GOVERNMENTS ENABLED WITH IPv6

GEN6

A NATIONAL-LEVEL IPv6 ADDRESSING CONCEPT FOR THE GOVERNMENT

This project has received funding from the European Union´s

European Commission

MANAGEMENT SUMMARY

Private networks reality in Governments

Governments (and also some private companies) partly use virtual private networks (VPNs) to establish secure communication paths to other governments. Sometimes, special networks are implemented to integrate several governmental organizations into one logical network. On the European level one such network is called sTESTA. Most European member states have similar networks on the national and/or regional level.

Different governmental organizations have their individual ICT strategy. Within the IP addressing in the local networks is not synchronized. Especially in states with a federal constitution the ICT is typically highly independent among the single government institutions. Their connections between networks today are established via highly restricted gateways. Complex transition mechanisms must be configured per each communication path. This causes delays in implementing new services and complexity in operation and troubleshooting. In consequence network complexity itself is often one possible reason to decline new ideas for governmental cooperation.

IP addressing in data networks

Information technology today is based on the Internet Protocol – in short "IP". This protocol is used in the Internet as well is in business networks, in government networks, and in provider networks. These networks mostly use the Internet protocol Version 4 – IPv4. To address each single system on the Internet, IP addresses used for hosts must be unique, i.e. they must not be reused in the Internet. With IPv4 there are only approximately 4.3 billion addresses available.

With the growth of the Internet, IPv4 addresses are running out. Therefore, nowadays IPv4 addresses are handed out only with strong restrictions and limitations. As a solution for the shortage of IPv4 addresses, the Internet protocol version 6 (IPv6) has been developed already many years ago. IPv6 provides among other improvements a significantly larger number of host addresses, to solve the address shortage problem.

With IPv4, the internal addresses of local networks, e.g. company or government networks, have been taken from a special address range, called private addresses. These addresses can be used, but only internally, and address translation between Internet and local networks is needed. In IPv6, private addresses of that kind are no longer available. Instead, nearly all IPv6 addresses are designed as Global Unique Addresses.

Usually the public IP addresses for an institution are supplied by the network provider. When changing the network provider, also the IPv4 addresses change. With IPv4 this is not a big challenge, as only the gateway and public server addresses have to change. On the local (Intranet) side the private addresses can remain as they were.

Because IPv6 does not provide private addresses in the sense of IPv4 anymore, the IPv6 addresses (address prefix) provided by the network operator have to be used for the whole network – even for the internal addressing. This results in dependencies and inflexibility regarding the selected network provider.

With IPv6, private addresses are no longer available in a kind known in IPv4. For normal use scenario it is necessary to use Global Unique Addresses (GUA) in the local networks. These GUA addresses must be used for the connections with other private networks, too. Still, even with IPv6 it is difficult to get information on the IPv6 range of every local network connected to the whole mesh of governmental networks.

Central IPv6 addressing concept

One possible solution to the problem of central IPv6 addressing is to distribute a centrally managed IPv6 address space across all relevant governmental organizations, which then in turn are connected to one of the governmental private networks. If the central address space is divided across the different governments, it is still clear for all users that IPv6 addresses in the range of the central network prefix are part of the national government network community. This transparency provides some level of protection against misconfiguration, and in consequence data leakage or corruption.

On the technical side network routing can be applied quite straightforwardly: traffic can be directed from the local networks to every destination addressed as part of the central address space, directly by being routed into the uplink to the governmental network mesh. This simple routing provides operational security by enhanced transparency as well.

For a small country it might be possible to create an address concept without using Global Unique Addresses, too. However, this approach will fail if there are connections to other countries. Therefore, on the European level it seems without an alternative option to set up a centralized address space, at least per country. In the optimal case it is possible to cover several countries beneath one IPv6 prefix to minimize the fragmentation in network routing.

The central addressing concept under the control of a governmental LIR (Local Internet Registry) has an additional advantage: addresses do not depend on a specific network provider. This means, that the government can change its local network provider but keep its existing addresses. Institutions can continue to use these addresses with another network provider. From the perspective of the government those addresses are and stay "their personal" addresses.

How to get central IPv6 addresses

On the top level, IP resources are managed by IANA. IANA distributes the resources to the five Regional Internet Registries (RIR). The responsible RIR for Europe and Middle East is RIPE NCC in Amsterdam. From the RIRs the addresses are distributed to Local Internet Registries (LIR). As IP addresses are part of a provider network service, every network provider effectively acts as a LIR to serve his customers with IP addresses. In principle everyone can become a LIR, if they can prove a requirement for the requested address space. It is possible to establish a LIR for a group of network users, e.g. for the government institutions of a country. For administrative reasons in such a case one organization must act as representative organization to RIPE NCC and operate as LIR.

To fulfil the requirements for the requested IPv6 addresses from the RIR, the planned address use and distribution must be shown in a generic address scheme. This address scheme should be a representation of the structures, which shall use the IP addresses later. It is essential to have a well validated initial address request, as a later extension of the address space is ruled out by other policies today and one needs to stick to the planned use of the assigned addresses. Nevertheless there are first initiatives to adopt single policies to the specific requirements of LIRs without own networks for later simplification of this restriction.

For the further distribution of the addresses from the LIR to the end users, different concepts are possible. If the LIR is able to set up a significant operational structure, this can be operated centrally by the LIR. For huge structures it might be useful to set up several sub-divisions beneath the central LIR (sub LIRs) which are responsible for the operational work for a limited circle of end users. This sub-structuring has been chosen in the German government LIR, where a sub-divisioning per region has been established.

The setup of a LIR is not a short term task. An address scheme needs time to be designed and assured. Especially for governmental structures in federal constitutions it is a complex task to get a complete view on all relevant organizations and their structures.

But this complete view is necessary for the initial address space request. After receiving an assignment, additional time will be necessary to enable an organizational structure for the distribution of the addresses inside the national government. This extra timespan can easily become larger than two years. This unavoidable time to handle all the details should be taken into account whenever starting with the establishment of an – absolutely useful – central IPv6 address space.

Private addressing challenges –
IP addressing and it's analogy in legacy letter service

Let's assume IP packets are letters. If we want to address an employee of a company we address the letter with the name of the employee and the shipping address of the company's location. The public mail service will deliver the letter to the company site. There, someone from the local company staff acts as a gateway. He will take the letter and add some local delivery information, usually the room number or some department information – and based on this the letter will be finally delivered locally to the recipient. In a similar way an outgoing letter is deposited in a local outbox. The company's in-house mail service collects the letter, envelops it, stamps it and delivers it as "company letter" to the public mail service. This processing is similar to the IPv4 communication of today, where private addresses are in use. There is a public address (the companies address), which is used by the whole world as unique address and always reaches the local mail service in the company. And there is a local address of the final recipient, which is known by the gateway operator (the company's in-house mail service). But this local address (e.g. room Nr. 27) is also used in several other locations.

The IPv6 mechanism implements two changes to this "mail delivery" way. At first, it introduces an additional address line – according to the longer IPv6 addresses. This allows a more detailed addressing, containing detailed location information, also for the in-house delivery. As the public mail service now has additional information it can deliver the mail directly – or at least in a pre-sorted way, so that the local mail service only does the delivering, but no (re-)addressing takes place. This means as the second change, that there is no gateway needed anymore at the edge between private and public – so similar to the today's address translating in IP networks, that isn't needed any more where native IPv6 is used.

INTRODUCTION

In most countries, secured governmental networks are installed to establish a private communication between governmental organizations (government intranets), outside public networks such as the Internet. Nowadays, the edges of these networks are connected via Network Address Translation gateways (NATs) where IPv4 is in use.

On the other hand, IPv6 works with real end-to-end communication addresses. This means that the subnet of each connected government has to be announced in the government intranet. Due to the large number of routes, this will not be possible without proper route aggregation, especially for small governments.

If secured networks will be used in the future, it is recommended to establish a national government IPv6 addressing plan for each country (if not also on European level) to avoid scalability problems with too many small networks (and therefore too many routes). This will reduce the fragmentation of routing in the secured networks and improve operational stability and security.

As best practice the setup of a central governmental Local Internet Registry (LIR) is recommended. The LIR should be established by receiving IPv6 addresses from the Regional Internet Registry. The further assignment to the governmental organizations is then exclusively performed by this governmental LIR, and not by other LIRs / providers.

This document often makes references to governmental use cases and existing national addressing schemes. The considerations made herein are similarly valid for huge organizations or any other association of organizations that currently use private networks as the preferred communication scheme with IPv4.

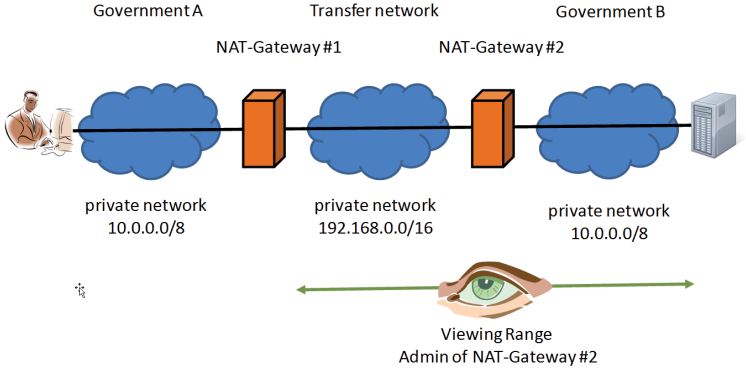
ADDRESS SPACE AND ADDRESSING

There are many stakeholders involved in IP addressing. The original idea behind the Internet protocol is to give every network node a globally unique IP address to allow end-to-end connectivity between any two nodes. Nowadays, this principle does not hold true anymore due to the global IPv4 address shortage and due to policy constraints that limit connectivity between nodes (mainly for security reasons).

Public servers and services must be reachable for all their clients. Therefore they need to have a globally valid IP address. As the number of such Internet-connected servers (and connected devices in general) increases, the number of unused IPv4 addresses diminishes. This scarcity of IPv4 addresses is the main driving factor behind the standardization and rollout of the newer IPv6 protocol.

For security reasons governments often operate well protected networks. Also the communication with other governments in most cases is based on internal networks. On a higher level special interconnection networks are established, like sTESTA on European level or national government backbones in most EU member states. So it is common sense to use protected networks for inter-government communication and to avoid the use of public networks like the Internet.

Today the governmental networks use private IP addresses in most cases. At the edge of the networks, to the Internet or to other governmental networks, a network address translation (NAT) is established. So for the IP-connection between governments over a central government backbone at least two NAT gateways will be involved.



If the infrastructure is getting more complex it might be possible that further NAT is required. In case of problems the troubleshooting is getting very difficult because no one has a view end to end of the communication line, because each network administrator only knows about the addresses directly connected to local gateway. Especially if multiple NAT instances are established, a troubleshooting process will need a step-by-step evaluation from NAT gateway to NAT gateway and in consequence take a long time.

The Internet was formally designed as an end-to-end network. Due to private addressing it was to cope with the limited IPv4 address space for a long time. Later than in marketing considerations of some vendors the NAT technology became a security feature due to the fact that someone can 'hide' a real endpoint address behind a NAT gateway. As a consequence of the complex nature of the NAT definitions the relevant configurations are always a source of mistakes and confusion. So in real networks most of the time NAT is more a bane than a boon – for the administrators and finally for the users, affected by non-operational IP connections.

With IPv6 the Internet should be lead back to the former idea of an end-to-end connectivity. Therefore in IPv6 NAT is not established. For all IPv6 communication it is assumed that real end-to-end connectivity is made available. Security can be reached by serious firewall and application level gateway administration, as in IPv4.

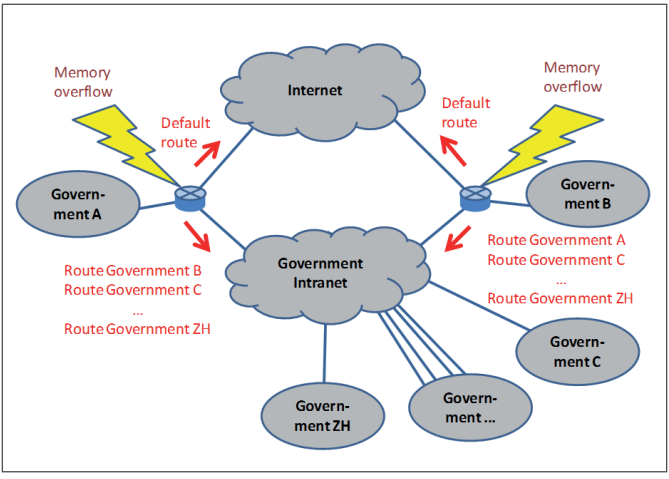
Having NAT technology not available has strong consequences for all government networks. Governments today never work on a network-island but have several IP connections to other governments. So it is usual that a government holds several dedicated links to other governments. By setting up NAT infrastructure at the networks interface the (internal) addressing can at both sites can stick to the existing local IP address space – but with the price of administrative effort for the NAT-gateway.

Considering the same situation based on IPv6 – without NAT - the final endpoint address at the remote site can – and must - be addressed directly. Unlike today it is not enough to know the address at the next NAT gateway, which is typically part of the own network. In consequence all remote connected networks must be recognized for routing with their destination IP addresses. So the remote address ranges must be available as routing entry at the local network edge routers.

DEDICATED ROUTING OF PRIVATE NETWORKS

For security reasons many countries established closed networks for a protected communication between national governments. These networks use special security and encryption to keep the communication private. Examples are RedSARA in Spain or the DOI in Germany or sTESTA at European level. These networks act as a kind of government intranet. Sensible information and applications are forced only to use this secure infrastructure.

Nowadays a NAT gateway is located at the edge of the networks. A governmental operator does not care which IP addresses are used at the other end of the communication, because it is hidden by NAT. Using IPv6 changes conditions on an essential level: every single network connected to the government intranet must be known by each connected partner. This is mandatory to secure a dedicated routing to a remote site using the secured government networks.

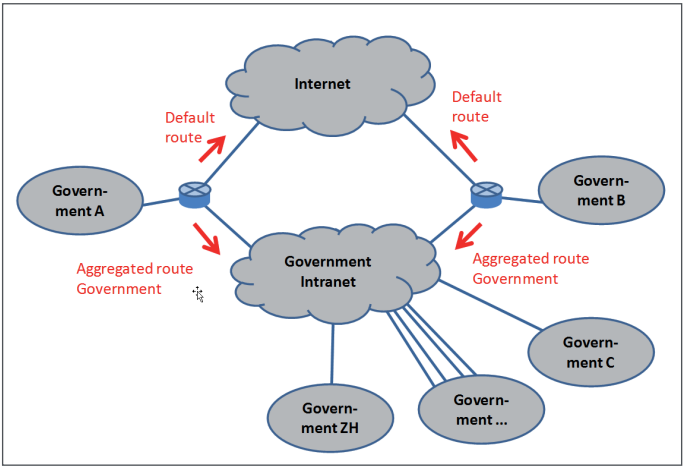


If every government receives its own IPv6 space from a local Internet registry the routing table will expand heavily in a short time. This results in huge routing tables, requiring high performance components at each network access point. The expected number of changes in the routing could not be handled in existing structures. Therefore, dynamic routing must be established. Today's encryption gateways do not support such a number of routes, because each route is established as an own security association between gateways. Furthermore, for security reasons today's encryption gateways do not support dynamic routing.

For inter-government communication each routing instance in networks on an communication path requires to know each route to each destination reached using this governmental intranet. These components have high memory requirements for their routing table and are very expensive. Alternatively, only selected routes can be administered, causing loss of communication and additional effort in administration.

Even if this technical restriction can be solved, the network will get overloaded with routing information. This loss of transparency reduces security and opens potential to new attack methods. An easy solution for this situation can be achieved by using a homogenous address space for all governments connected to the government intranet. In this way, only one single route has to be published from an edge router of the governmental intranet to the connected local network. Also the routing in the local networks is very easy, as there is only one global route to be set in the direction to the intranet gateway. Routing hence becomes very easy and transparent, and can be established in static routing tables, like in IPv4.

This concept works also at the European level, as long as all member states use one IPv6 address space which can be aggregated by one prefix for the governmental organizations in their country. In this case one more route entry for each member state has to be configured, but the number of networks stays manageable.



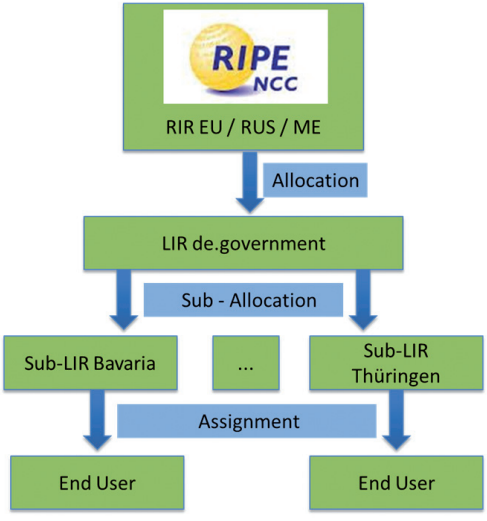
These considerations forced the national government of Germany and Spain to request one central address space in IPv6 at RIPE NCC. In Germany this address space has been assigned in 2009. The Spain inquiry is still in progress.

GOVERNMENTAL IP ADDRESS PLANNING

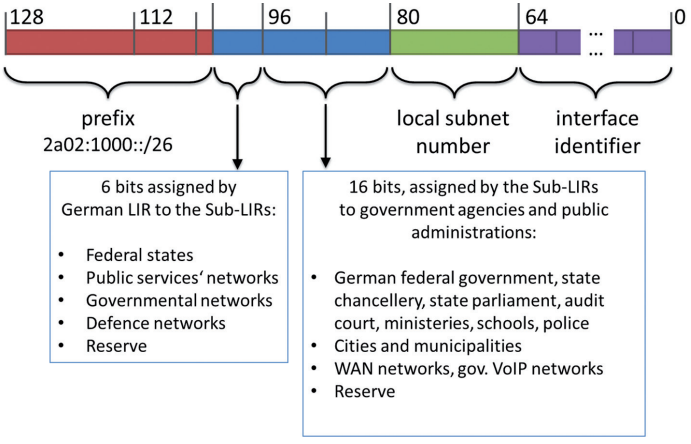
As mentioned previously, Local Internet Registries (LIRs) manage the domestic allocation of IP address ranges to Sub-LIRs and/or commercial users of these addresses. However, a country may want to use a separate address space for governmental use only. This allows for an overall simplified IP address structure across governmental institutions such as ministries, municipal services, schools, police etc. In effect, this approach allows for simpler, easily verifiable access permissions and routing structures, compared to the current situation where each local entity organises an IP address space for their local use in a way independent from the domestic Internet providers and their local availability.

For a central management of domestically used governmental IP addresses, an institution of that country needs to become a LIR, registered with the RIPE NCC (see figure below). This way has been chosen e.g. in Spain and in Germany in 2009. In case of Germany a central LIR called „de.government" has been set up.

The RIPE NCC, the European RIR, will grant an IPv6 prefix up to a /29 for such purposes without the need for an extensive justification. Only for a larger address space, i.e. a shorter prefix, an extended justification is mandatory.



As noted before, in Germany the LIR de.government plus a set of Sub-LIRs were founded. Upon extensive request, the RIPE NCC allocated one /26 prefix for use by de.government. Based on this prefix, the LIR takes care of the (top level) management of the IPv6 addresses for the public administrations in Germany. A domestic address plan determines the use of the next six bits, after the /26 prefix. This way, one or more /32 prefixes are allocated to sub-LIRs as the basis for /48 site prefixes they hand out on request to their customers. This split shown in the next figure:



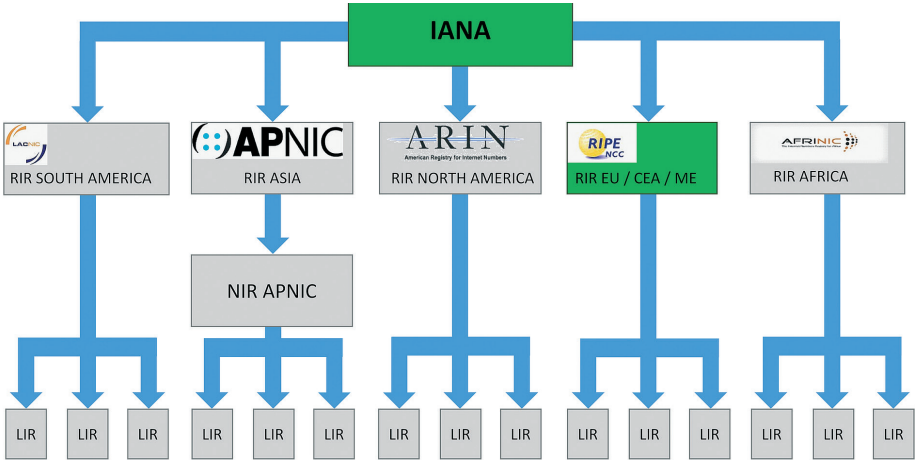
With such an IPv6 address assignment, 6 + 16 = 22 bits are determined by the LIR and Sub-LIR (blue parts in the figure above), and each customer can assign another 16 bits (the green part) to structure their local IPv6 addres space into local IPv6 subnets, as we described before.

The following picture shows partially the assignment of addresses from the LIR de.government to the Sub-LIRs of some states in Germany. As you will recognize there is one /32 as reserve between each state, so another block can be assigned. This ensures a contiguous address space, which can be aggregated for routing and also keeps rules for packet filter small and simple.

Präfix: 2a02:1000 /26			Regional Bits:	6			
Block	**Nr.**	**Dual**	**Präfix**	**Block**	**Nr.**	**Dual**	**Präfix**
00: Hamburg	0	000000	2a02:1000 /32	08: Niedersachsen	8	001000	2a02:1008 /32
01: Reserve	1	000001	2a02:1001 /32	09: Reserve	9	001001	2a02:1009 /32
02: Schleswig Holstein	2	000010	2a02:1002 /32	10: Reserve	10	001010	2a02:100a /32
03: Reserve	3	000011	2a02:1003 /32	11: Reserve	11	001011	2a02:100b /32
04: Bremen	4	000100	2a02:1004 /32	12: NRW Land	12	001100	2a02:100c /32
05: Reserve	5	000101	2a02:1005 /32	13: Reserve	13	001101	2a02:100d /32
06: Mecklenburg-Vorpommern	6	000110	2a02:1006 /32	14: NRW Kommunen	14	001110	2a02:100e /32
07: Reserve	7	000111	2a02:1007 /32	15: Reserve	15	001111	2a02:100f /32

HOW TO OBTAIN (A BLOCK OF) IPV6 ADDRESSES

The Internet Assigned Numbers Authority (IANA) manages the global IP address space on the top level. On request, it allocates IP (version 4 and version 6) address blocks in large chunks to the five major Regional Internet Registries (RIRs, see the following figure). The RIRs further subdivide these address blocks and distribute the smaller address ranges to Local Internet Registries (LIRs). The following figure exemplarily shows three LIRs per RIR, but many more do exist. Finally, these LIRs can be contacted by domestic entities in need of public IP addresses for their own, local private or public use. To obtain address space in Europe - please contact the RIPE NCC.



ALTERNATIVES, YOU MAY CONSIDER

End to End security over public networks

The requirement of an aggregatable address space for each country government is based on the existing internal networks. These networks are a fact nowadays and within for the near future. Thinking ahead, it might be possible to avoid such closed networks. This could be possible by establishing a consequent application security. Also the move from today's special encryption gateways to standard business encryption could reduce this requirement. Considering the recent findings in wiretapping in the Internet but also in sensible protected infrastructures, the opposite evolution will take place and the use of closed networks and encryption level will increase.

Use of Unique Local Addresses

With unique local addresses (ULA), a kind of private addresses exists in IPv6. In fact ULA are not the same and not for the same use than private addresses in IPv4. The ULA address space covers a subnet of /7. The non-collision idea in ULA bases on random choice of (small) networks for the users. Addressing all national governmental organizations of a country by randomly choosing the ULA is not an approach we recommend. We suggest the address space to be planned. Considering further that Germany received a /26 for their national governments and Spain is working on an subnet of the same size for the Spanish governments, it becomes clear that such an addressing concept will not work European-wide, when end-to-end communication over protected service networks and within unique addresses also must be enabled between member states. In that case, for each state a subnet of the ULA address space has to be assigned and has to be made obligatory in order to make communication possible over the secured networks. So an ULA addressing is expected as being nearly impossible on scaled levels.

SUMMARY

If there are private/protected networks in use among different governmental organizations IPv6 addressing must be harmonized across all the different governmental organisations that are connected together by these networks. This is only possible with officially acquired Global Unique IPv6 Addresses. To avoid frayed routing as a consequence of several small subnets claimed to the different governmental sites that are connected to the network, GEN6 recommends a central addressing scheme.

In addition, IPv6 addresses are maintained by a governmental LIR that is independent from the network operator. This LIR provides the addresses without a dependency to a local network operator. As this LIR is set up for the long term, and so is the address allocation to the local government organization, the IPv6 addresses can be used like provider independent addresses – although technically they are of the provider-aggregated type, in the sense of the RIPE policies.

Setting up a central address space needs some preliminary actions to consolidate the requirements and design an adequate address scheme. Also, an organization for the addressing handling in the LIR itself and its sub structures must be established. Experiences from other countries show that this task can easily take two or more years. Activities for a setup of a central address space therefore should start with enough reserve time to the point where the addresses are really needed in operation.

DISCLAIMER

This booklet was created by

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
Martin Krengel (Citkomm, Germany)
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

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