GOVERNMENTS ENABLED WITH IPv6
GEN6

IPv6 APPLICATION IN THE ROAD DOMAIN

This project has received
funding from the
European Union´s

European
Commission

INTRODUCTION

Cooperative services in vehicular scenarios are becoming essential for the future connected vehicle within the ITS (Intelligent Transportation Systems) research field. They are supposed to decrease road fatalities, improve the capacity of roads, diminish the carbon footprint of road transport and enhance the user experience during travels. Although there are many vehicular services envisioned for the short, medium and long term, these are usually categorized in the next groups [1,2]:

- Safety. These services are intended to reduce accidents and safeguard vehicle occupants and pedestrians lives. Some examples are collision avoidance, accident notification or emergency vehicle approaching.
- Traffic efficiency. In this group there are services that improve the road network capacity and reduce the travel time. Some examples are variable speed limit, dynamic management of road intersections or congestion detection and mitigation.
- Infotainment. Mainly oriented to provide value-added comfort services, Internet access and multimedia. Some examples are context-aware touristic guidance, video under demand and video conferencing.

For supporting this diversity of services it is clear that quite generic network architecture is needed that also assures the future compatibility among different providers. Due to this, during the last year there has been an intense work on standardization activities regarding cooperative ITS. First, the ISO TC 204 released the Communications Access for Land Mobiles (CALM) concept [3], but the later created group ETSI TC ITS improved CALM based on the results of the COMeSafety European project through the European ITS communication architecture [4]. The last update of this common ISO/ETSI effort has been recently provided by ISO, as can be seen in [3]. The architecture of the current European ITS communication stack, showed in Figure 1, should be instantiated totally or partially on vehicles, nomadic devices, roadside units and central points.

As observed, two management and security planes surround four horizontal layers based on the well-known OSI communication stack.

A key advantage of this architecture is the possibility to use multiple communication technologies, being the upper layers in charge of hiding the access management to the final applications. At the moment, the definition of the four horizontal planes is quite advanced, while management and security require further efforts in the next years. Nevertheless a controversy remains about the protocols to be used mainly in the networking layer. There are two main families of protocols currently adopted by standardization bodies (and the academia):
specific ITS protocols based on GeoNetworking [5], which is a multihop routing protocol oriented to the geo-dissemination of information in vehicular environments; and Internet Protocol version 6 (IPv6) technologies [6], based on the evolution of well-known Internet protocols defined within the Internet Engineering Task Force (IETF).

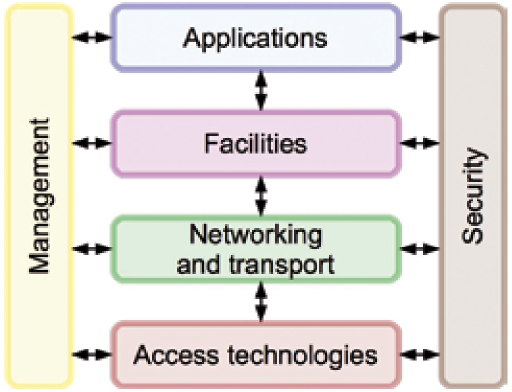


FIGURE 1/ REFERENCE ITS COMMUNICATION ARCHITECTURE

Although GeoNetworking offers more adapted functionalities for supporting vehicular communications, such as native geographical distribution or low packet overhead, IPv6 offers a more interoperable solution with the rest of the (future) Internet, supporting in a better way concepts such as Internet of Things (IoT) or Smart Cities, among others. Moreover, a number of well-known IETF protocols could be added for providing extra security, multicast, multi-homing, etc. The rest of this document follows this line, which is also justified by the ITSSv6 European project [7], and defends the application of IPv6-based technologies in the ITS segment.

IP PROTOCOL EVOLUTION

The first widely deployed protocol allowing packet-based communications between computers located in various networks was the Internet Protocol version 4 (IPv4). This protocol defines addresses of a fixed 32-bit length. This allows approximately 4 billions IP addresses to be used on the Internet. This figure appeared sufficient for the expected use of the protocol at that time, but the emergence of the commercial use of the Internet in the 90's decade led to an exponential use of IP addresses. To prevent the shortage of IP addresses, the IETF decided two measures: the specification of private IPv4 address spaces [8], to be used with Network Address Translation (NAT) [9], and the design of a new version of the IP protocol: IP version 6 (IPv6) [6].

The specification of this new protocol was finalized in 1998, defining addresses of a fixed 128-bit length. This allows a very large address space that is considered sufficient for most ambitious deployment scenarios (there would be enough addresses to identify every grain of sand on Earth). In addition to the address space, IPv6 defines new protocols to ease the management of the layer-3 protocol stack, such as Neighbor Discovery [10] that allows auto-configuration of IPv6 addresses.

While IPv6 is entering in its deployment phase, the depletion of the IPv4 address space is on-going, despite the measures taken by the IETF. The global IPv4 address pool is exhausted since February 2011 and several regions such as Asia and Europe are facing shortage of IPv4 addresses. The exhaustion for the European region finally happened on 14th September. Since then, Internet Service Providers (ISPs) and hosting services are not able to get new IPv4 addresses. The deployment of IPv6 is therefore critical to ensure the future growth of the services of these stakeholders.

To this date, IPv6 deployment is on-going in most network backbones. All major operating systems (Windows, Linux, BSD variants, Mac OS X, Android, iOS), most network equipment and services (routers, DNS, etc.) can support IPv6. However, there are still few ISPs (Internet Service Providers) in Europe offering IPv6 and support of IPv6 in applications (web and email servers, etc) is still lacking, although those issues are of limited importance in vertical segments such as ITS. It must nevertheless be acknowledged that IPv6 deployment is taking momentum and that soon IPv6 will become the rule rather than the exception. Certainly, the expansion rate of IPv6 is not fast enough, but the depletion of the IPv4 address space is now going to boost it.

IPv6 IN ITS

By the time ITS services requiring the use of the public IP addresses appear on the market, there will not be enough public IPv4 address available. The use of IPv6 scales to meet the addressing needs of a growing number of vehicles and connected devices, and provides the added functionality necessary in mobile environments. By relying on IPv6 in their ITS communication architectures, ISO followed by ETSI, COMeSafety and the Car-to-Car Communication Consortium have thus taken the right decision to guarantee sustainable deployment of cooperative ITS.

In their common answer to the ITS standardization mandate M/453 from the European Commission, CEN TC 278 and ETSI TC ITS lists a number of items for which IPv6-related standards are needed while the European Commission's standardization work programme includes actions turning around IPv6, given the fast coming ultimate depletion of the IPv4 address space and a number of alerting reports published in 2008, including one from the OECD [11].In its IPv6 Action Plan, the European Commission (DG INFSO) set an objective of a penetration rate of 25% of European Internet users and servers able to use IPv6 by 2010. This target is followed by some European nations.

Furthermore, IPv6 has the potential to decrease accident rates by enabling transmission of safety critical information. This document is not envisaged to demonstrate that this would be the case for the time critical type of applications, since the automotive industry and the SDOs (at this time) are not considering IPv6 for fast V2V communications. However, it is simple to note that not all data is time critical. There is no question that IPv6 could be a media-agnostic carrier of such non-time critical but safety essential information. Once the safety benefit of IPv6 is acknowledged, there are classical ways of calculating the economic impact of reducing road fatalities. E.g. the Safety Forum 2003 Summary Report estimated the cost of accidents at 160 billions euros.

A 1% reduction would reduce these costs by 1.6 billion euros annually. And of course, this does not take into account the reduction of pain and suffering experienced bysurviving family members and friends of accident victims that may not be adequately reflected in the method used to estimate the economic costs of traffic fatalities. As said, one of the main reason why Internet Protocol version 6 (IPv6) appeared was the depletion of IPv4 addresses, however, there are lots of extra technical advantages that also cover important needs in cooperative vehicular communications:

- IPv6 defines addresses of a fixed 128-bit length. This allows a very large address space that is considered sufficient for most ambitious deployment scenarios such as the vehicular one, where a number of vehicles and on-board devices should be addressed.

- Makes easier the integration of mobile IP technologies, such as Network Mobility basic support (NEMO) [12], maintaining Internet connectivity upon the change of point of attachment.

- Provides node auto configuration (IPv6 Stateless Address Autoconfiguration [13]), which is useful for nomadic devices entering the vehicle.

- Integrates security mechanisms. Now Internet Protocol security (IPsec) [14] is integrated in IPv6, and Internet Key Exchange version 2 (IKEv2) [15] can be used to establish security associations between network nodes.

- Manages multi-homed nodes, which are provided with more than one point of attachment to the network, through the use of Mulple Care of Addresses [16].

At the moment, current standards in ITS cooperative systems consider IPv6 communications. The most relevant document comes from ISO in [16], where network mobility concepts are integrated in the reference CALM architecture. However, the IPv6 support is being further defined among the different layers of the reference communication stack in areas such as flow management and security.

PARTICULAR STUDY CASES

A set of particular scenarios where IPv6 outperforms IPv4 and/or other protocol solutions are included in this section to justify the adoption of this protocol in ITS.

INTERNET ACCESS

A common service in vehicular environments is the Internet access from in-vehicle devices. In this scenario an on-board device installed in the dashboard, a laptop, or any other mobile device carried by a user, requires Internet access. Although this service could be directly provided through IPv4 using 3G, this is not a cost-effective and scalable way of accessing Internet in the next situations (at least):

1. High data volumes must be exchanged, such as file down loading or high definition multimedia content.
2. High-delay requirements are applicable by a particular application, such as the speedy reception of an alert in a particular road stretch.
3. More than one in-vehicle device wanting to access Internet at the same time. This case receives particular attention in public transport means, such as buses or trains.
4. Different access networks should be accessed due to 3G coverage gaps or crowded areas.

In this scenario, the usage of IPv6 technologies can provide further benefits to both drivers and passengers. The NEMO technology can support the seamless mobility of a mobile router providing Internet access to multiple in-vehicles devices. This case is depicted in Figure 2. Providing, for instance, a WiFi access to this mobile router, smartphones, tablets, laptops and the rest of networked vehicular devices can access to the Internet. A mobile router would be in charge selecting the most appropriate communication technology. Not only 3G, but also vehicular WiFi (i.e. IEEE 802.11p or ETSI G5) or WiMax could be also used when required and available to better support the requirements of applications and offload the 3G networks. Cost benefits are obvious.

VEHICLE-TO-VEHICLE INFOTAINMENT

Some services require communication between vehicles, such as messaging, route information exchange or audio conference. When IPv4 is used (usually through a 3G connection), these services must deal with:

1. NAT issues, since the configured IPv4 address could be a private address within the vehicle domain.
2. Always it is needed a backbone support for allowing the P2P communication, due to the lack of direct IP routes between end devices.
3. Performance and costs issues previously showed, derived from the 3G access.

IPv6 and the multiple communication technologies that could be transparently provided to in-vehicle devices through NEMO solve the previous problems. First, IPv6 auto configuration together with prefix delegation protocols can provide a global IPv6 address to each in-vehicle node NAT will be never necessary. In this way, real P2P communication can be provided for communicating application end-points in vehicles. As *Figure 2* shows, an indirect communication between vehicles can be established through Internet, by using the NEMO technology, or directly by using the Internal Network Prefix Discovery (INPD) protocol (formerly called Mobile Network Prefix Provisioning – MNPP) [18]. In this last case, INPD enables the exchange of IPv6 routing information among nodes in a vehicular ad-hoc nework (VANET) using direct wireless links. Since vehicles are provided with in-vehicle IPv6 prefixes, these could be shared with other vehicles to allow the direct communication.

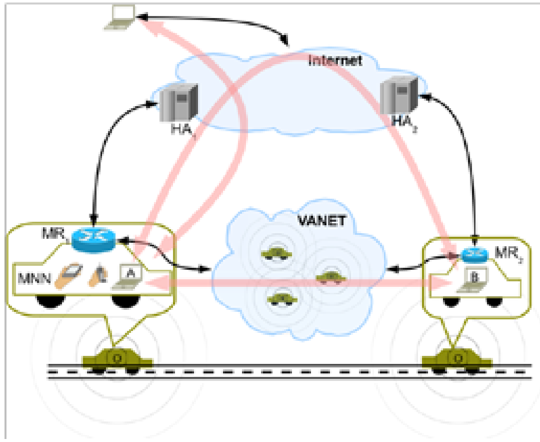


FIGURE 2
MOBILITY SCENARIOS

TRAFFIC EFFICIENCY SERVICES

Vehicular networks provided with IPv6 can further support traffic efficiency services such as congestion detection, management and notification, route planning, variable speed limit or road tolling, for instance. Most of these services require a vehicle-to-infrastructure communication link that could suffer from next problems when common IPv4 networks are used:

1. Lack of mobile network access within 3G coverage gaps.
2. Connectivity problems in congested road segments due to a limited 3G coverage.
3. Lack of localized notifications according to the road segment. A proper and individualized treatment of vehicles would be needed to provide such information
4. Lack of interoperability with Internet-based services; for example, when using non-IP communication protocols are used at the roads ide (i.e. proprietary communications with road devices or specific ITS protocols for communicating with vehicles).

Apart from the advantages previously described of NEMO, which are also applicable in this kind of scenarios, IPv6 multicast can provide further advantages for distributing information among in-vehicle devices coming from the infrastructure. Novel dissemination strategies can be envisaged also taking into account a mapping between the geographical position of devices and the IPv6 address temporarily assigned. Thanks to the number of available IPv6 addresses, the same group of in-vehicle devices could be provided with a different IPv6 addressing according to the current location.

Moreover, given the globally usage of IP technologies on the Internet, remote service points within the Internet could be directly accessed without any protocol translation or adaptation from vehicle nodes or road infrastructure devices such as variable message signs. Only if needed, and during the transition period from IPv4 and IPv6, there are standardized solutions such as NAT64 [19] that can support the access to IPv4-addressed services from an IPv6-based vehicular network.

SAFETY SERVICES

IPv6 can support many safety services such as crash notification, metrological alerts, road infrastructure alerts, and vehicle monitoring or emergency calls, among others. However, by using IPv4 or current deployments, the next limitations are found:

1. Relaying only on 3G networks could be a problem nowadays at some mountain and remote locations.

2. VANET solutions do not warrantee by their own the operation of safety services due to, above all, the expected low penetration of equipment (even in the long-term) and the availability of the wireless medium when many vehicles are in the surroundings.

3. IPv4 addressing does not allow the direct access to vehicle devices in potential IoT scenarios.

4. Solutions exclusively based on wide-area wireless technologies such as 3G do not warrantee that all vehicles within geographical areas are aware of notifications, due to possible availability problems.

The possibility of supporting different communication technologies managed by the IPv6 network layer (sing NEMO) can solve availability problems, as said, but also the overall performance of the communication could be improved, and not only because of WLAN network attachment points can be also used transparently. The MCoA technology can support more than one active communication flow between vehicles and infrastructure. In this way, the reception of a critical alert could be further guaranteed by transmitting it through more than one path, and more complex flow management techniques could be applied depending on the data traffic.

Moreover, IPv6 addressing and auto configuration capabilities can support the installation of directly accessible IPv6 devices in the vehicle body. Following this approach, or even providing IPv6 gateways when necessary, advanced infrastructure services could be envisaged to monitor the vehicle status, such as the engine operation, the oil level and quality, the tires pressure, etc.

SECURED SERVICES

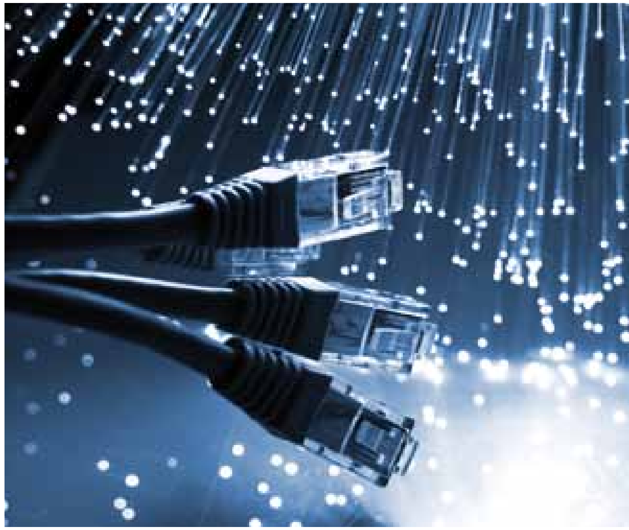
It would not be the first time communication security is not considered in a networked field at the design stages, but we are still in the momentum of ITS deployment. It is the time for integrating security features in vehicular communication from scratch. IPv4 does not conceive security in its own protocol design, unlike IPv6, which integrates IPsec and IKE as essential parts in its operation. Other protocols especially oriented to the ITS field try to re-invent the wheel with new security schemes (as happens in GeoNetworking), but interoperation is still not guaranteed and IETF has already worked on security issues for a long time, finally integrating the required protocols within the IPv6 protocol family.

Most of the future vehicular services, and even some of the currently available, such as fleet management systems, will need a means to guarantee the confidentiality of the data transmitted, the authenticity of the messages and the integrity of the payload. Services involving the user safety will require a special attention regarding these issues.

IPv6 provides IPsec, which can provide security tunnels between pairs of IPv6 nodes, guaranteeing confidentiality and integrity of the data transmitted. These tunnels can be even negotiated on real-time and transparently by using IKEv2. In fact, following the NEMO model showed in Figure 2, the local mobile router installed in the car could provide most of the security features, unloading mobile devices of performing cryptographic tasks, for instance.

NETWORK ACCESS

Managing the nodes entering in a network is both a security and a business model issue. This is of particular important in vehicular networks, where vehicles nodes should be granted to access the ITS network through a set of possible communication technologies. Current models based on 3G communication gives the telecomm operator all the responsibility, but when more than one communication technology is provided, an integrated network access scheme for ITS is found essential.



In general, the network access could be seen from the perspective of accessing to different services. Even Internet could be seen as a service. And in this context, a road management entity (for instance, a road operator) would require the necessary mechanisms for authorizing vehicles and/or users for accessing to certain services. For this reason network authentication, authorization and accounting (AAA) measures will be essential in future ITS cooperative services. IPv6 offers the necessary support for that, and protocols such as EAP [20] and PANA [21] could be transported over IPv6 for enabling AAA designs. It is important to also know that overlay schemes will be needed to deal with the issue that some communication technologies provide “layer-two” AAA features, such as WiFi or 3G, but others do not, such as IEEE 802.11p/ETSI G5. In this frame, interoperable IPv6-based networks will be the cornerstone.

TECHNOLOGICAL REVIEW

A brief review about the most interesting IPv6-based technologies applied in the ITS section are included in this part of the document.

NEMO

Network Mobility Basic Support (NEMO) [12] allows terminals within a mobile network to be globally connected to the Internet. Mobility capabilities are distributed between the Mobile Router (MR) and the Home Agent (HA) entities, in order to maintain the IPv6 addressing for the mobile network.

An unchangeable IPv6 Mobile Network Prefix (MNP) is delegated by the home network to MR for assigning addresses to the Mobile Network Nodes (MNN). Following the NEMO model, upon the reception of a Router Advertisement (RA) message from an Access Router (AR), the MR is aware of the existence of a new network. In this case, the MR, which already has a fixed IPv6 address within its home network (Home Address or HoA), generates a new auto configured IPv6 address within the new visited network. This address is called Care-of address (CoA), and it is immediately notified to HA. This notification is performed by the MR through a binding update message, which is acknowledged with a binding ACK sent by HA.

Only MR and HA are aware of the network change, since MNNs continue connected with MR using the same address. Hence, when any computer outside the home network (Correspondent Node or CN) communicates with any of the hosts connected in the vehicle, it uses the home address as destination and, hence, packets follow the route towards the home network.

As can be noted, HA redirects these IPv6 packets to the current IPv6 CoA of MR, which finally distributes the packets within the mobile network. In the same way, when packets are sent from any MNN to a CN, they are routed by MR towards the HA, which forwards them to the destination. Hence, HA and MR perform an IPv6 into IPv6 encapsulation to create a mobility tunnel. This model has a direct application in vehicular communications, where the in-vehicle network connecting nomadic devices maintains its connectivity though an on-board MR and a remote HA hosted by a network mobility management entity (e.g. the road operator).

MCOA

MRs can be provided with multiple network interfaces such as IEEE 802.11a/b/g, IEEE 802.11p, WiMAX or UMTS, for instance. When a MR maintains these interfaces simultaneously up and has multiple paths to the Internet, it is said to be multihomed. In mobile environments, multihoming capabilities can alleviate problems suffered by MRs such as scarce bandwidth, frequent link failures and limited coverage.

The possible configurations offered by NEMO when multihoming is used are classified according to the number of MRs in the mobile network, the number of HAs serving the mobile network and the number of mobile network prefixes advertised in the mobile network. NEMO Basic Support has a single MR, single HA and single MNP. In this configuration, a tunnel is established between the HA address and the CoA of the MR, even if the MR is equipped with several interfaces. Multiple Care of Addresses Registration (MCoA) [16] is thus proposed as an extension of both Mobile IPv6 and NEMO Basic Support to establish multiple tunnels between MR and HA.

Each tunnel is distinguished by its Binding Identification number (BID). In other words, NEMO Basic Support deals with interface switching at network layer, while MCoA supports simultaneous use of multiple interfaces, and this capability is especially useful in vehicular communications, where a continuous UMTS connectivity could be complemented, for instance, with an intermittent 802.11p channel.

IPSEC AND IKEV2

The IP Security (IPSec) protocol is an enhancement to the basic IP protocol that defines a set of security services for protecting IP traffic. Since it is defined at IP level, the security protection is transparent to other protocols carried over IP. The IPsec packet protection to IP packets can be applied through two security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). While the former provides authentication and integrity protection to the IP packet, the latter also provides confidentiality to the data transport within the IP packet.

These protocols can be applied in two different operation modes. In transport mode, the security services are applied to next layer protocols, i.e., the information carried within the IP packet. Conversely, in tunnel mode, the protection is applied to the whole IP packet, which is sent through a tunnel. The IPSec operation relies on the fundamental concept of Security Association (SA). A SA conceptually represents a unidirectional connection between two entities which implements certain security services through either AH or ESP protocol.

The establishment of an SA implies the negotiation of a set of security parameters such as cryptographic algorithms or key material that is used by the AH or ESP protocols. In particular, IKEv2 has been designed to provide such functionality. IKEv2 is a request/response protocol between two entities referred to as initiator and responder. It is executed at application layer and transported in UDP packets. While the initiator starts the execution, the responder acts as server during the negotiation. Security policies determine which traffic must be protected and, hence, the SAs to be created.

REFERENCES

[1] Y. Khaled, M. Tsukada, J. Santa, J. Choi, and T. Ernst, "A usage oriented analysis of vehicular networks: from technologies to applications," Journal of Communications, vol. 4, no. 5, 2009.

[2] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," ETSI TR 102 638, European Telecommunications Standards Institute, Jun. 2009.

[3] International Organization for Standardization, "Intelligent transport systems - Communications Access for Land Mobiles (CALM) - Architecture," ISO 21217, International Organization for Standardization, Ap. 2013.

[4] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Communications Architecture," ETSI EN 302 665, European Telecommunications Standards Institute, Sep. 2010.

[5] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture," ETSI TS 102 636-3, European Telecommunications Standards Institute, Mar. 2010.

[6] S. Deering, and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Dec. 1998.

[7] T. Ernst, J-H Lee, J. Santa, F. Pereñiguez, A.F. Skarmeta, "D2.1 Preliminary System Recommendations," ITSSv6 deliverable D2.1, May 2012.

[8] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear, "Address Allocation for Private Internets," RFC 1918, Feb. 1996.

[9] K. Egevang, and P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, May 1994.

[10] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861, Sep. 2007.

[11] The Organization for Economic Co-operation and Development (OECD), "Internet Addressing: measuring deployment of IPv6," Apr. 2010.

[12] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," RFC 3963, Jan. 2005.

[13] S. Thomson, T. Narten, T. Jinmei, "IPv6 Stateless Address Autoconfiguration," RFC 2462, Sep. 2007.

[14] S. Kent, K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, Dec. 2005.

[15] S. Frankel, and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," RFC 6071, Feb. 2011.

[16] R. Wakikawa, T. Ernst, K. Nagami, and V. Devarapalli, "Multiple Care-of Addresses Registration," RFC 6089, Jan. 2008.

[17] International Organization for Standardization, "Intelligent transport systems – Communications Access for Land Mobiles (CALM) – IPv6 Networking", ISO 21210:2012, Jun. 2012.

[18] J.-H. Lee, M. Tsukada, and T. Ernst, "Mobile Network Prefix Provisioning," Internet Draft, Oct. 2009.

[19] M. Bagnulo, P. Matthews, and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers," RFC 6146, Apr. 2011.

[20] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, Jun. 2004.

[21] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)," RFC 5191, May 2008.

This booklet is powered by UNIVERSIDAD DE MURCIA

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:
Antonio F. Skarmeta, Pedro M. Ruiz, Jose Santa Lozano and Alejandro Perez

Contact:

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

GOVERNMENTS ENABLED WITH IPv6
GEN6

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

- 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

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