GOVERNMENTS ENABLED WITH IPv6

GEN6

IPv6 STANDARDS AND RFCs

WHAT PROFILES CAN DO

This project has received funding from the European Union's

European Commission

MANAGEMENT SUMMARY

Since the early days of the Internet, the Internet Protocol Version 4 (IPv4) has been used to transfer digital data. Today this protocol is widely used in internal networks of agencies and organizations, as well as in provider networks across the globe. The Internet and all the networks using IPv4 today have to face a profound technological change because it is inevitable for all networks to support the successor IPv6 in the foreseeable future.

There are two key answers to the frequently asked question about the essential factors driving the Transition to IPv6:

- There is a huge transition pressure caused by the scarcity of new, still unused IPv4 addresses today (already in Asia, very soon worldwide).

- The world faces an increasing demand of IP addresses for networked small and large devices, from sensors to smart phones to washing machines that need to communicate over IP networks. By running out of IPv4 addresses the situation becomes even worse.

Both factors together massively accelerate the transition to IPv6, foremost in the core of the Internet, and within new devices. In the future, many devices will only have an IPv6 address rather than an IPv4 address and can only be contacted by this IP address. Therefore, a transition to IPv6 assures not only the availability of a sufficient number of IP addresses, but also the accessibility of one's services for the future without being dependent on a provider.

The IPv6 profile for the public administration described in this document supports the evaluation of existing devices and procurement processes. The definition of necessary / mandatory, useful / recommended and optional features of IPv6 devices enables the detailed specification of selection criteria. Requirements can be specified in terms of device roles (router, firewall ...) and usage contexts (stationary, mobile ...), simplifying the assessment of the fulfilment. The profiles can also be used to assess existing devices, concerning their usability in IPv6 environments.
All profile documents focus particularly on the needs and characteristics of governmental administrations (e.g., existing networks and security requirements), thus creating the basis for a targeted and structured start into the transition to IPv6 for the public administration.

For further detailed descriptions, have a look at the documentation published by the GEN6 project on the web page www.gen6-project.eu .

STANDARDS AND RFCs

The protocols concerning the global Internet are written as Standards documents (STDs) and Request for Comments documents (RFCs) by the Internet Engineering Task Force (IETF). Roughly 200 of those documents are concerned with the definition and operation of IPv6, including adoptions of related protocols (e.g. ICMP -> ICMPv6), so that an interoperation with IPv6 is possible, as it is with IPv4.

Informative RFCs

RFC documents are divided into different categories:

- Standards Track (Proposed Standard, Draft Standard or Standard)
- Informational
- Best Current Practice (BCP)
- Experimental

Therefore, one could expect that all relevant information for an IPv6 profile are contained within the standards documents, and that BCP documents only contain things like recommendations for network and device configuration. In practice, the borders between the document types are not that clear.

The reasons for this is the process by which standardization in the IETF works: New topics (for example some security mechanism) might be discussed by different working groups, and tackled with different approaches. This wide-spread interest and the participation of different groups till the final version of an RFC have a high influence on the final result.

It is this broad consensus process during the writing of an RFC document, which leads to relevant, practically usable protocol definitions in the RFC standards, but also sometimes to (still) open detail questions and a not-so-hard differentiation between the different types (STD, BCP …) of RFC documents.

Whoever is in charge to plan a transition to IPv6 will find a lot of guidelines in the internet but at a certain point in time when it get to the bits and bytes you have to deal with the RFCs. Over 200 documents to read and to search for the information you need for your project. That's where profiles will help you to identify the right information and parameters to get it up and running.

PROFILES? – PROFILES!

The profile document for the public administration provides support for the procurement of IPv6-capable hardware and software components. To reach this goal it specifies, which IPv6 standards have to be supported by a networked device or system, in order to fulfil its duties in an IPv6 environment.

It is very important that IPv6 will be introduced into network environments across-the-board, because of the IPv4 address shortage. This means that every new purchase of networked devices or software must take IPv6 capabilities into account to guarantee a level of readiness for the future – optimally even for an environment where IPv4 is not available anymore at all.

The adoption of IPv6 can be done in different ways:

- Based on an existing network infrastructure, IPv6 can be added to IPv4 in parts or whole of the network (e.g. a companies' Intranet). Using IPv4 and IPv6 together in a single network is called "dual-stack" approach.

- In newly created networks (or subnets) with clearly defined tasks and use cases, one can consider to run IPv6 in an IPv6-only configuration. For this to work, all components (hardware, software (OS, applications)) must be able to run without any IPv4 available.

- The detailed analysis of the scenarios stands at the start of building an IPv6-capable network, regardless of whether the network is based on existing componentsor created out of new acquisitions. Based on this, it needs to be defined, which network functions should be used (e.g. stateless autoconfiguration).
  The definition of scenarios and derived functions is an important precondition forapplying the profile documents. They determine, which sections of the profile have to be taken into account for the planned network, and in effect, which features are optional, recommended or mandatory.

The profile should be seen as a kind of checklist to determine the set of requirements that are important for the targeted network. This set can then later be used as input to the functional specification document to be used in procurement. It is not appropriate to just refer to the IPv6 profile in a "must-be-fulfilled" manner; it is merely a basis to lookup the concrete set of requirements.

Alternatively, such a set of requirements can be used to query detailed feedback from network equipment vendors about the applicability of their devices for the planned IPv6 network, based on a listing of relevant IPv6 standards (request for comments, RFC).In both cases, you can use the profile as a basis for communication between vendors and customers about detailed technical requirements, in the form of relevant IPv6 standards (request for comments, RFCs) and associated require¬ment levels. Additionally, we point out that the combination of technical systems in a network which all do fulfil the IPv6 profile does not necessarily lead to a fully functioning network setup – the fulfilment of the profile requirements is however a necessary minimal requirement for successful interoperation.

Note that the concrete configuration of the systems is not part of the IPv6 profile. This effectively means that setting up the networked systems in a useful and compatible way is a separate project, after procuring systems which have all the required features implemented. In practice, even systems which are compatible on paper and do support all the required features, may experience interoperability issues, due to slight differences in IPv6 implementations. Therefore, dedicated interoperability lab tests are recommended, to see systems behaviour in practice.

EXISTING PROFILES FOR IPv6

Existing IPv6 profiles usually describe mandatory / recommended / optional requirements for IPv6-enabled devices or implementations, based on STD and RFC documents. There may be additional technical requirements in any given use case, for example depending on specific quality- or security-related requirements. Use of the profiles (and conformance to any one of them) is only one step towards practical interoperability, as it depends also on the actual devices' configuration, and possibly also vendor (in)-compatibilities.

REQUIREMENTS FOR IPv6 IN ICT EQUIPMENT (RIPE-554)

The Réseaux IP Européens Network Coordination Centre (RIPE NCC) supports the technical coordination of Internet infrastructures within Europe. In this frame¬work the IPv6 working group has developed „Requirements for IPv6 in ICT Equipment“. These requirements have been documented in November 2010 in “ripe-501” [ripe-501]. As of June 2012 an updated version of this document is available in “ripe-554” [ripe-554].

The ripe-554 document – and specifically the requirements documented therein – can be seen as a supporting collection of best practices for the public sector and commercial companies alike.

Ripe-554 identifies the essential devices classes: Switches (for end users or enterprises), routers, end systems, security devices (classified as either packet filters, application layer gateways, or intrusion detection systems), CPE routers, mobile devices, and load balancers. For each class it identifies mandatorily and optimally implemented RFCs. During procurement, devices should be preferred that implement a majority of the optional requirements, in addition to all the mandatory ones, of course.

Ripe-554 is relatively coarse in its characterization of the different RFCs, as it does not differentiate between the requirements for independent features inside single RFC documents.

DEPARTMENT OF DEFENSE UNIFIED CAPABILITIES REQUIREMENTS 2008, CHANGE 2 (UCR 2008, CHANGE 2)

This document, which is actually from December 2010, describes quite comprehensively a multitude of requirements on IPv6 devices and implementations for procurement by the United States Department of Defense (DoD).
Subchapter 5.3.5 of it documents the requirements related to IPv6. An integral component of the document is the "DoD IPv6 Standard Profiles for IPv6 Capable Products version 5.0", from July 2010.

The document contains a detailed device classification, and it identifies mandatory, recommended, and optional features based on the classification of devices into simple end system / simple server, router, security device (packet filter, application layer gateway), switch, and end system (or specific application).

The document not only lists the required RFCs themselves, but also lists demands on specific functions, and preferences on how given features should be used.

IPv6 READY LOGO PROGRAM OF THE IPv6 FORUM

The vendor-driven IPv6 Ready Logo Program [IPv6Ready] of the IPv6 forum encompasses specifications for conformity tests and inter¬operability tests for IPv6 and related protocols:

The IPv6 base protocol (including SLAAC , ICMP , addressing architecture, explicit congestion notification (ECN), Neighbor Discovery (ND) and Path MTU Discovery)

- IPsec and IKEv2[4]
- Multicast Listener Discovery, Version 2
- SNMP MIBs[5]
- Mobile IPv6 and NEMO[6]
- DHCPv6[7]
- SIP[8]

For this purpose the IPv6 forum provides test suites for automated processing. A successful passing of such test suite authorizes a vendor to assign the IPv6 Ready logo to the tested devices series. There exist dedicated IPv6 test centres, which provide running of the test suite as a service. However, the IPv6 Ready logo can also be awarded by the vendor itself by signing a declaration of conformity, i.e. stating that a devices series has passed the IPv6 Ready tests successfully.

Those tests are – on purpose – very detailed and comprehensive. They take into consideration the targeted role of the system under test, and sometimes go into detail up to checking single messages and message exchanges between devices. On the other hand the number of referred RFCs in the IPv6 Ready tests is relatively small (36 compared to more than 200 in other IPv6 profiles). The IPv6 Ready tests include only checks that can be verified using a standardized external interface of the system under test. Internal variables, such as internal router states are not checked. This means that passing the IPv6 Ready tests does not automatically imply a fully correct implementation of a required feature.

We note especially that network protection functions, as provided by packet filters and application layer gateways, are not captured by the IPv6 Ready tests as these functions are not formally standardized in STD and RFC documents.

---

[1] *Stateless Address Autoconfiguration*
[2] *Internet Control Message Protocol*
[3] *Maximum Transfer Unit*
[4] *Internet Key Exchange*
[5] *Management Information Base*
[6] *Network Mobility*
[7] *Dynamic Host Configuration Protocol*
[8] *Session Initiation Protocol*

A PROFILE FOR IPv6 IN THE U.S. GOVERNMENT

This document [NIST_USGv6], in version 1.0 from September 2008, has been developed by the National Institute of Standards and Technology (NIST), an organization related to the US ministry of trade. The document divides networked devices into end systems, routers, and security devices (packet filter, application-layer gateway, and intrusion detection / prevention devices).

The network-related features are categorized by it into 12 groups: Base features, routing, service quality, transition between IPv4 and IPv6, link-specific features, addressing, IPsec-related features, network management, multicast, mobility support, application level requirements, and special requirements by security devices.

The document goes into much detail concerning the devices' intended usage environment (use cases), and the relations between different features, based on the defining RFC documents. This approach results in a quite complex document, because many features are required only conditionally, in dependence of others. Features are divided into mandatory and optional ones. It does not value or prioritize the optional features, however. The document specifies for each feature which RFCs must be implemented in order to fulfil the desired functionality.

In its goals, the [NIST_USGv6] document comes closest to our IPv6 profile document. Unfortunately, due to its age, some important parts of [NIST_USGv6] are not up-to-date anymore, so that the reader often needs to check for updated or newer RFC documents, to find the latest definitions, when assessing it. Up to the beginning of 2013 no newer version of [NIST_USGv6] has been released.

GUIDELINES FOR THE SECURE DEPLOYMENT OF IPv6

This NIST document [NIST_119], from December 2010, is most of all an IPv6 tutorial, but with a specific focus on IPv6 security issues. It especially informs the reader about those IPv6 security risks, which have not yet been finally solved (e.g. IP first hop security issues in Intranets).

IPv6 NODE REQUIREMENTS

RFC 6434 ("IPv6 Node Requirements") [RFC6434], from December 2011, is an update on RFC 4294 (published April 2006). It is foremost an informal summary and reference of all the fundamental IPv6 RFCs, their main features, and the relevance thereof.

The document divides networked devices into nodes, routers, and end systems. Unfortunately, the document does not regard transit systems (such as security devices without dedicated routing functionality) as a separate class, as all the profile documents mentioned before do.

Some RFCs of the "informational" type are also referred by our profile matrix document, as these sometimes are the ones which specify relevant parameters for practical use of a protocol. In any case it can be beneficial to read the informational RFCs in your area of interest too. In the remainder of this section we highlight important "overview type" RFCs that are relevant for working with our IPv6 documents and IP6 in general.

THE GEN6 PROFILE BASED ON THE GERMAN IPv6 PROFILE

The evaluation of existing IPv6 profiles showed that these profile documents do indeed not represent competing definitions, but represent complementary approaches, showing IPv6 aspects of components from different points of view and with their main emphasis on different IPv6 issues.

All considered profile documents relate to relevant standards documents (request for comments, RFC) and list features from these standards for different classes of devices and in different requirement levels. In this way, the profiles recommend which RFCs (all or parts thereof) are mandated, recommended, or optional, given a specific device, network environment, and use case.

The existing profiles differ in their terminology regarding requirement level, as well in their depth – where one profile may mandate a complete RFC, another may pick specific features from that RFC only. In our comparison and consolidation work we have aligned the data from the other profiles as best as possible, and have explained differences where needed, to motivate our recommendation.

The written results of our work on IPv6 profiles consists of a set of spreadsheets that document the referred standards, their recommends requirements levels, and the comparison to the other profile documents. Where the naming scheme of recommendation levels does differ between profile documents, it is suggested to have a more detailed look into the definition of them, especially when there is a need to work with one of the other profiles as well.

As the development around IPv6 is still very active, and many new RFCs related to IPv6 are still published each year, our recommendations will develop in future revisions of the profile documents, too. These upcoming standards, plus practical experiences of network equipment vendors and users mandate updating our documents in the future.

The GEN6 profile matrix has been structured along two “dimensions” to make it optimally accessible to the reader. These dimensions are:

- device classes and
- functional categories.

The different device classes are described on a separate table sheet. The recommendations per functional category themselves are structured hierarchically on each sheet. In order to avoid redundancies in the descriptions, we first define the "IPv6 node" as the basis for all other IPv6-enabled devices. The sheets for all other device classed then only define the requirements which are needed in addition to IPv6 node. As the profile is targeted initially towards the networks and devices or the public administration, this set had to be extended, leading to the set depicted in figure 1. The "white nodes" in Figure 1 are for structuring only, they do not represent a separate table sheet in the profile matrix.

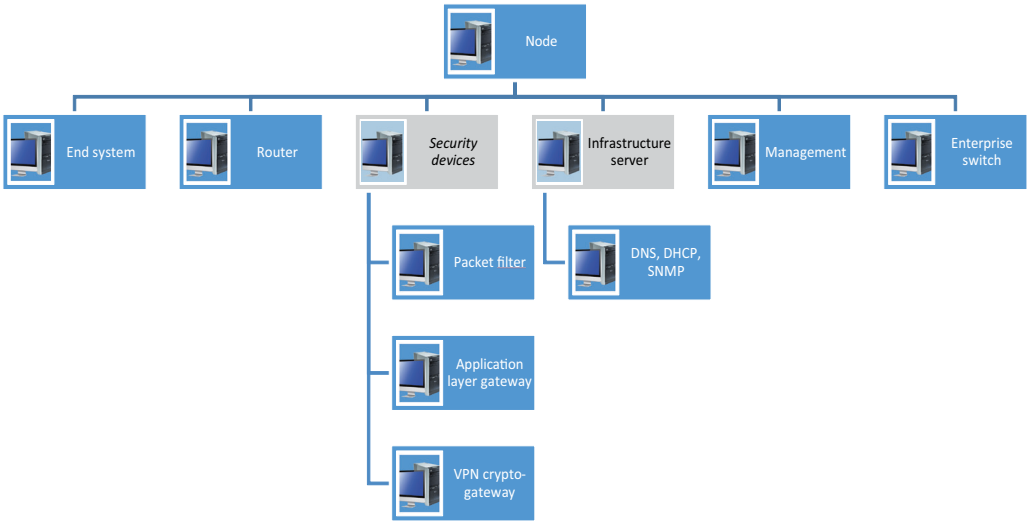

Figure 1: Hierarchy of Device Classes

These classes represent a generic instance of this class. The Node sheet as the basis defines all requirements which affect each IPv6-capable device. A concrete device may indeed implement the features of more than one device class. Take for example a current SOHO DSL gateway – it usually implements functions from the device classes router, packet filter, DNS / DHCP server, and possibly other infrastructure servers as well. Therefore, to collect all requirements for a given device, multiple table sheets have to be taken into consideration (cf. Figure 2).

Security devices (in the public administration) play a special role: Even though they are based on Node as well, their practical implementation may in fact deviate from some "MUST" type recommendations from the node sheet, if this is a functional necessity for their operation. The following figure shows the setup for home router and internet access point. Main feature are from the NODE device and additional requirements are from other device classes to describe the IPv6 capabilities of such a device.

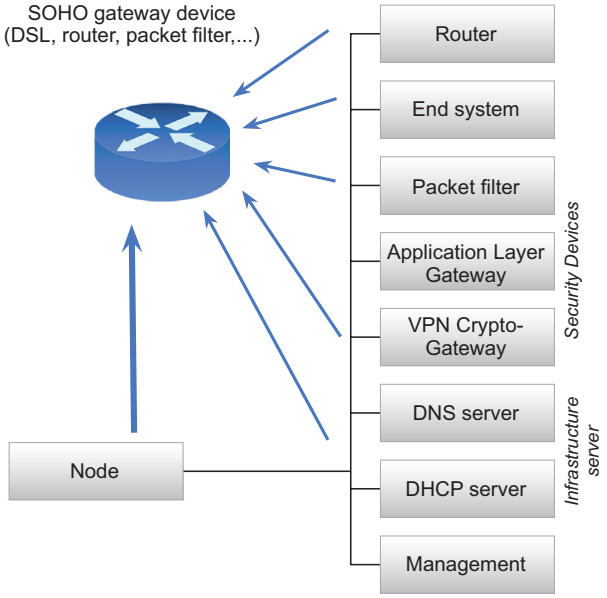

Figure 2: Complex Device Example Based on the SOHO Router Use Case

HOW TO READ THE PROFILE MATRIX

The following paragraphs document some examples on how to read our profile matrix document. For a better comprehension we have included here some excerpts (snippets) from the actual profile matrix document. These snippets can be easily found in the profile matrix document. The following examples show some aspects of its use:

Sheet Node:

Category	Category	Category	RFC	Title	Feature, function	Project recommendation	Comment
Communication of the IPv6 node							
	Basic requirements						
		Basic					
			RFC 2460		Internet Protocol, Version 6 (IPv6) Specification	mandatory	
					Flow Label Field not used and ignored (unless RFC 6437 is implemented)	mandatory	

Figure 3: Profile Example #1 – Feature / Function and Requirement Level

In this example the last line gives additional detail information, related to the specific feature. Each used feature or function which is referred in our profile matrix, will have assigned a recommendation level. If single features from an RFC are explicitly listed in our profile matrix, then (in rare) cases they may show a requirement level that differs from the one given in the RFC itself. Also, our document sometimes assigns requirement levels to a feature which did not show any requirement level in the RFC document at all.

Sheet "Management":

Category	Category	Category	RFC	Title	Feature, fun ction	Project recommendation	Comment
Device functionality							
	Management and configuration					mandatory	
					Access to management / configuration via IPv6 and IPv4	recommended	
					Support of deactivation of an IP variant (IPv4 / IPv6) not used for management / configuration	recommended	if a separate management / configurations interface will be used

Figure 4: Profile Example #2 – Feature / Function without a Related RFC

The second example shows requirements from within the profile matrix which were not specified by an RFC document initially. This is usually the case in our document when the requirements are of a more abstract level, and represent a requirement not represented by a single RFC document. In this example we show the requirement to have devices configurable (remotely) via IPv4 as well as IPv6. The comment field gives additional information, here, under which conditions this specific recommendation is relevant.

IPv6 AND SOFTWARE

Using the previously defined devices profiles for networked devices using IPv6, we mainly ensured connectivity and interoperability on the network layer (layer 3), see the following figure:

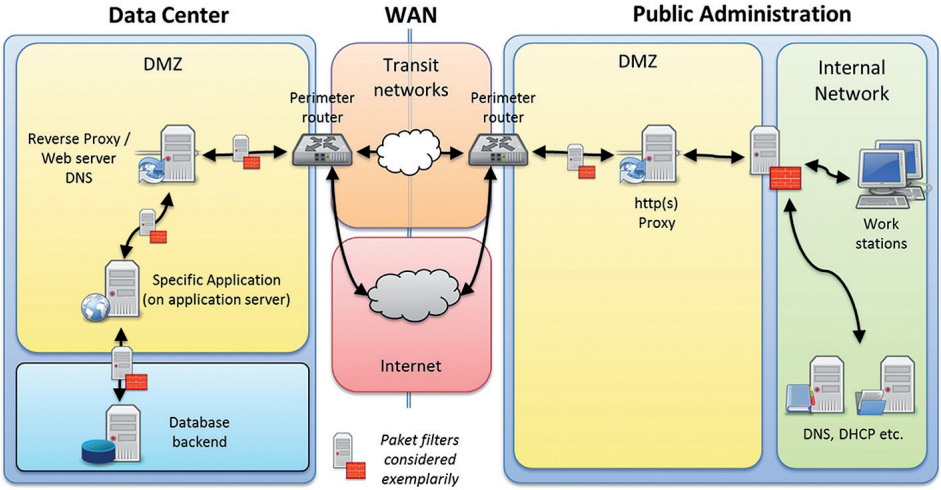

Figure 5: Testbed Connectivity on the Network Layer

The figure shows our proposed reference architecture for use in public administration networks; we describe more details about this architecture in [IPv6_Transition]. This reference architecture figure depicts the logical end to end communication between certain applications. As shown, the use of such an application can affect a communication path covering the work place PC, local networks, administrative WAN networks for coupling administrations, and data centre equipment on the server side. Thus, running and maintaining such an application depends on multiple related devices, networks, and software installations.

The following sections analyse these dependencies in more detail. The chapter concludes with the description of a practical process for a systematic approach to check these dependencies.

COMPONENT-INTERNAL REQUIREMENTS

For this section assume that the goal of making a device work in an IPv6-capable environment is to run it in either an IPv4 / IPv6 dual-stack or an IPv6-only network environment. For a device (running a networked software) to work in such an environment it needs to support at least the base requirements documented in our IPv6 hardware profile.

Following this, each application component to work with an IPv6-enabled network has to support a set of base requirements as well:

- Setting up of outgoing IPv6 connections
- Accepting of incoming IPv6 connections
- Handling of IPv6 addresses for DNS name resolution

Depending on the concrete application, additional requirements may apply, for example:

- If an application uses IP addresses not only for network connections, then the respective functions (e.g. for logging, use in session management, or database entries) must also be IPv6-capable.

- Where during transition some functional elements of the application (e.g. DNS name resolution) still rely on IPv4 being available too (which is fine for dual-stack environments), we strongly recommend to check the application in an IPv6-only environment as well, to be aware of its (non-)functioning in an environment that completely lacks IPv4.

- Where software is available in source code form and is deemed to be IPv6-capable, it has to be assured that upon compilation the IPv6-support is also compiled in (usually by setting compile time parameters such as "–enable ipv6").

DEPENDENCIES FROM OTHER (EXTERNAL) COMPONENTS

Following the previous chapter, we can now have a look at dependencies of a software application on further components and on systems in its (network) environment. The following figure shows classes of dependent systems for an inspected component, e.g. an application:

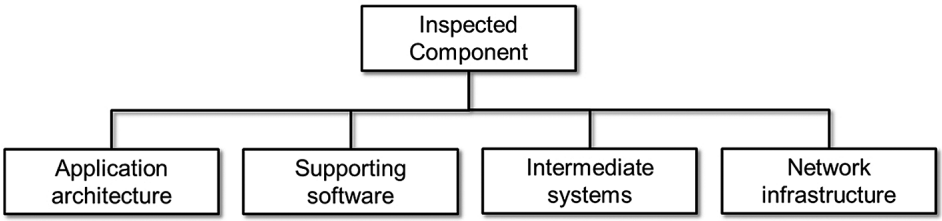

Figure 6: Application Dependencies and External Components

Each class stands for a set of one or more concrete components. Therefore, we can refine them into the (non-complete) list of grouped components. Application Architecture separates different client types such as thin and fat clients; Supporting Software is about generic services like web- or print servers, directory services or database management software. Intermediate Systems are components such as firewalls, VPN servers or application layer gateways, and the class Network Infrastructure contains basic services such as DNS, DHCP or bind. For being IPv6-ready, a dual-stacked application has to ensure that all these dependencies fulfill the IPv6 requirements in order to work properly.

WHERE TO FIND ADDITIONAL INFORMATION

Due to long-grown structures, the public administration already uses a broad portfolio of products, and in different states of maturity. It is therefore recommended to update all existing systems to the latest stable release of software and firmware before starting the migration. Current information on the state of IPv6 support of well-known ICT solutions can e.g. be found here:

http://ipv6int.net/systems/index.html
http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems
http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support
http://www.deepspace6.net/docs/ipv6_status_page_apps.html

Document References for related ICT profile documents:

[IPv6_Transition] BVA, „IPv6 Migrationsleitfaden für die öffentliche Verwaltung“ / “IPv6 Transition Guide for the Public Administration“, online at http://www.ipv6.bva.bund.de

[IPv6Ready] IPv6 Ready Logo Program, https://www.ipv6ready.org/

[NIST_119] NIST, “Guidelines for the Secure Deployment of IPv6“, December 2010.

[NIST_USGv6] NIST, „A Profile for IPv6 in the U.S. Government – Version 1.0“, NIST Special Publication 500-267, July 2008, http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf

[ripe-501] Jan Žorž, Sander Steffann, „Requirements For IPv6 in ICT Equipment“, RIPE NCC, ripe-501, Nov 2010, http://www.ripe.net/ripe/docs/ripe-501

[ripe-554] Merike Käo, Jan Žorž, Sander Steffann, „Requirements for IPv6 in ICT Equipment“, RIPE NCC, ripe-554, online at http://www.ripe.net/ripe/docs/current-ripe-documents/ripe-554

[UCR08_2] Department of Defense, „Unified Capabilities Requirements 2008, Change 2 (UCR 2008, Change 2)“, December 2010
Changes to UCR 2008, Change 2, Section 5.3.5, IPv6 Requirements, online at http://www.disa.mil/Services/NetworkServices/UCCO/~/media/Files/DISA/Services/UCCO/UCR2008-Change-2/07UCR08Chg2Section535.pdf

[UCR08_3] Department of Defense, „Unified Capabilities Requirements 2008, Change 3 (UCR 2008, Change 3)“, September 2011, online at http://www.disa.mil/ServicesNetwork-Services/UCCO/~/media/Files/DISA/Services/UCCO/UCR2008-Change-3/01_UCR08_Chg3_Sections_1-4.pdf

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 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:
Carsten Schmoll (Fraunhofer FOKUS, Germany)
Uwe Holzmann-Kaiser (Fraunhofer FOKUS, Germany)
Carlos Gómez Muñoz (MINHAP, Spain)

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:

- Government motivation for IPv6 transition
- Smart communication solutions in emergency situations
- IPv6 Application in the road domain
- IPv6 Address Planning and Transition
- 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