GOVERNMENTS ENABLED WITH IPv6

GEN6

IPv6 IMPLEMENTATION

IN EXISTING eGOVERNMENT INFRASTRUCTURES

This project has received funding from the European Union's

European Commission

INTRODUCTION

After some years of postponed IPv6 adoption, in February 2011 the depletion of the central repository of IPv4 Internet addresses managed by the IANA finally motivated countries to walk down the road to the almost infinite address space provided by IPv6. The dependence of the global economy on the connectivity offered by Internet access has forced to start the long and complex process of IPv6 transition in all countries. While the basic technological aspects can be considered resolved, the expected coexistence of both protocols for a long time to come raises the need to coordinate actions at national and supranational levels.

Governments have played in the past a tractor role in promoting new technological innovation supporting the evolution from industrial society to the knowledge society, so it is necessary that they exercise leadership once again in the transition to IPv6. This need has been identified as a priority by the European Union, which, in the „European eGovernment Action Plan 2011-2015", demanded governments to lead by example by taking "action to upgrade IPv6-relevant eGovernment infrastructure (portals, websites, applications etc.) and online services of public interest".

In that sense, some European governments have already started their IPv6 transition, acquiring valuable knowledge about the challenges of the process. Among them, Germany, Spain, and Turkey have carried out, as part of the GEN6 project, three national pilots of transition to IPv6 focused on the upgrade of different elements of the eGovernment infrastructure: government networks, website and services, and data centres.

This booklet describes some relevant aspects of the IPv6 transition in eGovernment services, based on the experiences of these national pilots, which will help you to design your own way to IPv6.

NETWORK ARCHITECTURE AND STRUCTURE

Transition planning

One of the first things you need to consider in your transition is whether you are dealing with the network of one (or several) governmental units or with a government national network that connects different administrations (such us the DOI in Germany or Red SARA in Spain). There exist important differences in the transition to IPv6 between both cases. These differences are not so related to technical issues as to organizational and coordination issues. In the case of governments' national networks addressing is one of the key elements due to the complexity of obtaining large IPv6 spaces. Therefore planning for temporary IPv6 assignments while managing the process of getting the permanent ones may be a good practice for fostering the transition.

In case of the rollout of IPv6 in a governmental unit, it is recommended that the transition starts "from the edge", i.e., from the Internet-exposed networks. This gives the opportunity to enable IPv6 first where it is needed and visible the most, with enabling public services with IPv6. Still isolated IPv6-enabled islands can then be connected in later steps. For enabling the "Internet edge", the Internet uplink and the demilitarised zone (DMZ), especially the website(s), are the most relevant components. Initially, the need of a connection to the IPv6 Internet is more crucial than the transition of the internal infrastructures, since IPv6 connectivity is not always easy available. This must be checked in detail, in order to verify that there is a provider that really supports IPv6 on a given solution. Usually it will be integrated into an existing multi-provider setup. Besides, the transition of the web-servers and web-services is generally easy because the infrastructure of the demilitarised zone is commonly not as complex as the subnets of the backend networks.

Apart from the external connectivity with the Internet, internal connectivity to other governmental institutions or to the government national network has also to be considered, as well as VPNs and legacy lines (leased lines, dialup etc.).

Another reasonable approach, when the transition project touches different networking areas with different priorities, is to plan and act upon those areas independently in the first phase. After finalizing the activities in one segment, connect it with other areas already finished. That is, network segments are enabled for IPv6 one by one, so that IPv6 connectivity can be tried in small steps. This way, the transition is most often done in a button-up fashion, i.e. migrating the layer-2 and layer-3 devices first, then end systems and servers, and last but not least the active applications.

In the end, the good news on network structure is that the overall layout of your local networks (inside / outside, security zones, DMZ etc.) can stay the same as before, since all the concepts which led to this structural design are independent from the IP version used. Still, many configurations, e.g. routes, access control lists, and filter rules must be extended so that the same functionality and levels of security and performance are provided by the network after the addition of IPv6.

IPv6 addressing

One of the most important steps for the IPv6 transition is the IPv6 address allocation and address assignment. For the address allocation one of the crucial points is to determine the IPv6 prefix length. You may leverage the current IPv4 address space used, considering there will be no NATs (i.e. no private IPv6 addresses in an IPv6-enabled network). You should keep in mind that each device will be assigned a globally unique IPv6 address. You also have to think about the source for these IPv6 addresses, that is, whether you will get the IPv6 address space from the government national IPv6 addressing plan or you will ask your RIR for your own address space or you will use IPv6 addresses obtained from your ISPs.

After address allocation you should plan the assignment of the IPv6 addresses to the subnetworks. The critical point here is that at least a /64 prefix must be used for each subnet in an IPv6 network. Exactly a /64 prefix must be used for each subnet with end systems (clients). You can determine how many IPv6 addresses will be required at each subnet by looking at the current IPv4 setup and logs.

Due to the address shortage when using IPv4, subnets with public IP addresses were often structured in a way to make them only as big as needed, e.g. using a /28 IPv4 network for a DMZ subnet for around a dozen of servers. For IPv6 subnets, with the huge IPv6 addressing space available, such restriction does not apply. You do not need to worry, in every case a /64 IPv6 subnet will have room for as many clients as you had in any size of IPv4 subnet. Moreover in IPv6 the bits for subnetting are restricted to the first 64 bits only. This means that even for a transfer network with only two active hosts a network with 2^64 IPv6-addresses has to be designed. As network components are designed with this restriction in mind one should not try to use more bits for the subnet, as this may cause malfunctions in the network components used.

However, in most cases, IPv6 will be deployed together with IPv4, so that both protocols can be used (dual stack approach). This will impose some restrictions in the design of the IPv6 address scheme.

In that sense, maintaining the current network architecture and trying to reflect the previous IPv4 addressing plan structure into the new IPv6 addresses has proved to be a good approach to reduce the complexity of the transition in the initial stages. This can also be seen as an opportunity to document, re-think, and possibly restructure your own local networks (or parts of them) before the actual transition takes place. Cleaning up your long-grown, and possibly sub-optimal, network before going dual-stack is a much less tedious task than doing it at the same time or afterwards.

When thinking about the numbering of subnets and endpoints, it is good practice to define a structure that allows the use of aggregatable address ranges. In that sense, you can reserve some bits of the IPv6 address prefix for the location of the network, and some bits for its use (e.g. transfer networks, server segments, DMZ, management network, or LAN ranges), and aggregate based on them. In the case of the host part, you can define some bits for the device category, (e.g. router, server, client, loopback address, printer, phone etc.), and also use part of the IPv6 address to carry information of the IPv4 address (e.g. the second and third word of the address carries the 3rd and 4th byte of the IPv4 address of the system), in order to facilitate the analysis of the logs by the network administrators.

Finally, you will have to think how addresses get configured (static vs. dynamic; with stateless or stateful techniques; with or without privacy extensions). Usually, static addresses with manual configuration are reserved for servers, and dynamically assigned addresses for clients.

Transition approach

One of the key elements of the transition is to define the overall approach regarding the technical implementation: whether you will use dual-stack, IPv6-to-IPv4 translation, IPv6-native infrastructure etc.

In most cases, dual-stack will be the only option to consider. Up to now, there is no realistic way to implement an IPv6-only infrastructure on the client side, while on the server side it is also not useful to separate the IP traffic by protocol version, especially when the existing infrastructures are very heterogeneous. In this case, the application data would have to be kept in a synchronous state for both IP worlds. Therefore, to avoid this additional effort and increased technical complexity (which can lead to separate or duplicate the systems on the application level), the dual-stack approach is usually chosen as the basic concept.

However, it is good to consider in advance that probably different transition mechanisms will have to be deployed in order to have your services ready in IPv6. Though dual-stack should be the preferred approach for the reasons mentioned before, tunnels cannot be avoided in some cases when networks must connect through non IPv6 ready infrastructures, something that it is not unusual since many telecom operators do not offer IPv6 transport yet in all their networks. IPv6-to-IPv4 translation, on the other hand, can be an effective means of achieving IPv6 visibility from the outside world without devoting too much effort, and should be evaluated as an option, at least in the beginning. In fact, this is a commonly used approach for IPv6 access to web applications aimed at citizens, implemented by a reverse proxy solution established as an application level gateway (e.g. for HTTP).

Finally, apart from the undoubted benefits, you should also keep in mind that dual-stack increases management workload for the network operation since the administrators are responsible for the security and monitoring of both protocols now.

And, as always in ICT projects, besides the technical issues you need to investigate the administrative and human resource issues for the IPv6 transition, because surely you will need to convince not only the management but also the implementation teams of the need of going down the road to IPv6.

NETWORK DEVICES LEVEL

All networked devices in an IPv6-enabled network (usually a dual stack network) should be checked on their IPv6-readiness. Some devices, such as e.g. routers, must be able to support IPv6 in such an environment. Other devices, such as end systems, may well run as IPv4-only in a dual-stack network. Switching on IPv6 in their local network may have unknown side-effects to their connectivity – therefore every device needs to be checked in preparation.

For the most crucial devices (routers, switches, and security devices) their administrators should check the IPv6 support in detail, depending on their needed functionalities. For this purpose it can be helpful to check their features one by one by e.g. consulting the IPv6 readiness standards (gold or platinum version), or the publicly available IPv6 profiles tables. Especially for IP routers not only the IP packet forwarding engine(s) must be able to handle IPv4 plus IPv6, but any existing and used routing functionality (exchange of routing information and computation of routing tables) must also support IPv6.

This can demand switching to a newer version of the used routing protocol, too, and therefore


must be planned with care not to disturb the working IPv4 routing. Probably the most crucial checks must be made when enabling IPv6 security devices with IPv6, as its features for IPv6 may not be on par (yet) with those for IPv4.

In that sense, you have to take into account that some network and security appliances may be problematic in terms of IPv6 deployment. There is no clear and common definition of "IPv6-enabled" for network and security appliances. Although it does not differ too much for the basic functionalities such as packet forwarding, routing etc.. For the advanced features such as flow exporting, mobility or multicast the definition of IPv6-enabled may differ. Therefore, institutions that require getting an IPv6-enabled appliance should define clearly their requirements and level of support, such as Quality of Service or mobility support. This can be done by specifying a detailed list of standards to be supported by a device, for example by listing the Requests For Comments (RFCs) that the device must implement.

Moreover, you should not forget that in addition to running the "core" functions (e.g. packet forwarding) of a network device on IPv6, sooner rather than later the device should also be able to be configured via IPv6, i.e. its management interfaces should support both IP protocol versions, too. The same applies to the ability to provide monitoring information, e.g. packet counters. Especially for routers, IPv4 and IPv6 counters, and the respective SNMP MIBs should be available. If needed, devices must be upgraded with a newer firmware version, which may add newer IPv6 features to a device (or IPv6 support at all).

As you can see, one of the main issues in the transition is determining the actual compatibility of the existing equipment and services with IPv6. Probably, you will find that not all existing devices and services support IPv6 yet. Though some of them can be easily upgraded, there are others whose updating would require considerable investments. This is why it is important to define clearly which equipment and software that does not support IPv6 should be really upgraded or replaced in the transition. A reasonable approach is focusing initially on those elements that are essential to provide IPv6 transport capabilities, while leaving in IPv4 the ones that do not, such as those that support network operation.

The good news is that, due to the procurement policies implemented by many governments demanding IPv6 compatibility, nowadays most of the network devices used in governmental networks support IPv6 as they are or after an upgrade of the software versions. From the experience of the GEN6 pilots, you may not expect problems at the switching level other than the potential lack of IPv6 support in their management.

In the case of the routing level, IPv6 is broadly supported by commercial routers, so their IPv6 enablement is not a challenging experience; you may have to pay more attention if you use software routers, because for some older operating systems, such as e.g. SUSE Linux 11.3, IPv6 support is not technically mature. The challenges are often in the details, for example in the configuration of dynamic routing with IPv4 and IPv6, or in the implementation of fail-over solutions in a dual-stack environment. Be prepared that not all configuration changes will work as expected after the first try.

NETWORK BASE SERVICES LEVEL

For all basic network services inside a local network an upgrade is needed to support the transition to IPv6. "Upgrade" will at least mean to slightly modify the configuration of an existing service. It can mean the installation of a newer version of the service (plus configuration), or, in the extreme case, switching to a completely different tool for the purpose altogether. It is highly recommended to verify the IPv6 capabilities of network services before actually starting the transition (consult handbooks, Internet, manufacturer, support).

Affected base network services include servers for:

- DHCP (plus, if used, DHCP relays)
- DNS (support for AAAA records, plus connectivity via IPv6)
- NTP
- Directory services, such as LDAP
- SMTP mail servers (MTAs)
- IKEv2 for automatic IPsec tunnel management

Additional network-related servers include, but are not limited to:

- Network monitoring and surveillance solutions
- Proxies, reverse proxies and load balancers
- Firewall and intrusion detection systems
- Gateways and tunnelling appliances (e.g. VPN concentrator)
- Management tools, and managed entities (e.g. IPv6 support for SNMP agents)
- IP address management (IPAM) solutions

Special care must be taken when transitioning "NAT boxes", i.e. middle-boxes that perform IPv4 source address rewriting (also called masquerading), since NAT is not available for IPv6. The lack of source NAT for outgoing IPv6 connections means that desired properties of NAT such as hiding network structure or endpoint identifiers (if needed) must be obtained by other means, e.g. by using an HTTP proxy for outgoing connections.

From the experience of the GEN6 pilots, preparing network base services for IPv6 is not especially problematic, since most of the products used (e.g. Microsoft base network services for Windows Server 2008 R2, BIND for DNS, Squid for reverse proxy, Stonegate and PaloAlto for the firewalls, Snort for the IDP/IPS) support IPv6. Some issues can be found in the setting up of the load balancers and reverse proxies, due to the need of a proper adjustment of the Maximum Transmission Unit (MTU). Regarding VPN connections, the procedures for establishing IPv6 tunnels are quite similar to those of IPv4, so no significant problems should be expected there.

In the case of monitoring, most of the commonly used tools (such as Nagios or CISCO works) support IPv6. For open source solutions, much of the monitoring job is performed by test programs and scripts contributed by the community, and most of them are IPv6-aware. You will need to configure these tools, but no big challenges are to be expected here.

In the case of management tools, a common approach is to leave the management networks, in the first stage of the IPv6 transition, running in IPv4. On the one hand, some of the commonly used management tools do not support IPv6 (e.g. Dell Remote Access Controllers (DRAC) version 4); on the other hand, since probably no IPv6 only government network is to be seen in the near future, management data can be fetched and configuration data can be send via IPv4. The use of SNMP over IPv6 is usually not foreseen, 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.

Security aspects of using IPv6

The security aspects of running an IPv6-capable network for eGovernment services are one of the most crucial parts of the IPv6 transition. Some of these are technical aspects that originate from the involved devices (e.g. firewalls) or from the use of IPv6 addresses, but others are also non-technical aspects such as training for technicians and other employees. All of them have to be considered to keep the same level of security as it exists nowadays in an IPv4-only network environment.

The autoconfiguration features of IPv6 will require some more attention for the things going on at the network level. Router discovery and address autoconfiguration may produce unexpected results and security holes in environments with unattended but IPv6-capable and enabled systems.

You should watch out for IPv6 prefixes announced through the VLANs and should keep track of the IPv6 addresses that a server or a device has. If a router or a layer 3 switch is configured accidentally (or because of the default configuration) to announce IPv6 prefix to a VLAN, this would cause servers and devices with their autoconfiguration setting enabled to get new IPv6 addresses without your notice. As a result you would see unexpected IPv6 addresses in your logs and flow data. This is a case especially for older versions of Microsoft Windows hosts and servers, due to the IPv6 tunnels (ISATAP and Teredo support) enabled by default in them.

It is worth to mention that the authenticity and confidentiality of the transmitted information are considered crucial aspects in IPv6 since the IPsec protocol implementation has initially been set as mandatory in every node of the network, but finally relaxed to recommendation due to extremely constrained hardware deployed in some devices (e.g., sensors, Internet of Things (IoT)) where a full IPsec implementation is not justified. This security protocol is also present in IPv4, but as an optional choice. This fact let administrators to easily set cryptographic protections over their data links. It implies setting and managing a set of IPsec policies to determine which traffic is desired to be protected. The IPsec tunnel generation and key management can be performed manually, however, this is not very practical. IPsec requires an automatic way to perform this. Currently, the default automated key management protocol is IKEv2.

Obviously, these and the rest of the applied security policies will need to be updated in the IPv6 transition. These policies include access control rules (firewall rules, access control list rules etc.) and performance criteria in order to protect the whole system from DDoS like attacks. Do not forget to extend the configuration of the security devices in order to represent the


same rules for IPv6 which were already configured for IPv4 – such rules are usually not applied automatically for both protocol versions. Also, be aware that you will need to configure the security tunnels of your VPN. All VPN solutions (servers as well as clients) must support IPv4 and IPv6, else some client may for example transmit IPv4 through a VPN tunnel but IPv6 traffic outside of an activated tunnel.

In terms of IPv6 compatibility of the security devices, most of the commonly used equipment is already IPv6-enabled, or can be made IPv6-ready after upgrading firmware or software versions. You will have to check then your firewalls, IDS and IPS, the affected application layer gateways (proxies and reverse proxies), and other security subsystems such as virus scanners, including those active on end systems.

Finally, after completing the IPv6 transition, it is good practice to have security tests performed by an external information security company in order to check confidentiality, integrity and availability of the whole system. Recently, several different types of attacks have been observed over IPv6. For the time being, simple attacks such as SYN floods are the most common types, however, IPv6 threats will surely get more frequent and complex in the future.

APPLICATION LEVEL

Finally, the use-case-specific applications software (user clients as well as server software) that uses IP network connectivity must be checked for their operation with IPv6. This is true for use in an IPv4/IPv6 dual-stack environment, and even more so in an IPv6-only environment – being able to work in an IPv6-only environment will become important in the future, for sure. "Application software" can be anything in this context, from web servers and web browsers to specific governmental applications, and apps running on mobile devices.

From the experience of the GEN6 pilots, applications built on a high level language (and run-time) are often less dependent on the version of IP being used for network connectivity. This is because with a high level language setting up an IP connection uses a higher abstraction. When only hostnames are used instead of literal IP addresses, a program can be completely unaware of the IP version that is available and used by the system underneath. Programs that are programmed in a language with less abstraction, such as e.g. C, often explicitly handle IP addresses and connections for IPv4, and IPv6 support has to be enabled first by configuration, or even by re-compilation of the program. Also, transparent support for IPv4 and IPv6 is less often an issue with scripting languages, due to their high level of abstraction. Some programming languages provide both, explicit and implicit IP version selection, e.g. by allowing to write both, new IPv4Connection() / new IPv6Connection() and new IPConnection() in the source code.

In addition to software listening for incoming connections or connecting to services by itself, related systems can be IPv6-unaware. This can, for example, cause problems with those systems devoted to IP address logging, log analysis and/or storage of IP addresses in databases. In that sense, a typical problem is to have a table column or a data reserved space too small for storing longer IPv6 addresses. In the case of IPv6 address storage, due to the options for writing an abbreviated form of an IPv6 address, it is good practice to either normalise all logged literal IPv6 addresses, or to store any logged IP addresses in binary form (suggested in case they are stored in a relational database).

To avoid these pitfalls, it is therefore recommended to test business-critical applications at first in a laboratory environment, in different setups (IPv4-only host/server, dual-stack host/server, IPv6-only host/server), with literal and with textual endpoint identifiers, and thoroughly check auxiliary systems for monitoring, logging, and analysis of data containing IP addresses as well.

Regarding applications actually running with IPv6, the experience of the GEN6 pilots can be summarised as this: either the installed application works with IPv6 out-of-the-box or a deep error analysis is needed (i.e. more work than just enabling IPv6 in the application's configuration). This is because easy solutions for fixing the IPv6 compatibility problems are rare, and an investigation of the network connections traffic of the application is commonly required.

In many cases, due to the fact that eGovernment applications serve millions of users via high available architectures (what brings many different challenges and complexity to be managed) the use of industry standard equipment and software is important. Hence, vendor-produced and licensed applications are preferred rather than in-house-produced scripts and applications which may be dependent on a single developer.

The good news about commercial products used to run eGovernment applications is that you may expect few issues with IPv6, since most of them are already adapted to the new protocol, or they can be adapted easily by updating to the latest versions.

There can be some problems in the case of specific applications (e.g. if they were developed by small companies a long time ago, and have not been updated), but this should be noticed at the end of your practical tests. And also one word regarding open source solutions: some can be problematic in IPv6 support, since IPv6 features may not be prioritized in the code development of the project. While open source solutions for network management are often IPv6 aware, solutions more focused on the application level may present problems here.

In case you have to deal with in-house applications and scripts (e.g. a script that shows the users' latest three login IP addresses on the login web page), you may expect no issues either, once the good practices for development, such as abstracting the network layer from upper layers, increasing the length of IP address fields, and using host names instead of IP addresses have been followed. Though some review and adaptation of the source code is probably unavoidable, this will be in most cases just a few patches.

Practical tests

As has been mentioned before, it is highly recommended that you plan for some tests of your eGovernment applications running in an IPv6 environment before performing the actual transition of the life systems. A setup of a test environment with the same configuration as the production environment is desirable. This includes not only the network structure and network elements but also typical end systems and installed software. If possible, it is also advisable to have this test environment for hardware appliances and software applications prepared to run in IPv4-only, dual-stack, and IPv6-only modes, in order to realistically evaluate the differences in performance in the three cases.

Once this test environment is set up, any new feature should be first tested in the test environment and, after completing the tests successfully, may be moved to the production environment. These tests should be performance and conformance tests, including access and penetration tests over IPv6. This is especially relevant in the case of critical features such as monitoring and security services, due to their role in preventing the production environment from attacks and unauthorized access. It is recommendable to check out applications in a test environment in an IPv6 only mode. Experiences show that applications sometimes start working well with IPv6, but, in later stages of use, communication falls back on IPv4. This is often caused by integrated drivers and third party software that may be not in the focus of the application vendor itself. However, you must take into account that in the case of eGovernment services that are largely used by citizens, you may obtain significant differences in performance between the test and the production environment.

Additionally, IPv6 implementation in large scale infrastructures can pose some problems simply due to the fact that some details may not be seen in the pre testing. These infrastructures usually have strict procedures for implementing changes. This may lead to need several attempts before getting to a successful configuration.

Prior to all that, you will need to perform connection and performance tests (including throughput, jitter etc.) while setting up the connections between your institution and its external networks (Internet, other government units, government national network). These tests will require, among others, checking traffic processing through VPNs, HTTP communications, and DNS IPv6 capabilities. After these connections are established, it is advised to create a separate IPv6 test LAN in order to test devices, configuration and security policies.
From the experience of the GEN6 pilots, practical tests have shown that the main concepts of IPv6 are not so different from the concepts used in IPv4, so its implementation should not be difficult for most of the networking staff. Care must be taken of not overlooking things or making mistakes due to the new, unaccustomed addressing scheme. This is especially important when thinking of security, since all security elements must be configured to handle both protocols.
At the end, the bottom line is that IPv6 implementation must be tested seriously and not only claiming on the point that it is "just another IP protocol in parallel".

CONCLUSIONS

The three eGovernment national pilots in the GEN6 project (Germany, Spain and Turkey) have similar targets: examining existing eGovernment services currently based on IPv4 and building a pilot for selected services to ease the transition to IPv6.

Although the environments in which the pilots are being implemented (technical and administrative responsibilities, existing infrastructures, pre-existing addressing plans, administrative level etc.) are rather diverse, as well as the challenges encountered and possible solutions, there are common findings that can be valuable to other governments that are planning to start a transition to IPv6.

On the technical side, there are some overlaps to be exploited when common infrastructure components are updated, such as switches, routers, operating systems, and DNS, e-Mail, and firewall systems. All these need to have a sustained IPv6 support, working in a real-live environment, to make possible the transition of eGovernment applications and services that are based on them.

The single most important aspect of the transition of an existing government service to IPv6 is business continuity. Therefore, and depending on the technical environment, different techniques are advisable to add IPv6 support to an eGovernment service. In the three GEN6 pilots, IPv6 has been enabled in addition to the existing IPv4 support, what means that all pilots have mainly chosen the dual-stack approach (whereby each involved networked component is configured to run IPv4 plus IPv6 at the same time). In some cases, to complement this basic approach, some servers have been made available via IPv6 to the outside world by adding an HTTP reverse proxy "in front" of them. It must be noted that all pilots have chosen to build an IPv4-only test bed initially, which resembles the environment of the real (business) applications as closely as possible, and to work on the transition of this test bed. Knowledge gained in this process is of invaluable help for the transition of real servers or services later on.

In summary, the transition to IPv6 is possible, though some aspects may need further investigation. In those cases where there is a temporary lack of IPv6 support, using a dual-stack approach can provide the required business continuity. Anyhow, structured planning and testing are always essential for the success of the initiative.

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-NC 3.0) licence. Consequently, you are free to share (copy, distribute, transmit) this work, but you need to respect the attribution (respecting the pro-ject 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 capa-ble 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 powered by

This work was 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:
Carlos Gómez Muñoz, MINHAP;
Antonio Skarmeta, UMU;
Carsten Schmoll, Fraunhofer FOKUS;
Martin Krengel, Citkomm

"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 in:
info@gen6-project.eu
www.gen6-project.eu

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
- Requirement analysis for eGovernment services with IPv6

Copyright of certain GEN6 partners and the EC. Shared, reproduced or copied "as is", following the Creative Commons "Attribution-NonCommercial-NoDerivs 3.0 Unported (CC BY-NC-ND 3.0) licence".

Layout by Citkomm, all photographs © 2014 by fotolia.com