewall is a software or hardware that is used to control the traffic transmission based on a set of rules. These rules include filters about IP information such as IP addresses, port numbers and protocol used. A firewall that will be used in an IPv6 network should be able to identify IPv6 packets, IPv4 packets as well as tunnelled traffic (IPv6 in IPv4 and IPv4 in IPv6). Moreover, a firewall should be able to filter ICMPv6 packets by ICMPv6 type and ICMPv6 code fields. Firewall rules should be updated accordingly in the IPv6 deployment phase.

A 3.1	Germany	Various commercial and non-commercial firewall systems will have to be considered. They must allow controlling both IPv6 and IPv4 traffic usually, and their management interfaces or systems must support IPv6 as well. As stated above the firewall rule sets will be reviewed with the enabling of IPv6. The timeline for enabling IPv6 in production systems will have to respect the security and so the firewall needs in a reasonable way.
A 3.2	Spain	The firewalls that are within the scope of the Spanish pilot are those that will secure the IPv6 traffic between Internet and Red SARA and between MINETUR's network and its clients' networks through Red SARA. These firewalls are the following: • The external firewall in the connection area between Red SARA and Internet • The internal firewall in the connection area between Red SARA and Internet • The external firewall in the connection area between Red SARA and MINETUR network • The internal firewall in the connection area between Red SAR and MINETUR network It is required for all of them to offer IPv6 features in parity with the ones being used for IPv4, plus additional specific features for IPv6. In particular, they must be able to: • Filter IPv6 packets, on an IP address and port basis • Close the VPN connections established using IPsec
A 3.3	Netherlands	Gemeente Alkmaar uses two firewall clusters to secure internal systems and exposed DMZ systems. Both these firewall clusters need to fully support IPv6.
A 3.4	Turkey	IOS, JunOS and related software should be upgraded. New acquirements will be made where a software upgrade is not applicable.

Table 8-1: Use of Firewalls

8.2 Intrusion Detection/Prevention Systems

Intrusion Detection/Prevention Systems (IDS/IPS) are used to monitor and analyse the network traffic in order to detect any illegal activity (attacks, misuse, etc.) in the network. This detection may be done using static rules, network signatures or behavioural analysis. In order to detect an activity; an IDS/IPS makes deep packet inspection (DPI) i.e. analyses every packet including packet payload. An IDS/IPS should be able to identify IPv4 and IPv6 traffic. Especially tunnelled traffic (e.g. as in Teredo transition mechanism IPv6 packets are encapsulated into UDP packets) constitutes a real threat if not analysed. IDS/IPS rules and signatures should be updated properly for the IPv6 network.

A 3.1	Germany	IDS will have to be updated.
A 3.2	Spain	It is required for all the IDS/IPSs through which IPv6 traffic will pass within the scope of the pilot (located in the connection areas between Red SARA and Internet and between Red SARA and MINETUR's network) to offer the same security level in IPv6 than in IPv4. The management of these IDS/IPSs is shared between Red SARA and the CCN-CERT since the CCN-CERT is the Spanish competent authority in the field of Response to Information Security Incidents and it is linked to the international CERT network. In particular, they must be able to: • Monitor the traffic in the connection area • Filter events using both generic rules (for all entities connected to SARA) and rules specific to the particular entity provided by the CCN-CERT • Transfer the filtered events to the central management console located in the CCN-CERT
A 3.3	Netherlands	The IDS/IPS functionality is integrated in one of the firewall clusters of Gemeente Alkmaar. As stated for the firewall IPv6 will need to be fully supported.
A 3.4	Turkey	In TURKSAT, IPS/IDSs have been configured as in-line mode. Devices have support for IPv6 in IPv6, IPv4 in IPv6, IPv4 in IPv4, GRE with IPv6, IPv6 with MPLS and IPv6 with VLAN. Necessary signatures will be updated and activated.

Table 8-2: Intrusion Detection/Prevention Systems

8.3 Access Control Lists

Access Control Lists (ACLs) are set of rules that generally works on edge routers and defines which packets (routing updates as well as usual traffic) will be allowed into the network. These rules may be denying all traffic from a specific IP address or allowing routing updates only from specific nodes. ACLs should be updated along IPv6 deployment. This update includes IPv6 support of Layer-3 devices (routers, Layer-3 switches etc.) and changing ACL rules for IPv6 packets, IPv6 routing protocols (OSPFv3, RIPng, etc.).

A 3.1	Germany	ACLs will have to be extended to IPv6 addresses and IPv6 protocol requirements.
A 3.2	Spain	From the point of view of the role that Red SARA is playing within the scope of the pilot (acting as a connectivity platform between entities), access control is managed by the end applications and therefore there are no Red SARA ACLs involved. In the case of MINETUR, ACLs are not used by the eITV application on which the pilot is based.
A 3.3	Netherlands	Besides in the firewalls Gemeente Alkmaar has only implemented access control lists for limiting access to in-band management. These ACL's will have to be changed when IPv6 is enabled on the device.
A 3.4	Turkey	Necessary ACLs at the firewall will be re-written.

Table 8-3: Access Control Lists

8.4 Planning the Security Tests

A 3.1	Germany	For each chapter of the project plan security considerations and tests will have to be noted and performed. This will be integral part of the project work and each team leader will be responsible.
A 3.2	Spain	The use of IPv6 must maintain or improve the level of security compared to IPv4. Due to the specific features of the new protocol, not all testing procedures and tools used in IPv4 are suitable for IPv6. In that sense, the execution of IPv6 specific security tests during the pilot will be planned, covering equivalent topics as those covered in current IPv4 security tests.
A 3.3	Netherlands	Security auditing of Gemeente Alkmaar is done by external parties. These parties will be required to provide specific testing plans for IPv6
A 3.4	Turkey	Information Security group will plan performance, conformance and security test after the conclusion of transition configurations.

Table 8-4: Planning the Security Tests

9. CONCLUSIONS

Requirement analysis is one of the major steps in realising the national pilots in the GEN6 project. This deliverable includes the results of the requirements analysis on the four pilots to be realized in Netherland, Germany, Spain and Turkey.

The participants of the pilots identified for the requirement analysis seven main categories, which are network architecture requirements, network level requirements, network hardware requirements, business applications requirements, support applications requirements, management requirements and security. Within those categories, 73 items have been identified for clearly indicating the needed steps in realizing the pilots.

Spain indicated requirements for 70 items, while the number of requirement items specified by Turkey is 72 and by Germany it is 72. Netherlands 66. Besides these numbers there are common technical requirements among these pilots that can be classified as follows.

All four pilots require IPv6 connectivity as they will be giving their services over public Internet connection. It is observed that network ingress and egress points between governmental institutions should be made IPv6 enabled in all of the pilots. Considering geographical properties (i.e. number and location of sites) of the pilots, there exist various participating institutions mainly centred at one city. For instance; Spanish pilot seems to be established in Madrid whereas Netherlands pilot in Alkmaar and Turkish pilot in Ankara. External connectivity requirements of all four pilots are also similar as they all will serve to citizens. All pilots require an IPv6 uplink from their telecom operators/ISPs which are expected to satisfy SLA conditions which already exist for IPv4 network. In other words IPv6 connectivity for uplinks is expected to be at a production grade.

It is found that in general, institutions manage their own facilities such as housing, power supply etc. Both shared and dedicated infrastructures exist in all pilots. Moreover, the connections between institutions are usually dedicated, whereas shared infrastructures are used at some points in all 4 four pilots. As the availability of governmental services is crucial all four pilots for instance, Spain, Netherlands and Turkey pilots use multi-homing by deploying multiple links to the same ISP.

The pilots' machine parks are not single vendor oriented; both vendor and open source solutions exist. For instance, it is observed that several OSs (Ubuntu Server, Windows Server 2008, CiscoIOS etc.) will run over different platforms in each pilot. Almost all of these OSs are IPv6-enabled which is an advantage for the pilots. Similarly, various database servers (MySQL, MSSQL, PostgreSQL etc.) and application servers (JBoss, MS .NET Framework etc.) are deployed within pilots. An advantage for all pilots is that current releases of this software have IPv6 support.

Pilots are planning to use dual-stack as a transition mechanisms, involvement of tunnels is not desired. Regarding the dual-stack connectivity requirements; current pilot infrastructures are based on IPv4. Dual stack implementation with full native IPv6 connection is the main aim of all pilots. All of the pilots stated addressing plan requirements and plans should be compliant with the current local policies. Regarding to this requirement, it is vital for GEN6 project to create best practise for addressing plans for institutions. Pilots allocate different block sizes. For example, it is seen that Germany has IPv6 block size of /48 whereas Turkey and Netherlands have /32 for the pilot host institutions. For address configuration of hosts and routers, hybrid solutions will be deployed for address configuration. General consensus for Firewalls and various servers is to assign IPv6 addresses statically. On the other hand, end user devices are planned to deploy SLAAC or DHCPv6 to configure their IPv6 interfaces. Requirements regarding network equipments are also included in the document. All pilots have agreed that IPv6 support for Layer 3 devices is necessary. In addition to this, Netherlands and Turkey pilots have stated that there is a local principle which mandates purchase of IPv6-enabled devices. There are no specific requirements stated for IPv6 support of Layer 2 devices either for specific functionalities or for management purposes. Spain pilot has just stated that for Layer 2 devices security functionalities (Rogue-RA mitigation etc.) should be considered as a requirement.

It is seen that Germany, Netherlands and Turkish pilot deploy BGP for external routing. Related configuration should be made for these routing entries in order to announce the address blocks to global IPv6 network. For internal routing, Germany and Netherlands pilots deploy OSPF and there are requirements to deploy dynamic routing protocols where OSPF is used. Spain pilot has stated that the routing configuration decision will be made by the telecommunications operator. Turkey pilot has stated that static routing is being deployed for internal network currently and static routing will be deployed for the internal IPv6 network. Thus, for all pilots IPv6 support of routing protocols is given as a requirement.

As governmental institutions serve a large number of citizens (for the Turkish case, more than 13 million) Load-balancers are deployed at some points of the network should be made IPv6-enabled for Spain, Netherlands and Turkey pilots.

All pilots deploy VPNs in their network and IPv6 support of various VPN solutions are stated as a requirement for all pilots. As an interesting example; Netherlands pilot has stated that heavy use of NAT complicates management and troubleshooting. IPv6 may be seen as a solution to these issues as every node will have a global IPv6 address. Also network equipment and OSs located in the entry/exit points of VPNs should be IPv6-enabled.

The pilots deploy various kinds of applications to give the related services to citizens. As a brief explanation, Spanish pilot is working on vehicle registration system whereas Netherlands pilot on e-identification and Turkish pilot on e-government Gateway.

All pilots require both internal and external access to the applications. External access will be achieved through web interfaces of the applications using HTTPS. They require both IPv4 and IPv6 support for the deployed applications in order to give the services over a dual-stack network. As a part of applications, dual stack support of DNS servers and usage of DNS addresses rather than literal addressing has been stated. Applications deployed in pilots mostly depend on web applications since they give their services to citizens using web applications. Hence, each pilot requires the deployed components such as web server, virtual hosts and application servers to support IPv6. Fortunately, current releases of most of these components are known to have IPv6 support (e.g. Apache Web server, IIS Web server). It is also observed that there are still some applications that do not have IPv6 support such as Glassfish.

It is observed that each participating country has legal considerations regarding to the personal data protection. As Netherlands pilot has stated, these legal considerations do not include networking protocols such as IPv4 or IPv6. These regulations should be valid for both IPv4 and IPv6. In addition, Turkey has a circular defining IPv6 transition plan of public institutions.

Requirements regarding support applications (virus scanners, e-mail, NTP) are enlisted in the document. These requirements do not seem to be vital for the pilots. Some improvements about these support applications are updating virus scanners over IPv6 or making e-mail and NTP servers IPv6-enabled. DNS requirements are common for all pilots. DNS servers used in the pilots should be registered to the related NIC. For all pilots, ccTLD's have already IPv6 support. Additionally, forward and reverse DNS records should be defined for the top-level domain names used in the pilots.

Management requirements are similar for all pilots. This includes update of current network management and security procedures as well as traffic monitoring and logging applications. Training is another title that all pilots have stated their necessity about. Lastly, it is apparent that all pilots require an update for documentation such as testing, deployment or operation guides.

Lastly security requirements are similar and as expected they are highly critical for the pilots. Firewall rules, IDS/IPS rules and ACLs should be extended to be applied on IPv6 traffic.

The results of the requirements analysis in this deliverable are represented in the form of a checklist for all participants working in the pilots. A detailed list of the requirements with a brief description of each item in the list is also summarized in the work plan with defined actions for each pilot. Consequently, this document will be used as a guideline in GEN6 for national transition activities towards enabling IPv6.