GOVERNMENTS ENABLED WITH IPv6

GEN6

REQUIREMENT ANALYSIS

FOR eGOVERNMENT SERVICES WITH IPv6

This project has received
funding from the
European Union´s

European
Commission

INTRODUCTION

GEN6 project includes four different types of national case studies (also called national pilots) to provide general guidelines for planning and realizing the steps in enabling IPv6. This booklet bases on the requirement analysis results of these pilots. They have been launched in three different countries and have been realizing IPv6 upgrade of eGovernment Network Infrastructures, e-Identification, Services and Applications. This booklet aims highlighting the common and different aspects of enabling IPv6 while taking into account the different approaches to IPv6 in these pilots. Also this booklet may be used as a guideline for an institution which is willing to give IPv6 support to its services.

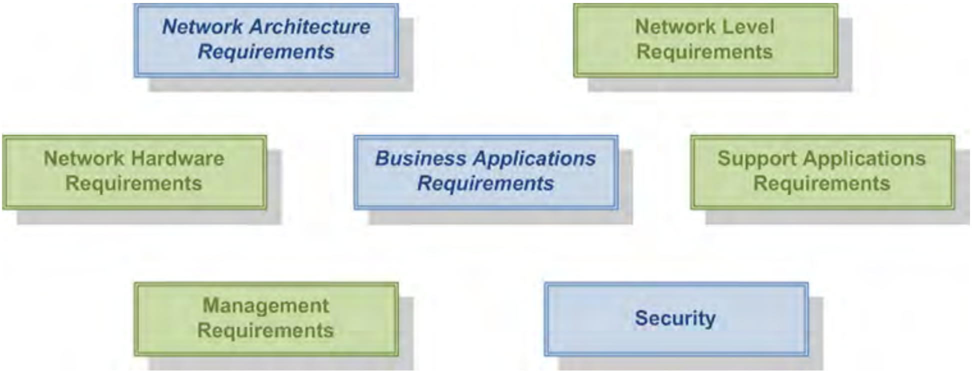
Within this document requirement analysis study may be defined as the identification of the needs for enabling IPv6 in each pilot with clear definitions and plans for future actions.

- Initial step for identifying the needs of these pilots.
- A checklist to complete the required steps for enabling IPv6.
- The work plan of each pilot which points the main milestones of the IPv6 transition.

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. As a result of this approach requirements are collected under the following 7 main categories which aggregate 73 topics in total.

- Network Architecture Requirements
- Network Level Requirements
- Network Hardware Requirements
- Business Applications Requirements
- Support Applications Requirements
- Management Requirements and Security

HOW DID WE CATEGORIZE THE REQUIREMENTS?



Network Architecture Requirements

Network Level Requirements

Network Hardware Requirements

Business Applications Requirements

Support Applications Requirements

Management Requirements

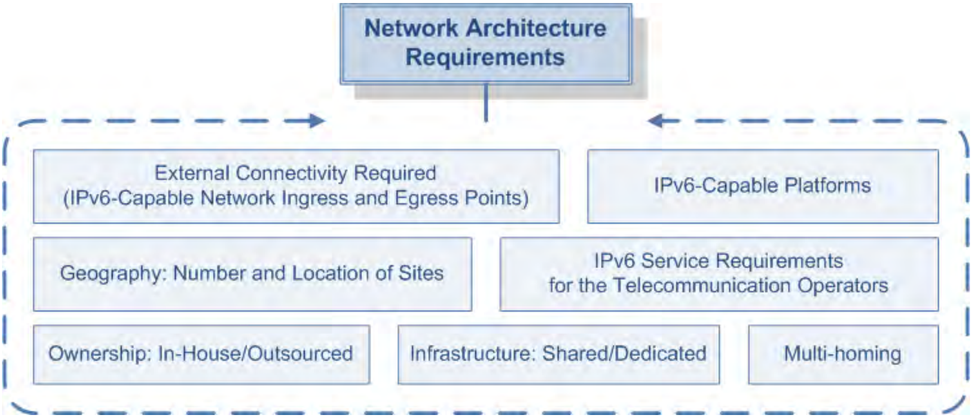
Security

The most recognizable effect of IPv6 transition is observed at the network layer. For this reason, the requirement analysis on the network layer has a notable importance. Hence three out of seven categories are directly related to network analysis of the respective institutions. These main categories include a wide scope from geographical location of participating institutions to addressing plans and network hardware.

IPv6 transition will inevitably require current applications to be investigated. These applications are observed under two main categories namely business applications and support applications. After listing the relevant applications that will be affected by the transition, these applications should be analysed deeply, especially trying to answer if the application has IPv6 support. You may find the use cases observed for web servers, user front-end applications, application security (IPsec, TLS/SSL), middleware requirements and DNS registration based issues under the respective categories.

Implementing a new protocol will require management and security procedures to be reviewed as well. Related topics are analysed through the last two main categories namely management and security requirements which include network monitoring, training, documentation, updating security policies (firewall, ACL rules etc.) and implementing security tests.

WHAT SHOULD YOU CONSIDER ABOUT NETWORK ARCHITECTURE?



Network Architecture Requirements

External Connectivity Required (IPv6-Capable Network Ingress and Egress Points)

IPv6-Capable Platforms

Geography: Number and Location of Sites

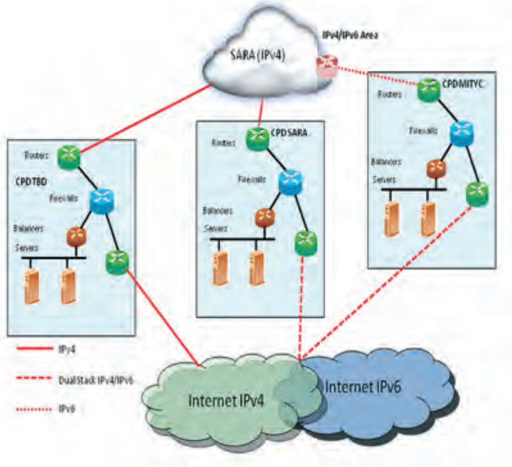
IPv6 Service Requirements for the Telecommunication Operators

Ownership: In-House/Outsourced

Infrastructure: Shared/Dedicated

Multi-homing

Network architecture requirements mainly depend on the participating institutions. Hence you should define and analyse them explicitly. Drawing network topologies between the institutions helps you to dig up the requirements easily. Resulting figure should include the information on how they are connected to each other as seen in the overview of the Spanish Pilot figure below.



RECOMMENDATIONS REGARDING THE NETWORK ARCHITECTURE

Find out the requirements regarding to the connectivity between the network of the participants in the pilot, the Internet and the network of other organizations.

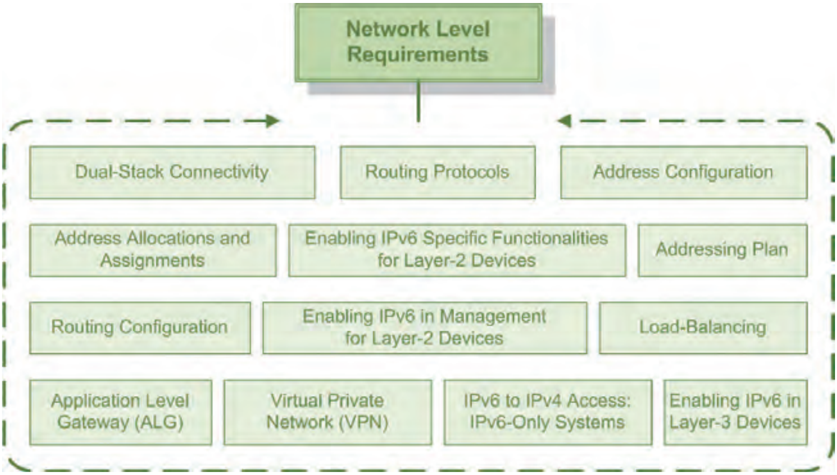
- The connection to the Internet
- The connection between the institutions
- The connection to the end users

One of the important items that need to be considered under this title is **geography and number of locations for the IPv6 transition.** As expected the location of the sites that will be connected through the participant organization network during the pilots plays a critical role.

Recommendations:

- Identify the sites that the transition will affect.
- Specify a contact person for each of these sites in case of an intervention.
- Plan a training of the stuff in different locations may be taken as another consideration.
- Identify ownership of the sources (network equipment, links, software and human resources etc.) and status of the infrastructure (shared or dedicated).
- Check respective telecommunication operators whether they are ready for IPv6 transition.

WHAT SHOULD BE DONE IN THE NETWORK LEVEL?



Network Level Requirements

Dual-Stack Connectivity

Routing Protocols

Address Configuration

Address Allocations and Assignments

Enabling IPv6 Specific Functionalities for Layer-2 Devices

Addressing Plan

Routing Configuration

Enabling IPv6 in Management for Layer-2 Devices

Load-Balancing

Application Level Gateway (ALG)

Virtual Private Network (VPN)

IPv6 to IPv4 Access: IPv6-Only Systems

Enabling IPv6 in Layer-3 Devices

- Enlist the restrictions and scope of the IPv6 support.
- Setup and maintain a well-organized addressing plan independently from the address family used in a network.

Dual stack where you can; tunnel where you must!
Dual stack refers to the transition method where devices are able to run IPv4 and IPv6 in parallel. Thus, it allows hosts to reach IPv4 and IPv6 content simultaneously, offering a very flexible coexistence strategy.

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 AND CONFIGURATION

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.

> ***IPv6 Address Configuration***
>
> *The IPv6 address configuration 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. Here it is worth noting that an interface may use multiple IPv6 addresses at the same time.*

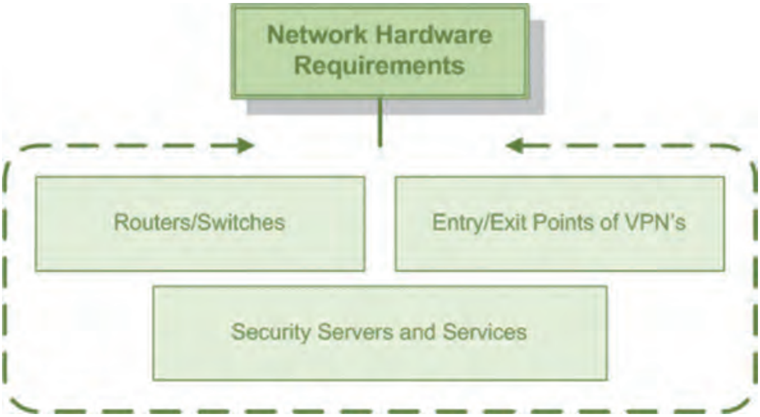
Check layer 3 devices for IPv6 support?

Layer-3 devices may be said to have the most critical role for the IPv6 transition. Especially if the institution selected to use dual stack; starting from the backbone router, all Layer-3 devices should be made IPv6 enabled. Good news about this issue is that most of the modern devices and operating systems have native IPv6 support. Problem arises when a legacy Layer-3 device is in use through the network.

What about Layer-2 Devices?

Transport of IPv6 over Layer-2 devices does not need significant changes.
Though one should check the **MLDv2 snooping, DHCPv6 Snooping, duplicate address detection, rogue-RA mitigation** support for a Layer-2 device.

RECOMMENDATIONS REGARDING THE NETWORK HARDWARE

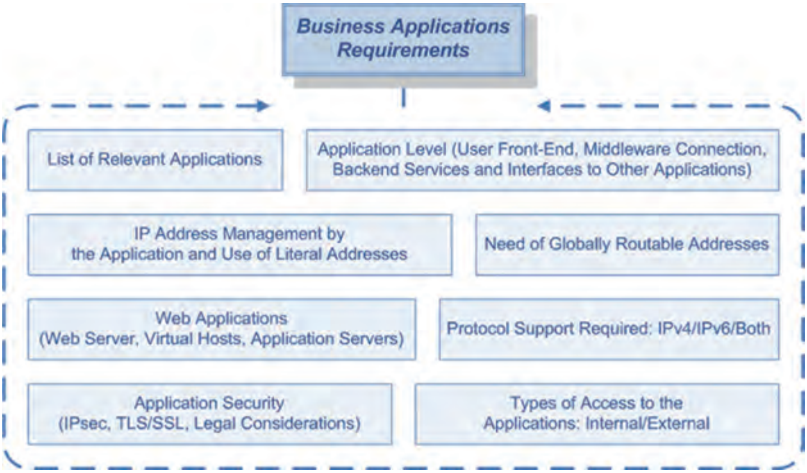

Network Hardware Requirements
Routers/Switches
Entry/Exit Points of VPN's
Security Servers and Services

Routers are one of the mandatory items to be checked for the IPv6 transition as outlined under "Network Level Requirements" section. All used equipment has to be checked for IPv6 compatibility and interoperability with the other routing components used in the institution network, including the provider operated uplink routers if exists.

Requirements for the deployed **switches** may vary depending on the infrastructure. For instance; in one partner-network switches are 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. Otherwise, Layer-3 switches should be checked for the IPv6 support and should be configured and included in the address planning study.

Entry/exit points of VPNs may include VPN gateways and IPv6 support of these network devices should be checked. In addition security service hardware providing actions such as, intrusion detection/prevention, packet filtering or deep packet inspection in a network should be checked for IPv6 compatibility.

WHAT SHOULD YOU CONSIDER REGARDING THE BUSINESS APPLICATIONS?


Business Applications Requirements
List of Relevant Applications
Application Level (User Front-End, Middleware Connection, Backend Services and Interfaces to Other Applications)
IP Address Management by the Application and Use of Literal Addresses
Need of Globally Routable Addresses
Web Applications (Web Server, Virtual Hosts, Application Servers)
Protocol Support Required: IPv4/IPv6/Both
Application Security (IPsec, TLS/SSL, Legal Considerations)
Types of Access to the Applications: Internal/External

- Obtain a comprehensive list of all applications and services running inside an IT infrastructure.
    - The state of documentation of the network.
    - Complexity and variety of the IT infrastructure elements and offered services, the clarity of responsibilities.

- It is hard to deal with legacy technologies or some functions or components of older technology in the depths of the applications.
- Make a list about IPv6 readiness of the deployed applications.

Investigate the following items for the relevant applications:

- *Types of access to the applications: Internal/External*
- *Protocol support required: IPv4/IPv6/Both*
- *Need of globally routable addresses*
- *IP address management by the application and use of literal addresses*

RECOMMENDATIONS REGARDING THE BUSINESS APPLICATIONS

Web applications is expected to be one of the categories that the generated relevant application list would include since most of the governmental services is running web or application servers in order to keep their services up and running.

- Web servers, virtual hosts and application servers should be checked for IPv6 support.
- All application level requirements should be considered at the planning phase of IPv6 transition. For instance the user front-end, as a sub item of the application level requirements, 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.
- Additionally, middleware and backend connection should be investigated if a change is required regarding the IPv6 support.
- Middleware and backend connection can often be viewed independently from the front-end ones.

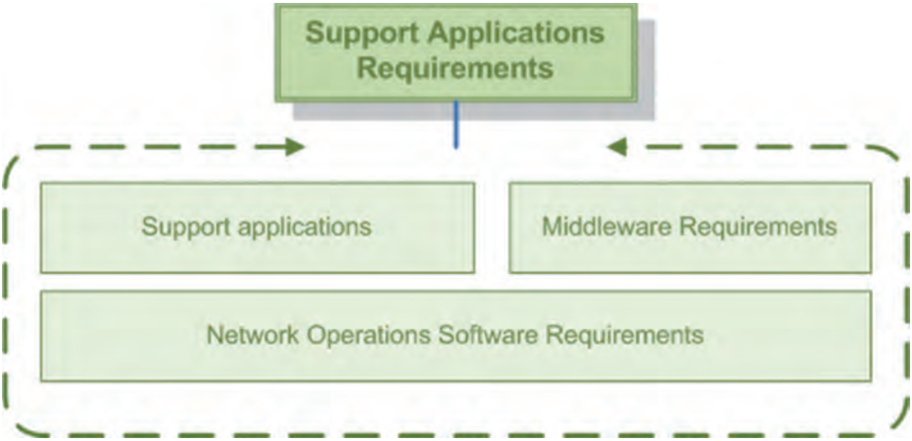
Consider Application Security!

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.

Moreover, if the services are deploying secure communication channels, such as IPsec, TLS/SSL etc., the requirements regarding these protocols should be investigated.

As a last note, throughout the design or implementation of a system, ***legal considerations*** *should be taken into account besides the technical issues. This is especially important when dealing with the governmental infrastructures.*

RECOMMENDATIONS REGARDING THE SUPPORT APPLICATIONS

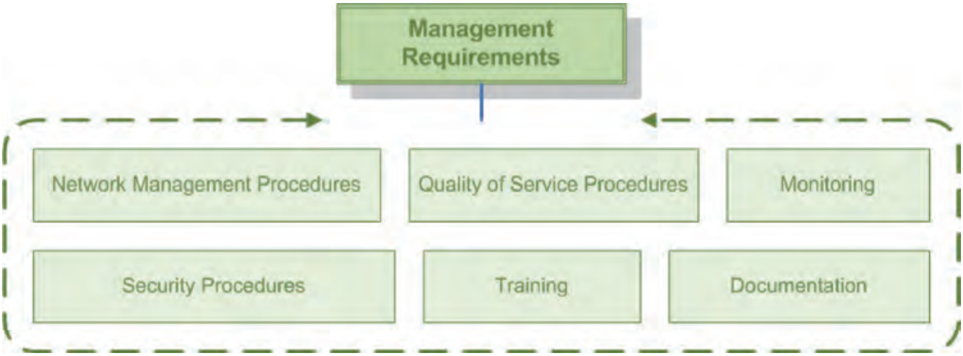

Support Applications Requirements
Support applications
Middleware Requirements
Network Operations Software Requirements

Support applications such as **antivirus software, e-mail and network time protocol (NTP) servers** should also be considered through the IPv6 transition. 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. Additionally, **e-mail and NTP servers** should be checked for IPv6 compatibility and should be made IPv6 enabled if applicable.

Next step should be making a list of deployed **operating systems, databases, application servers and proxies.** The main advantage in this step is that most of the modern middleware systems do have IPv6 support. This list will make it easy to see which application updates are required or which components in the system should be changed. It is observed for the GEN6 pilots that these applications do not vary much.

DNS servers have a critical role in the IPv6 transition. Here one should consider two different cases. Firstly **respective domain names** should have AAAA record to be accessed over IPv6. For this purpose, Network Information Centre (NIC) records (forward and reverse) should be updated. These records may be queried over IPv4. Secondly, **DNS servers** should be checked for IPv6 support. If the DNS servers are IPv6 enabled, they may be queried over IPv6 as well.

RECOMMENDATIONS REGARDING THE MANAGEMENT APPLICATIONS



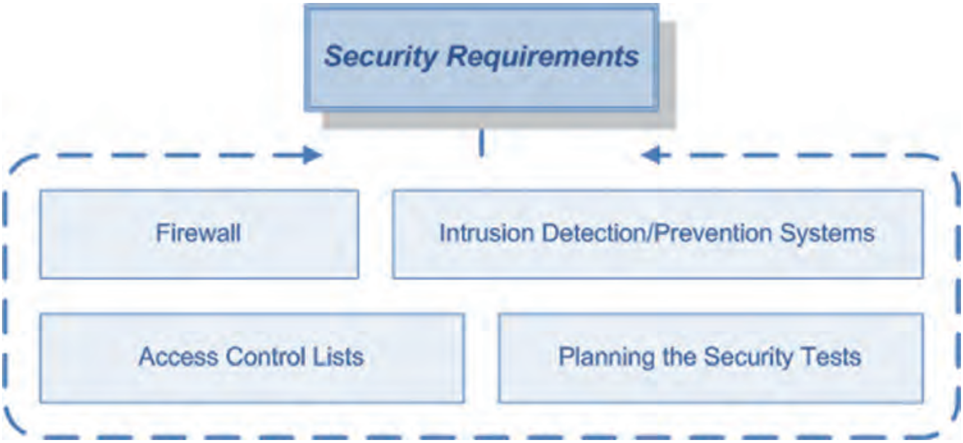
Network management procedures define how to sustain administration and maintenance of network systems. The ISO Telecommunications Management Network model defines the appropriate management tasks under the five categories Fault, Configuration, Accounting, Performance and Security (FCAPS). For a professionally 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.

KEY RECOMMENDATIONS REGARDING THE NETWORK MANAGEMENT

- 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.
- 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 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.

WHAT ABOUT NETWORK SECURITY?


Security Requirements
Firewall
Intrusion Detection/Prevention Systems
Access Control Lists
Planning the Security Tests

Security appliances and software are used to control the traffic transmission based on a set of rules in general. These rules include filters about IP information such as IP addresses, port numbers and protocol used.

- Firewalls 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).
- A firewall should be able to filter ICMPv6 packets by ICMPv6 type and ICMPv6 code fields. Hence security appliances should be updated accordingly.

FINAL REMARKS

Requirement analysis is one of the major steps for the IPv6 transition. This booklet presents the critical points of the requirement analysis of three national pilots being realized in Germany, Spain and Turkey.

Considering the variety of topics needed to be addressed in the requirement analysis of IPv6 transition, it is difficult to identify and categorize the titles. To ease this process for the future transitions, GEN6 project participants have specified 7 main categories which aggregate 73 topics in total. This categorization can be used as a reference for the IPv6 transition of a governmental institution.

DISCLAIMER

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

The information herein does not necessarily express the opinion of the EC. The EC and the document authors are not responsible for any use that might be made of data appearing herein and effects that result from doing so. The GEN6 partners do not warrant that the information contained herein is capable of use, or that use of the information is free from risk, and so do not accept liability for any direct nor indirect loss or damage suffered by any person using this information.

This booklet is prepared by TÜBİTAK ULAKBİM

This work was in part supported by the European Commission as part of the project “Governments Enabled with IPv6” (GEN6). GEN6 is about stimulating EU-wide deployment of IPv6 by means of best practices and guidelines in existing eGovernment infrastructures.

Authors

Emre Yüce (TÜBİTAK ULAKBİM)
Onur Bektaş (TÜBİTAK ULAKBİM)

This booklet is based on the deliverables in work package 3 of the GEN6 project. All participants in this working package have contributed to this booklet indirectly. They are not explicitly mentioned here. Details on the requirement analysis made and the involved partners and authors can be found on the projects web site at the category publications - deliverables.

Contact

To get in contact with the GEN6 project or the partners please contact us.
info@gen6-project.eu
www.gen6-project.eu

GOVERNMENTS ENABLED WITH IPv6
GEN6

This booklet is part of a series of information on IPv6 transition in eGovernment. See www.gen6-project.eu/publications/booklets/ for further available booklets. Booklets already published:

- Smart communication solutions in emergency situations
- Energy efficiency in school networks with IPv6
- IPv6 application in the road domain
- Addressing and transition from IPv4 to IPv6 in government networks
- Why are governments on IPv6? Start your IPv6 project right now
- IPv6 standards and RFCs - what profiles can do
- Secure election infrastructures based on IPv6-clouds
- A National-level IPv6 addressing concept for the government

Layout by Citkomm, all photographs © 2015 by fotolia.com