www.euro6ix.net

Title:	Document Version:
Deliverable D4.2 **Privacy and Civil Liberty Concerns in Relation to IPv6**	3.6

Project Number:	Project Acronym:	Project Title:
IST-2001-32161	Euro6IX	European IPv6 Internet Exchanges Backbone

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
30/06/2003	30/06/2003	R – PU

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author:	Organization:	Contributing WP:
Kaisor Basar	E&A	WP4

Authors (organizations):

Jordi Palet (Consulintel).

Abstract:

This is the first legal deliverable which examines the legal implications of IPv6 on privacy and civil liberty, a crucial issue which needs to be dealt with comprehensively in order that privacy concerns do not create an obstacle to the widespread implementation of IPv6 in Europe. In particular we focus on the issue of whether the use of unique identifiers in some types of IPv6 addresses are as potentially dangerous to privacy as some commentators suggest or whether this issue has been dealt with in a satisfactory manner within the IPv6 design.

The deliverable sets out the European legislative background to privacy (and data protection) and puts the IPv6 privacy issue into perspective against this background providing answers to the questions above.

Keywords:

Addressing, Article 29 Data Protection Working Party, Data Protection, European IPv6 Internet Task Force, Fundamental Freedoms, Human Rights, Privacy, RFC3041, Stateless Address Autoconfiguration, Unique Identifier.

Revision History

The following table describes the main changes done in the document since its creation.

Revision	Date	Description	Author (Organization)
v1.0	07/04/2003	First draft to include Index and Chapters 1 and 2	Kaisor Basar (E&A)
v2.0	24/05/2003	Second draft to include legislation	Kaisor Basar (E&A)
v3.0	30/05/2003	Third draft	Kaisor Basar (E&A)
v3.1	01/06/2003	General review, naming and template update. Correction on several IPv6 technical aspects. Table of figures and figures.	Jordi Palet (Consulintel)
v3.2	10/06/2003	General review and minor amendments prior to Aveiro meeting	Kaisor Basar (E&A)
v3.3	16/06/2003	Amendments and conclusions	Kaisor Basar (E&A)
v3.4	27/06/2003	Final revision	Kaisor Basar (E&A)
v3.5	30/06/2003	Final Review and minor changes	Jordi Palet (Consulintel)
v3.6	03/07/2003	Small mistake corrected	Jordi Palet (Consulintel)

Executive Summary

The privacy concerns about IPv6 centre on the use of unique identifiers in a certain type of IPv6 address. Some argue that this will leave a digital fingerprint every time someone enters the web allowing detailed automated profiling of an individual. This issue was first raised in the US at the end of the 90's where stories began to appear that IPv6 was bad for privacy. The debate has now moved across to Europe where concerns have been raised by an official publication of the Article 29 Data Protection Working Party, an independent advisory body on data protection and privacy established under the first Data Protection Directive (95/46/EC) ("Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipment: The example of IPv6 adopted on 30th May 2002").

Also prior to this Article 29 Opinion, another EU body, the Commission to the Council and the European Parliament published a paper in February 2002 entitled "Next Generation Internet – priorities for action in migrating to the new Internet Protocol IPv6" which set out a list of issues to be dealt with to assist the successful deployment of IPv6 in Europe. One of the specific tasks called for was an extensive study into any privacy issues raised by the new Protocol.

One of the tasks of the Euro6IX project is to undertake such an extensive study in order to deal with the potential privacy issues in IPv6 and specifically in this first deliverable we confront the issue concerning the use of unique identifiers raised in the Article 29 Data Protection Opinion. We have analyzed the issues against the background and development of European privacy and data protection laws to identify what are the privacy obligations for the designers of the new Protocol and whether they have fulfilled these obligations particularly in respect of addressing.

This is the first of three deliverables due from Euro6IX dealing with the legal aspects of IPv6. The second deliverable due in December 2003 will concentrate on the data protection legislation in more detail (rather than the general concept of privacy) and the final paper in October 2004 will deal with a various issues such as IPsec and IPRs (Intellectual Property Rights).

Table of Contents

Table of Figures

1. INTRODUCTION

The Internet is an area which some argue has caught legislators off-guard. First the debate about the manner and extent of regulation for an open network is still unresolved. Secondly, the issues raised in a fast evolving technological field do not always neatly fit into current legal concepts or legislation. Just as one set of problems is dealt with, it seems that a host of new ones arise. Our task in this deliverable is to concentrate on one specific legal issue surrounding the Internet - privacy. More specifically we are concerned with the privacy issues raised by the new Internet Protocol – IPv6.

Dealing with the issue of privacy is fundamental in order to generate consumer confidence and ensure the successful widespread development of IPv6 in Europe. Irrespective of how well IPv6 is designed and how many additional possibilities it provides for better quality, faster appliances on the Internet, if people do not have confidence that it will protect their privacy (i.e. think it is unsafe), this will hinder its widespread deployment in Europe. Bad news rather than good news grabs the headlines and therefore if unchallenged stories are published about how IPv6 could allow every aspect of a citizen's life on the Internet to be tracked, it could be easy for this perception to develop in Europe. If this public perception is allowed to take hold, this could cause untold damage to IPv6's deployment.

The bad publicity started in the US during the late 1990´s when press reports began to appear about privacy concerns relating to the use of unique serial numbers in IPv6 addresses. The concerns mainly focused on the possibility of monitoring individuals on an unprecedented nature based on tracking their activities through their IPv6 address embedded in every packet of information transmitted. For example, Bill Frezza wrote a highly publicized article entitled "Where's All the Outrage About the IPv6 Privacy Threat" that contained the following passages:

"What happens when companies such as Intel or Microsoft are found to have embedded unique identifiers in their hardware or software that pose potential privacy problems for Internet users? As we know from experience with both the Pentium III Serial Number flap and the Microsoft Win98 Registration Wizard brouha, professional privacy advocates sound the alarm, the press launches a feeding frenzy, Wall Street shudders and the alleged corporate miscreants are flogged into backing off.

Now, what happens when the Internet Engineering Task Force does the same thing, specifying an addressing structure in its next-generation Internet protocol, IPv6, such that every packet can be traced back to each user's unique network interface card ID? Apparently, nothing.

The spooks and weirdos in Washington, ever eager to empower the surveillance state as they fight a rear-guard action against strong encryption, must be thrilled with such a gift. … Where are the professional privacy advocates on this issue?…. Could it be that this unusual averting of the collective gaze is just an embarrassing attempt to avoid airing the family's dirty laundry?"

This debate crossed the Atlantic and both the European Council and the Article 29 Data Protection Working Party of the European Commission have recognized the possibility of similar privacy concerns. Our role is to analyze what the concerns are, how they fit into the current European legal framework, whether these concerns are justified and if so, identify what needs to be done.

This work is performed by as part of the Euro6IX project (http://www.euro6ix.org), an IST European Funded project to design, construct, implement and test IPv6 in a large European network in order to encourage its widespread implementation. The Euro6IX project consortium consists of telecommunications companies, universities, mobile operators and Internet consultants working on the technical aspects of IPv6.

2. EURO6IX AND IPV6

IPv6 has been called the New Internet or the Internet for the New Generation. The problem with the rapid growth in the "Old" Internet over the last years is that it is running out of addresses. The Internet's basic communications are made possible by a system called IP (which stands for Internet Protocol) which requires every Net connected computer or device to have a digital address called an IP address. The current version of the Internet protocol is called IP version 4 (or IPv4) and this has been used for about 20 year. However IPv4 only has room for only about 4 billion addresses and it is estimated that these addresses will run out in 2005. Additionally the distribution of the addresses in IPv4 is unbalanced as a third of the world's addresses are reserved for the US (66.90%) where in fact two US universities have more allocated addresses than the whole of China (which has 1.65% of the world's addresses).

The computer scientists who developed the Internet and preside over its basic structure foresaw the address shortage problem and about 10 years ago developed a basic new version of the Internet Protocol called IPv6. This has enough capacity to provide a billion billion addresses for each square metre of the earth's surface. Mathematically speaking, this has been done by moving from a 32-bit IPv4 address to a 128-bit IPv6 address, which will allow for the predicted future growth of the Internet and Internet related technologies.

A smooth move from IPv4 to IPv6 is a huge task and needs a substantial investment in research and technology so that a large-scale trial for the continuing development and architecture can be conducted on an international level. This is the task of Euro6IX.

Apart from addressing the shortage problem, the development and introduction of IPv6 will allow a general overhaul of the architecture and design of the Internet to create a faster, better quality, more secure service. IPv6 solves the scaling issues of today's Internet and supports new features while enhancing others, including end-to-end connectivity, plug & play autoconfiguration, built-in security, mobility, multicast, anycast and support of larger data packets.

Whilst the introduction of the New Internet is both necessary and inevitable, concerns about the design of one type of IPv6 address using unique identifiers may give rise to privacy issues that need to be considered.

2.1 What is Privacy?

Privacy is and has always been one of the most important and comprehensive of all human rights. It is also one of the hardest to protect. Without privacy, other rights like freedom of speech or assembly would be less meaningful.

Privacy has many important aspects. In part, it is what you choose to let other people know about you and in part it is the ability to remain anonymous. Privacy is about who controls the information you choose to share with other people. For example, you might decide to share your address with an on-line bookseller you are buying a book from but you would not want them to publish your address to all visitors to the web page and they would be breaching your privacy if they did so.

In general when we talk about our right to privacy, we mean the right to:

- Keep our personal information to ourselves.
- Have the choice to remain anonymous or unidentified with respect to certain personal and public activities. These activities would include the exercise of public rights like freedom of assembly, or private choices like our spending habits or our manner of worship.
- Live our lives without being under surveillance (or watched) by other people.
- Conduct private communications.
- Have physical privacy and personal space.
- To be left alone, both as consumers and as citizens.

The only way for an individual to guarantee to protect his privacy is to stop interacting with the world. Obviously this is impossible and undesirable for ordinary citizens and therefore general principles needs to be developed to make sure that when interaction took place, some protection was available.

2.2 What is the Foundation for the Right to Privacy?

The modern day basis for European privacy is the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950. The Convention, established by a now defunct body called the Council of Europe and open to any European Country to ratify, was intended to put the protection of human rights and fundamental freedoms on a "legal" footing following the horrors of the Second World War. It encompasses a number of fundamental rights such as the right to life, the right to a fair trail, the right against torture and amongst these fundamental rights we also find the right to privacy.

The Convention's definition of the right to privacy (contained in Article 8) extended to four separate areas where an individual has the right to have his privacy respected:

1. Private life.
2. Family life.
3. Home life.
4. Correspondence.

This Convention was adopted before the European Community or Union (as we know it today) was formed. However as human rights were one of the founding principles of the EU and an indispensable condition for its legitimacy, the Heads of State or Government decided in a meeting at the Cologne European Council (June 1999) that there was a need to formalize these rights and to ensure that they were more visible within the Union. This led to the proclamation of the EU Charter on Fundamental Rights adopted on 8th December 2000.

The right to privacy as set out in the 1950 Convention was mirrored in Article 7 of the EU Charter that stated:

"Everyone has the right to respect for his or her private and family life, home and communications".

The word "correspondence" used in the 1950 Convention has been replaced by "communications" in the EU 2000 Charter to reflect the various means of interaction in the

technological age as correspondence has old fashioned connotations such as traditional postal mail or "snail mail".

2.3 What is the Link between Privacy and Data Protection?

Since the 1950 Convention a new facet of privacy had developed, directly linked to technological advances and in particular the increase in the automated processing of information. This new facet of privacy became known as data protection. Data protection is the sword used to protect privacy in the technological age. Whilst Article 7 of EU Charter 2000 reflected the fundamental right to privacy as enshrined in the 1950 Convention, it also contained a new fundamental right not dealt with in 1950, the right to data protection.

Article 8 of the 2000 EU Charter states that:

1. "Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority".

2.4 Why is Data Protection Necessary?

Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology and the information society. When personal human interaction was replaced by technological means, this left a trail of information about the interaction. This trail is known as data. When this data is linked to an individual is becomes personal data. The concerns arose as it became apparent that it was easy to automatically collate, store and disseminate this information about individuals.

The potential misuse of this personal data created a huge new danger to an individual's privacy in all four areas where a person was entitled to protection: Private life, family life, home life and communications. As the popular maxim states, information is power. Rather than remaining anonymous and in control of one's privacy, the computer and telecommunications age had potentially shifted the balance of power into the hands of others, those who had access to the data.

However technology was (and is) clearly beneficial and impossible to stop and so a balance needed to be struck between allowing technology to advance and protecting an individual's privacy in respect of the data trail or information he left behind. Specific rules governing the collection and handling of such data needed to be developed.

2.5 What Rules Govern Data Protection?

The genesis of modern data protection legislation can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. National laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978) followed.

The first major European legislation was the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data that set out specific rules covering the handling of electronic data. These rules defined personal data and established the necessary protection at every step from collection to storage and dissemination.

The 1981 Convention effectively forms the basis of modern European thinking on data protection and explicitly created the link between data protection and privacy, basing the protection of personal data on protecting the fundamental human right to privacy (Article 1). The Convention's object was to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them. It aimed to create some rules about how personal information should be treated and how individuals could have control over personal information collected and used by others. The Convention expressly stated that the unfettered exercise of the freedom to process information may under certain circumstances "adversely affect the enjoyment of other fundamental rights".

The Convention defined "personal data" as "*any information relating to an identified or identifiable individual ("data subject")*."

The basic data protection principles established in the 1981 Convention were developed in three subsequent EC Directives.

1. Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

2. Directive 97/66/EC of the European Parliament and the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

3. Directive 2002/58/EC of the European Parliament and the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications Sector.

The first Directive established a framework to allow the free movement of data but at the same time ensure that the fundamental right of privacy was protected. It recognized that continuing advances in technology developed new ways to capture, transmit, manipulate, record and store personal data and therefore was expressly drafted in such a way as to be adaptable and applicable to technological advances.

The legal definition of "personal data" was expanded from the Convention to encompass "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*." The relevance of this definition, particularly in relation to identification numbers, to the development of the Internet and IPv6 will become apparent later in this Paper.

The Directive established general rules on the lawfulness of the processing of personal data and deals specifically with issues such as the principles relating to data quality, the criteria for making data processing legitimate, special categories of processing, information to be given to the data subject, the data subject's right of access to data, exemptions and restrictions, the data subject's right to object, confidentiality and security of processing, notifications, judicial

remedies, liabilities and sanctions, transfers of personal data to third countries, codes of conduct and supervisory authorities.

Article 29 of Directive 95/46/EC also established an independent Working Party whose ambit was inter alia to examine, opine, advise and recommend on how the processing of personal data impacted on the rights and freedoms of natural persons. As we stated in the introduction, this Article 29 Working Party was the European body that published the Opinion on the specific potential dangers to privacy relating to the use of unique identifiers in IPv6.

Directive 97/66/EC (telecommunications sector) sought to extend the principles of Directive 95/46/EC to the telecommunications networks as the Commission stated that "new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user and the development of the information society is characterized by the introduction of new telecommunications services". The use of public telecommunications networks created new "forms" of data, which did not necessarily fit neatly into the existing data protection definitions and therefore this Directive was a way of ensuring that the legislation dealt adequately with these technological advances.

The Directive above in turn needed to be adapted to take into consideration developments in the Markets and Technologies for Electronic Communications Services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. Therefore Directive 2002/58/EC was adopted as a response to new advanced digital technologies being introduced (e.g., widespread access to digital mobile networks). These advanced digital technologies entailed new possibilities for users but also new risks for their data protection and privacy. The Directive 2002/58/EC sought to provide confidence to users that their privacy will not be at risk with these new developments.

Directive 2002/58/EC did not create major changes to the substance of Directive 97/66/EC. It merely adapted and updated the existing provisions to new developments in electronic communications services and technologies. Therefore, the majority of provisions of the existing Directive were simply carried over in the new proposal. The new regulatory framework was intended to recognize the convergence of telecommunications, media and information technology. It covered all communications infrastructure and associated services and was intended to be technology-neutral. The intention was that the same service is regulated in the same way, regardless of how it is delivered.

Recital 5 of Directive 2002/58/EC states that

"The Internet is overturning traditional market structures by providing a common global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy."

The three Directives above taken in conjunction were intended to ensure that there was sufficient protection for any form of automated processing in any technological form. The Internet, and therefore IPv6, will be subject to the Directives and the rules that this imposes[1]. The adequacy of these Directives in respect of IPv6 is outside the scope of this current paper and will be dealt with in the second deliverable due in December 2003.

[1] Article 29 Working Party document on the Processing of Personal Data on the Internet adopted on 23rd February 2003 (WP16).

The fundamental principles of data protection extracted all require that personal information must be:

- Obtained fairly and lawfully.
- Used only for the original specified purpose.
- Adequate, relevant and not excessive to purpose.
- Accurate and up to date.
- Accessible to the subject.
- Kept secure.
- Destroyed after its purpose is completed.

These general principles form the cornerstone of European data protection law. As we shall see those involved in the design and implementation of IPv6 need to bear these principles in mind to ensure that the New Protocol complies with these requirements.

3. WHAT ARE SOME OF THE GENERAL PRIVACY CONCERNS REGARDING THE INTERNET?

3.1 Where are the Inherent Dangers in the Internet Protocol?

To understand the reason for the privacy concerns in the Internet (and IPv6) it is necessary to understand how the Internet works. The Internet is a network of computers communicating with each other on the basis of the Transport Control Protocol/Internet Protocol (TCP/IP). For the Internet Protocol to function and computers to be able to communicate with each other, every computer is identified by a single numerical IP address (in IPv4 this is a 32 bit address and in IPv6 a 128 bit address).

3.2 Is an IP Address Personal Data?

The answer to this question is important because if an IP address is considered personal data *per se* then the processing of this personal data is protected by the privacy and data protection rules.

The definition in Article 2(a) of Directive 95/46/EC states that personal data means any information relating to an identifiable or identified person, such as for instance data relating to an identification number, his/her physical, physiological, mental, economic, cultural or social identity. It is important to note that the Directive states that if there is a possibility of identifying a person from the information, and then it is considered personal data.

Recital 26 of Directive 95/46/EC states that to determine whether a person is identifiable, account should be taken of all means likely reasonably to be used either by the controller or by any other person to identify the said person.

Processing of personal data is defined in Article 2(b) as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Therefore if an IP address were considered personal data, the fact of communicating using the IP address would be considered processing.

The Article 29 Working Party's has stated that as "recital 26 of Directive 95/46 specifies, data is qualified as personal data as soon as a link can be established with the identity of the data subject (in this case, the user of the IP address) by the controller or any person using reasonable means. In the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means."

Therefore an IP address (irrespective of whether this is in IPv4 or in IPv6) is considered personal data because a link can potentially reasonably be made between the address and the individual by some of the actors in the Internet. As we shall see in IPv6 the privacy (data protection) problem was seen as even more serious as one form of address (by using the unique identifier) potentially made the link between the address and the individual easier to determine.

3.3 Actors in the Internet

The various participants in the Internet are:

- The software, computer and telecommunications industries that design the network and services available.
- Telecommunications operators who provide the network for data transfer.
- Internet Access provider responsible for the Internet transport system.
- Internet Service Providers, which provide services such as HTTP (often the same as the ISP).
- The user.

Each of these actors has its own data protection responsibilities and ought to look at their role and the service that they provide to ensure that their actions are data protection compliant.

A Report and Guidance published by the International Working Group on Data Protection in Telecommunications ("Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet") in 1996 provided a useful overview of Internet privacy concerns for the Internet in general.

The document explained that the vast growth of the Internet had created what can be regarded as the first level of the emerging Global Information Infrastructure (GII) that potentially created numerous problems in relation to privacy. There are various participants in the Internet and each of these has different tasks, interests and opportunities and the principles of privacy and data protection needed to be maintained at all these different stages.

Given that the Internet does not have one governing body to oversee privacy and data protection issues on a global scale, the “user is forced to put trust into the security of the entire network, that is every single component of the network, no matter where located or managed by whom”.

The paper stated that there are certain bodies (international, regional or national) that manage various functions on the Net and given the fact that there is no Internet Governing body, the role of these bodies is important, in particular when developing the protocols and standards for the Internet, fixing rules for the identification of servers connected and eventually for the identification of users. This is directly applicable in the context of IPv6.

“A balance has to be struck between a person who does not want to leave his fingerprints on the Net and the fact that providers will want identification and authentication to help with charging and marketing tasks”.

3.4 Privacy Guidelines

Whilst the role and function of each specific actor can be examined in greater detail to determine the data protection and privacy concerns, the Group published a 10-point plan as an overview of the principles to be borne in mind when determining how the balance in section 3.3 above should be maintained as new protocols, standards and services were developed.

The 10-point plan stated:

"There can be no doubt that the legal and technical protection of Internet users' privacy is at present insufficient[2].

On the one hand the right of every individual to use the Information Superhighway without being observed and identified should be guaranteed. On the other hand there have to be limits (crash-barriers) with regard to the use of personal data (e.g. of third persons) on the highway.

A solution to this basic dilemma will have to be found on the following levels:

1. Service providers should inform each potential user of the Net unequivocally about the risks to his privacy. He will then have to balance these risks against the expected benefits.

2. In many instances the decision to enter the Internet and how to use it is subject to legal conditions under national data protection law. Personal data may only be collected in a transparent way.

3. Initiatives to arrive at closer international cooperation, even an international convention governing data protection in the context of trans-border networks and services are to be supported.

4. An international oversight mechanism should be established which could build on the existing structures such as the Internet Society and other bodies. Responsibility for privacy protection will have to be institutionalized to a certain extent.

5. National and international law should state unequivocally that the process of communicating (e.g. via electronic mail) is also protected by the secrecy of telecommunications and correspondence.

6. Furthermore it is necessary to develop technical means to improve the user's privacy on the Net. It is mandatory to develop design principles for information and communications technology and multimedia hard and software, which will enable the individual user to control and give him feedback with regard to his personal data. In general users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service.

7. Technical means should also be used for the purpose of protecting confidentiality. The use of secure encryption methods must become and remain a legitimate option for any user of the Internet. The Working Group supports new developments of the Internet Protocol (e.g. IPv6), which offer means to improve confidentiality by encryption, classification of messages and better authentication procedures. The software manufacturers should implement the new Internet Protocol security standard in their products and providers should support the use of these products as quickly as possible[3].

8. The Working Group would endorse a study of the feasibility to set up a new procedure of certification issuing "quality stamps" for providers and products as to their privacy-friendliness. This could lead to an improved transparency for users of the Information Superhighway.

9. Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society without questioning the principle as such.

[2] We should remember that this was published in 1996
[3] The issue of IPv6 security will be dealt with in our final deliverable due in October 2004.

10. Finally it will be decisive to find out how self-regulation by way of an expanded "Netiquette" and privacy-friendly technology might improve the implementation of national and international regulations on privacy protection. It will not suffice to rely on any one of these courses of action: They will have to be combined effectively to arrive at a Global Information Infrastructure that respects the human rights to privacy and to unobserved communications."

The relevance of point 9 above to IPv6 will be explained later.

The Article 29 Working Party as well as looking at specific issues regarding the Internet provided some general guidelines. It stated that:

- "The Internet was conceived as an open network at world level (www) through which information could be shared. It is however necessary to find a balance between the "open nature" of the Internet and the protection of the personal data of the Internet users (proportionality).
- Enormous amounts of data on Internet users are collected on the Internet while often users are not aware of this fact. This lack of transparency towards the Internet users needs to be addressed in order to achieve a good level of personal data and consumers' protection.
- Protocols are technical means that in fact determine how data are to be collected and processed. Browsers and software programmes also play an important role. In some cases they include an identifier that makes it possible to link the Internet user to his/her activities in the Net. It is therefore the responsibility of those involved in the design and development of these products to offer users privacy-compliant products. In that sense it is important to mention that article 14 of the Telecoms Directive of July 2000 declares that, where required, the Commission shall adopt measures to ensure that technical equipment incorporates the necessary safeguards to guarantee the protection of personal data and privacy of users and subscribers."

The question of anonymity was specifically dealt with in Recommendation 3/97 Anonymity on Internet dated 3rd December 1997. This stated that:

"Over the past 25 years it has become apparent that one of the greatest threats to this fundamental right to privacy is the ability for organizations to accumulate large amounts of information about individuals, in a digital form which lends itself to high-speed (and now very low-cost) manipulation, alteration and communication to others. Concerns about this development and the potential misuse of such personal data has led all European Member States (and now the Community with Directive 95/46/EC) to adopt specific data protection laws which set down a framework of rules governing the processing of personal information.

A feature of telecommunications networks and of the Internet in particular is their potential to generate a huge quantity of transactional data (the data generated in order to ensure the correct connections). The possibilities for interactive use of the networks (a defining characteristic of many Internet services) increases the amount of transactional data yet further.

As on-line services develop in terms of their sophistication and their popularity, the problem of transactional data will grow. Everywhere we go on the Internet, we leave a digital trace. As more and more aspects of our daily activities are conducted on-line, more and more of what we do, our choices, our preferences, will be recorded.

Transactional data are only a threat to individual privacy if the data relate to an identifiable person. Clearly one way of addressing privacy concerns would therefore be to seek to ensure that wherever feasible the data traces created by using the Internet do not permit the identification of the user. With anonymity guaranteed, individuals would be able to participate in the Internet revolution without fear that their every move was being recorded and information about them accumulated which might be used at a later date for purposes to which they object."

However the principle of anonymity must be balanced with the "principle of proportionality". The Recommendation is that on the key issue of anonymity, the same rules as regard offline behavior should be followed on line.

Finally the Recommendation concludes that:

"The ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on-line as they currently enjoy off-line." However this should always be balanced, taking into account other considerations such as prevention of crimes.

More importantly with regard to the Internet Protocols, which has a bearing on IPv6, the Recommendation stated that:

"User access and activity on the Internet is very rarely anonymous…, the technical configuration on Internet protocols does not easily allow true anonymity …"

The Internet posed a problem because "the use of the infrastructure is often directly based on the processing of personal data, such as certain Internet Protocol addresses".

Against this background we look at the issue of the new Internet Protocol and whether the use of a certain type of IP addresses conforms to the privacy guidelines established above.

4. WHAT ARE THE SPECIFIC PRIVACY CONCERNS FOR IPV6?

As mentioned in the introduction, commentators raised concerns about the privacy issues surrounding IPv6 in the United States in the late 90's and these concerns have been officially raised in Europe. IPv6 needs to be deployed as soon as possible and therefore these concerns need to be addressed to prevent any potential obstacles being put in the way.

The first official paper was released when the European Commission published COM (2002) 96 dated 21st February 2002. This publication was a communication from the Commission to the Council and the European Parliament entitled "Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6". The aim of this document was to set out the European Commission's views on issues concerning the deployment of IPv6 in Europe and one of the issues specifically dealt with was privacy.

The European Commission's thinking is highlighted in the following paragraph:

"However for new Internet enabled services to be deployed in a timely manner, it is of key importance to structure, consolidate and integrate European efforts on IPv6, and notably to develop the necessary base of skilled human resources, to fully harmonize, where needed, the policy approaches, to sustain the research effort, to promote the standards and specifications work and to ensure that all sectors of the new economy likely to be impacted by IPv6 are fully aware of potential benefits accruing from its adoption.

Further to the work carried out by the IPv6 Task Force, the Commission proposes a set of actions to ensure that the European Union maintains the initiative and leadership in these global developments. These actions require a concerted action aiming at the structuring, consolidation and integration of European efforts on IPv6, notably through:

1. An increased support towards IPv6 in public networks and services.
2. The establishment and launch of educational programmes on IPv6.
3. The adoption of IPv6 through awareness raising campaigns.
4. The continued stimulation of the Internet take-up across the European Union.
5. An increased support to IPv6 activities in the 6th Framework Programme.
6. The strengthening of the support towards the IPv6 enabling of national and European Research Networks.
7. An active contribution towards the promotion of IPv6 standards work.
8. The integration of IPv6 in all strategic plans concerning the use of new Internet Services."

Having set out the background, the Communication specifically deals with the potential privacy issues for IPv6.

"Due to the fact that the Internet has, from the very beginning, been considered as an open network, there are many characteristics of its communication protocols, which, more by accident

than design can lead to an invasion of the privacy of Internet users. Concerns are expressed on a regular basis regarding the need to find a balance between the "open nature" of the Internet and the conflicting needs to effectively maintaining and debugging a network and the protection of the personal data of the Internet users. The fundamental right to privacy and data protection is enshrined in the EU Charter on fundamental rights and developed in detail in the EU data protection directives 95/46/EC and 97/66/EC which both apply to processing of personal data on the Internet. In its Communication on the Organization and Management of the Internet Domain Name System of April 2000, the Commission stated already that an IP address can be personal data in the sense of the legal framework (for example dynamic IP addresses). Also the Article 29 Data Protection Working Party, the independent EU advisory body on data protection and privacy established by Directive 95/46/EC, draws the attention at several occasions to privacy issues raised by the use of the Internet. The Article 29 Data Protection Working Party as well as the International Working Group on Data Protection in Telecommunications (the "Berlin Group") work specifically on IPv6.

It is therefore of indispensable that the European Commission and the European Union as a whole consider privacy issues in the further development of Internet. While privacy issues are currently being taken into account in the development of IPv6, it is essential that the trust and confidence of Internet users in the whole system, including in the respect of their fundamental rights, is ensured".

In its conclusions the European Commission asked for the parties to:

"Study the impact of the further evolution of the Internet including the new generation IPv6 protocol, on the fundamental right to privacy and data protection, so as to ensure that the required standards and specifications take these aspects into full consideration".

Having called for a general study into the privacy issues, a few months later in May 2002, the Article 29 Working Party published a document entitled "Opinion 2/2002 on the use of unique identifiers in telecommunications terminal equipment: The example of IPv6".

This paper highlights the danger to privacy in respect of "the possibility of the integration of an unique identifier number in the IP address as designed according to the new protocol".

The thrust of this paper is that IP addresses attributed to Internet Users are personal data and therefore they are subject to the guidelines provided in the EU Directives.

"As recital 26 of Directive 95/46 specifies, data are qualified as personal data as soon as a link can be established with the identity of the data subject (in this case, the user of the IP address) by the controller or any person using reasonable means. In the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using existing technical means".

The problem with the use of unique identifiers as part of the IP address was that it went against the data protection principles (as described in the previous sections). In particular the paper states:

- "The unique identifier of an interface, such as the one that might be integrated in IPv6, would constitute an identifier of general application and its use is regulated as such in the legislation of the member States of the EU.
- The principle of proportionality implies that, making a balance between the fundamental rights of data subjects and the interests of different actors involved in the transmission of

telecommunication data (such as companies, telecommunication access providers), as few personal data as possible have to be processed.

- This principle has implications on the one hand on the design of the new communication protocols and devices, and on the other hand on the content of national policies related to the processing of telecommunication data: While technology is per se neutral, applications and design of new telecommunication devices should be privacy compliant by default. Besides, it should be avoided to generalize measures forcing the systematic identifiable character of telecommunication data.

In that perspective, in the framework of a telecommunication connection, network and access providers should offer to any user the option to use the network or to access the services anonymously or using a pseudonym.

EC Directive 97/66 provides for the possibility for any user to restrict the identification of calling and connected addresses. In Internet communications, anonymity could be reached using solutions such as regularly changing IP addresses used by an individual.

- Considering the risks of manipulation and fraudulent use of a unique identifier, the working party recalls that protection measures are needed, taking into account in particular that telecommunication providers are responsible for the security of services they offer. In the framework of the European Union legislation, access providers are obliged to inform subscribers of residual security risks.
- The requirements for privacy compliant default settings in communication devices and for privacy compliance of telecommunication services have been implemented at a European level through specific obligations laying mainly on producers of telecommunications equipment, and on telecommunication operators and service providers.

Therefore the specific privacy concern, first raised in US, and now taken up in Europe is the potential risk associated with the use of unique identifiers in the IP addresses under IPv6.

5. WHAT IS THE BASIS FOR THESE PRIVACY CONCERNS?

The privacy concerns highlighted in section 4 above are based on one design of the addressing format in IPv6 as approved by the Internet Engineering Task Force. This is the technical body advising on how the Internet should be developed and it provides standards for the Internet through the publication of various technical standards known as RFCs.

5.1 Request for Comments (RFC)

The Requests for Comments (RFC) document series originated as a set of technical and organizational notes about the Internet beginning in 1969. Memos in the RFC series discussed many aspects of computer networking, including protocols, procedures, programs and concepts. These official specification documents of the Internet Protocol defined by the Internet Engineering Task Force (IETF) and the Internet Engineering Steering Group (IESG) gained increasing importance and were recorded and published as standards track RFCs. This meant that RFCs became unofficial standards about how the Internet should be developed. As a result, the RFC publication process plays an important role in the Internet standards process. RFCs must first be published as Internet Drafts so that experts in the relevant areas have an opportunity to comment on the issue at hand before a consensus on the way forward is reached and the RFC becomes a standard.

The simple procedure is that in practice the specification undergoes a period of development and several iterations of a review by the Internet community and eventually is adopted as a standard by the appropriate body.

There are three maturity levels for RFC

- Proposed Standard.
- Draft Standard.
- Standard.

5.2 Does an IPv6 Address have a Unique Identifier?

There are various different types of addresses in IPv6 but the privacy issue relates to the address generated by stateless address autoconfiguration. The technical detail, which explains how this works, can be found in the following documents - RFC2373 relating to the IPv6 addressing architecture, RFC2642 entitled “IPv6 Stateless Address Autoconfiguration” and RFC2374 titled “IPv6 Aggregatable Global Unicast Address Format” and subsequent documents (draft-ietf-ipv6-unicast-aggr-v2-02.txt). We do not propose dealing with the technical intricacies of addressing but explain in simplistic terms how this type of address is created and whether the privacy concerns about unique identifiers are justified.

The rationale behind stateless address autoconfiguration is to generate a global unique address without the need for a DHCP (Dynamic Host Configuration Protocol) server. DHCP is the protocol, which allows a network administrator to supervise, manage centrally and automate the assignment of IP addresses. In layman’s terms these papers listed above set out the blueprint for the 128-bit IPv6 address. Using the analogy of postal address, the common standard is to put the name of the recipient, followed by the street (including number), city, state, post or zip code and country. Following this standard the address of this law firm would be:

- Ecija Abogados
- C/ Jorge Juan 9
- Madrid
- Madrid
- 28001
- Spain

This standard is now globally accepted and used in traditional postal correspondence. There is a similar standard or formula for the new IPv6 addresses in order to allocate the 128-bit address.

3	13	8	24	16	64 bits
FP	TLA ID	RES	NLA ID	SLA ID	Interface ID
PUBLIC TOPOLOGY				SITE TOPOLOGY	

Figure 5-1: IPv6 Aggregatable Global Unicast Address Format

The numbers in the first line of the table refer to the "bits" or "digits". Each of the bits relates to a different layer to enable communication on the network. The address is split into two parts the public topology and the site topology. Therefore the site would be "private" depending on each individual network and the public topology relates to the "public" network to allow Internet communication.

Each of the relevant parts are explained below

FP Format Prefix (001)

TLA ID Top-Level Aggregation Identifiers (TLA ID) are the top level in the routing hierarchy. The routing topology at all levels must be designed to minimize the number of routes into the routing tables. Each organization assigned a TLA ID receives 24 bits of NLA ID space. This space can be delegated to approximately as many organizations as the current IPv4 Internet. Organizations assigned a TLA ID can provide service to organizations providing public transit service and to organizations, which do not provide public transit service. The organizations receiving an NLA ID may also choose to delegate their space to another NLA ID's.

Res The Reserved field is reserved for future use and must be set to zero.

NLA ID Next Level Aggregation Identifier is used by organizations assigned a TLA ID to create an addressing hierarchy and to identify sites. The organization can assign the top part of the NLA ID in a manner to create an addressing hierarchy appropriate to its network.

SLA ID Site-Level Aggregation Identifier The SLA ID field is used by an individual organization to create its own local addressing hierarchy and to identify subnets. It is a 16-bit field, so it supports 65,535 subnets. The approach chosen for structuring an SLA ID field is the responsibility of the individual organization.

Interface ID — Interface identifiers are unique serial numbers or addresses that are link dependent and therefore used to identify interfaces on a link. They are required to be unique on that link. It is this part of the address which caused the privacy concerns as we shall see below. An interface is defined as a node's attachment to a link. Interface Identifiers are unique serial numbers or addresses, which are link dependent. An identifier for an interface is (at least) unique per link.

In the last IETF documents, this has been simplified as:

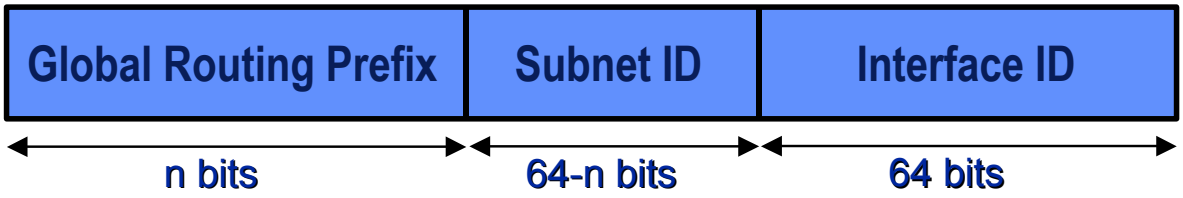

Figure 5-2: Updated IPv6 Aggregatable Global Unicast Address Format

IPv6 uses the 128 bits to provide addressing, routing, and identification information on a computer interface or network card. Some IPv6 systems use the right 64 bits to store an IEEE defined global identifier (EUI64). This identifier is composed of company id value assigned to a manufacturer by the IEEE Registration Authority. The 64-bit identifier is a concatenation of the 24-bit company identification value and a 40-bit extension identifier assigned by the organization with that company identification assignment. The 48-bit MAC address of a network interface card may also be used to make up the EUI64.

The problems relating to privacy were grounded on the basis that the Interface ID, which would be based on the ID of the hardware interface as described above, would identify each machine individually. Therefore every time one went on the Internet to send and receive packets of information, this would effectively leave a fingerprint which can be traced back to the individual.

5.3 How is an IPv6 Address Configured?

RFC2642 explains how stateless address autoconfiguration combines an interface identifier with a prefix to form an address.

The RFC states:

“This document specifies the steps a host takes in deciding how to autoconfigure its interfaces in IP version 6. The autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both), and in the case of addresses, whether they should be obtained through the stateless mechanism, the stateful mechanism, or both. This document defines the process for generating a link-local address, the process for generating site-local and global addresses via stateless address autoconfiguration, and the Duplicate Address Detection (DAD) procedure”.

“One of the design goals for stateless autoconfiguration is that:

- Manual configuration of individual machines before connecting them to the network should not be required. Consequently, a mechanism is needed that allows a host to obtain or create unique addresses for each of its interfaces. Address autoconfiguration assumes that each interface can provide a unique identifier for that interface (i.e., an "interface

identifier"). In the simplest case, an interface identifier consists of the interface's link-layer address. An interface identifier can be combined with a prefix to form an address."

In layman's terms this RFC outlines further how this type of addresses under IPv6 is self-generating rather than allocated and based on the unique identifiers in the hardware.

5.4 What is the Problem with Stateless Address Autoconfiguration?

The potential privacy problem with this type of IPv6 addresses is described in detail in RFC3041. The documents highlights the fact that any communication system which has a constant address or identifier for incoming and outgoing communication has potential privacy concerns (this is the same for IPv4 or IPv6)

"Stateless address autoconfiguration defines how an IPv6 node generates addresses without the need for a DHCP server. Some types of network interfaces come with an embedded IEEE Identifier (i.e., a link-layer MAC address), and in those cases stateless address autoconfiguration uses the IEEE identifier to generate a 64-bit interface identifier. By design, the interface identifier is likely to be globally unique when generated in this fashion. The interface identifier is in turn appended to a prefix to form a 128-bit IPv6 address.

All nodes combine interface identifiers (whether derived from an IEEE identifier or generated through some other technique) with the reserved link-local prefix to generate link-local addresses for their attached interfaces. Additional addresses, including site-local and global-scope addresses, are then created by combining prefixes advertised in Router Advertisements via Neighbor Discovery with the interface identifier.

Not all nodes and interfaces contain IEEE identifiers. In such cases, an interface identifier is generated through some other means (e.g., at random), and the resultant interface identifier is not globally unique and may also change over time. The focus of this document (RFC3041) is on addresses derived from IEEE identifiers, as the concern being addressed exists only in those cases where the interface identifier is globally unique and non-changing".

RFC3041 spells out the potential privacy problem with the use of the unique identifier as a constant part of the address in the following manner:

"The use of a non-changing interface identifier to form addresses is a specific instance of the more general case where a constant identifier is reused over an extended period of time and in multiple independent activities. Anytime the same identifier is used in multiple contexts, it becomes possible for that identifier to be used to correlate seemingly unrelated activity. For example, a network sniffer placed strategically on a link across which all traffic to/from a particular host crosses could keep track of which destinations a node communicated with and at what times. Such information can in some cases be used to infer things, such as what hours an employee was active, when someone is at home, etc.

Web browsers and servers typically exchange "cookies" with each other. Cookies allow web servers to correlate a current activity with a previous activity. One common usage is to send back targeted advertising to a user by using the cookie supplied by the browser to identify what earlier queries had been made (e.g., for what type of information). Based on the earlier queries, advertisements can be targeted to match the (assumed) interests of the end-user.

The use of a constant identifier within an address is of special concern because addresses are a fundamental requirement of communication and cannot easily be hidden from eavesdroppers and

other parties. Even when higher layers encrypt their payloads, addresses in packet headers appear in the clear. Consequently, if a mobile host (e.g., laptop) accessed the network from several different locations, an eavesdropper might be able to track the movement of that mobile host from place to place, even if the upper layer payloads were encrypted.

5.4.1 The Concern With IPv6 Addresses

The division of IPv6 addresses into distinct topology and interface identifier portions raises an issue new to IPv6 in that a fixed portion of an IPv6 address (i.e., the interface identifier) can contain an identifier that remains constant even when the topology portion of an address changes (e.g., as the result of connecting to a different part of the Internet). In IPv4, when an address changes, the entire address (including the local part of the address) usually changes.

If addresses are generated from an interface identifier, a home user's address could contain an interface identifier that remains the same from one dialup session to the next, even if the rest of the address changes.

A more troubling case concerns mobile devices (e.g., laptops, PDAs, etc.) that move topologically within the Internet. Whenever they move (in the absence of technology such as mobile IP), they form new addresses for their current topological point of attachment. The “road warrior” who has Internet connectivity both at home and at the office typifies this today. While the node's address changes as it moves, however, the interface identifier contained within the address remains the same (when derived from an IEEE Identifier). In such cases, the interface identifier can be used to track the movement and usage of a particular machine. For example, a server that logs usage information together with a source address is also recording the interface identifier since it is embedded within an address. Consequently, any data-mining technique that correlates activity based on addresses could easily be extended to do the same using the interface identifier. This is of particular concern with the expected proliferation of next-generation network-connected devices (e.g., PDAs, cell phones, etc.) in which large numbers of devices are in practice associated with individual users (i.e., not shared). Thus, the interface identifier embedded within an address could be used to track activities of an individual, even as they move topologically within the Internet.

In summary, IPv6 addresses on a given interface generated via Stateless Autoconfiguration contain the same interface identifier, regardless of where within the Internet the device connects. This facilitates the tracking of individual devices (and thus potentially users).”

6. DO THESE PRIVACY CONCERNS HAVE A SOLUTION?

6.1 RFC3041 – Privacy Extensions for Stateless Address Autoconfiguration

As stated above, in respect of the unique number (IP address), IPv6 pioneered a labor saving way for "interface identifiers" to be formed automatically in devices, as one of the various methods of setting up addresses. The privacy concern related to the fact that both this and the interface identifiers in "always-on" environments result in permanent numbers as part of the addresses and allow the tracking of individuals.

Market researchers use techniques (data-mining) that can track Internet usage and, if addresses don't change, match them to individuals. This is of particular concern with the expected proliferation of next-generation Internet-connected devices (e.g., PDAs, cell phones, etc.) that could be associated with individual users. With the growing use of "always-on" links (DSL, cable modems), users are increasingly subject to data mining that tracks their unchanging Internet address.

Thomas Narten of IBM and Richard Draves of Microsoft Research published a procedure to deal with this issue and ensure privacy of IPv6 users - RFC3041 titled "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" published in January 2001 by the IETF. The procedure works on the basis of an algorithm developed jointly by Narten and Draves, which generates randomized interface identifiers numbers and temporary addressees during a user session for outgoing communications. Randomly generated numbers would replace the unique interface identifier and RFC3041 standardized how and when that would be done. The aim of this was to eliminate the concerns privacy advocates had with IPv6 by generating a random identifier(s) for the same node for outgoing communications making it difficult to determine the connection between a node and an individual.

The summary at the beginning of the document states:

“Nodes use IPv6 stateless address autoconfiguration to generate addresses without the necessity of a Dynamic Host Configuration Protocol (DHCP) server. Addresses are formed by combining network prefixes with an interface identifier. On interfaces that contain embedded IEEE Identifiers, the interface identifier is typically derived from it. On other interface types, the interface identifier is generated through other means, for example, via random number generation. This document describes an extension to IPv6 stateless address autoconfiguration for interfaces whose interface identifier is derived from an IEEE identifier. Use of the extension causes nodes to generate global-scope addresses from interface identifiers that change over time, even in cases where the interface contains an embedded IEEE identifier. Changing the interface identifier (and the global-scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node”.

6.2 How RFC3041 Works

We have set out below a brief explanation of how the RFC3041 works in practice. As explained, Stateless Address Autoconfiguration is a mechanism to create a 128-bit IPv6 address. The left hand 64 bit is the "prefix" and the rightmost 64-bit is the unique identifier or EUI-64 IID.

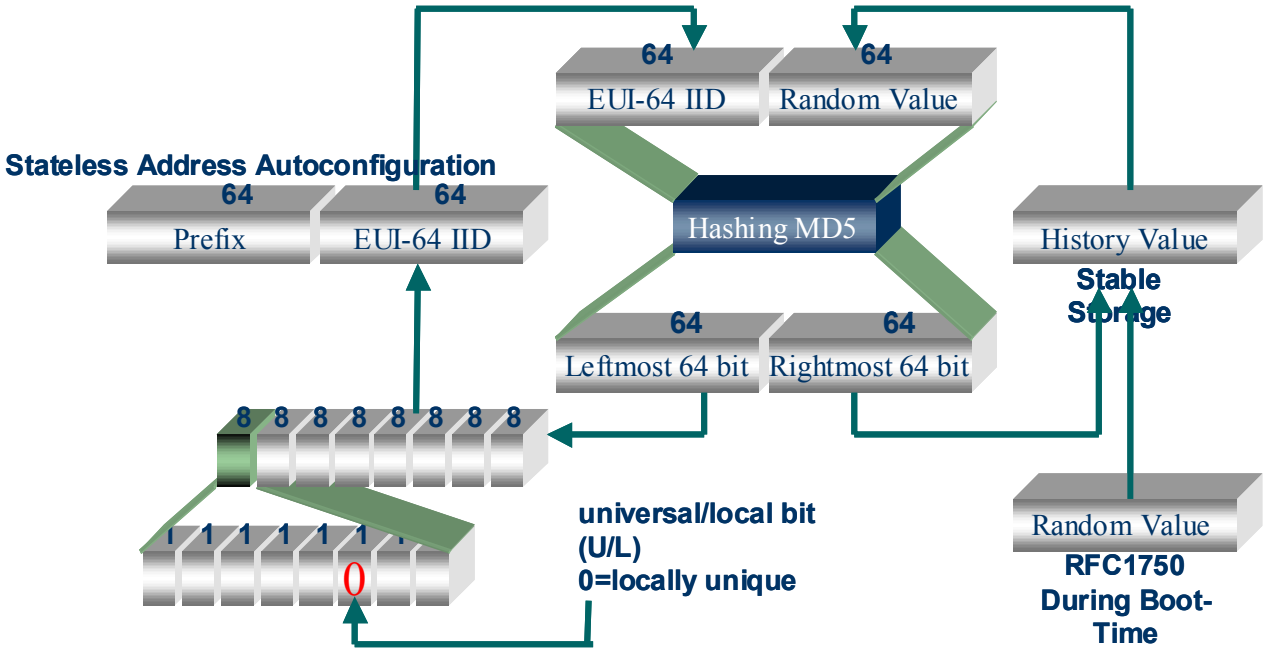

Figure 6-1: How Interface ID is Created

As seen from the diagram above, a random number would replace the EU1-64IID. The mechanism would attach a 64 bit random value to the EUI-64 IID for history purposes and a hashing algorithm would take place. This is a one-way algorithm that cannot reconstruct the original number. This algorithm would create a new random 128-bit number. The leftmost 64-bit forms part of the Stateless Address Autoconfiguration (which now has no link to the appliance as it is a randomly generated number not based on the unique identifier) to create an IPv6 address and right identifier remains as stable storage to prevent duplication.

This address would be used for outgoing communications. The terminal equipment uses two types of addresses: N address is generated based on the unique MAC address, and is used for entering communications (e.g. the terminal is always reachable using that permanent address), and another RFC3041 address generated on a random basis, to be used at the initiative of the terminal for outgoing connections. Thus, when the terminal (and the user behind) is responsible for the connection, it could not be identified through its MAC address.

RFC3041 established for the mechanism to be used to change IP addresses in certain timeframes although it does not provide recommendations about how often this should take place. If widely implemented it provides a solution to the privacy issues presented above and the implementation should be application specific.

6.3 What Force does it have?

RFC3041 is a "Standards track" RFC and it is currently in the category of a "proposed standard" (PS), which is the third of the three levels of maturity set out in above. This means that it is not yet a standard but should eventually become one.

Given that it is only a proposed standard, the force of the document may be called into question. It could be argued that whilst it is a potential solution, it is only a proposed solution. If it is not widely implemented, then the privacy problem still exists. However given the way that the Internet has developed, many things being used in daily Internet live (PPP, POP3, IPv6, FTP and TCP extensions, etc.) are still in "PS" category due to the fact that the IETF process is slow. Many of these things have the force of being a standard through widespread acceptance and implementation, which provide them with the "de facto" standard status. RFC3041 has been implemented in Microsoft Windows XP and Linux operating systems and the force of this speaks for itself.

Taking this into account, it is safe to say that RFC3041 is a "Standard", in all but name and it is on the "standards track". Given the fact of relatively short existence as an RFC since 2001 and the length of time that it takes to move through the standard track procedure, it is actually "normal" that it is currently still a Proposed Standard.

In March this year the IETF IPv6 Working Group that is responsible for the specification and standardization of the Internet Protocol version 6 (IPv6) stated that they were in the process of updating RFC3041 and publishing the updated version in June 2003. We shall wait to see what changes there are and how this may affect the above.

6.4 Practical conclusions

The technical solution above works because of the distinction between "initiator" and "target" communications (the equivalent of sending or receiving a letter). The privacy solution in IPv6 is relates to the scenarios when the Internet Device an "initiator" or sending communications.

The expectancy is that in the IPv6-based Internet, many devices will have two kinds of IP addresses:

- "Unique, stable addresses, assigned in any of the several possible ways (e.g. by manual configuration, by an address server like DHCP, or by auto-configuration using embedded factory assigned LAN addresses), for the purpose of being a target, and for use when initiating communications to the other trusted targets.
- Temporary, transient addresses, such as those containing random numbers in the place of the unique identifier (as per RFC 3041) for use when initiating communications to less trusted targets, such as public web servers.

The choice of which kind of address to use when initiating communications is somewhat analogous to the choice that must be made when placing a telephone call in the presence of the "Caller ID" feature i.e. whether or not to reveal the calling party's number to the called party. IPv6 addresses offer both choices[4].

[4] Steve Deering & Bob Hinden "Statement on IPv6 Address Privacy" dated November 6, 1999

7. WHAT STEPS HAVE BEEN TAKEN TO ACHIEVE A EUROPEAN CONSENSUS ON IPV6 PRIVACY

7.1 The Role of the European IPv6 Task Force

The European Commission set up an IPv6 Task Force ("EC IPv6 TF") in 2001 to help with the widespread deployment of IPv6 in Europe and one of its role's was to answer queries or criticisms raised about IPv6. Some of the EC IPv6 TF members are also involved in the Euro6IX project and both parties have a mandate to see the privacy issues dealt with effectively.

The EC IPv6 TF was concerned that the Article 29 Working Party Opinion (WP58) potentially resulted in an unbalanced view of the benefits of IPv6 and therefore organized a meeting with the Internet Group of the Article 29 Working Party ("Article 29 WP") to try and discuss this issue in more detail and explain the privacy enhancing features of IPv6. Several partners of Euro6IX and the IPv6 Task Force formed part of the group that attended a meeting in Brussels on 25th February 2003 on this specific issue.

The EC IPv6 TF published a position paper prior to the meeting, which made the following points:

- The EC IPv6 TF recognizes that the use of unique identifiers in any kind of technology or communication media (e.g. Ethernet, WLAN, GSM, ID cards, IPv4 and IPv6) represents a potential threat to privacy.
- But the EC IPv6 TF also notes that the use of stable identifiers is an important practical requirement in any communication system.
- All communications are subject to privacy issues and IPv6 is no exception.
- IPv6 has provided a mechanism (RFC3041) that goes a long way to solving the problem, potentially providing a higher degree of protection to the users than is possible in IPv4.
- In addition IP security (IPsec) mechanisms are available in full IPv6 implementations (RFC2460). Although their use is not mandatory, this offers an improvement over IPv4, where IPsec support is not present by default.

"The following key considerations must be taken into account when reviewing the privacy implications with IP based communications, both for existing IPv4 and the emerging IPv6.

1. IPv4 has privacy issues with static IP addresses being used as identifiers. These can be tracked just as other devices and items used by a person can be.

2. IPv6 by default where stateless autoconfiguration is used will construct IPv6 addresses that allow the correlation of activity where the same device is connected to different networks because a constant identifier (based on hardware in devices) is embedded in the IPv6 address.

3. RFC3041 fixes the problems of correlation by allowing an IPv6 device to generate a random identifier to embed in the address.

4. Many Internet systems use IP addresses as a (weak) authentication mechanism. Use of privacy extensions prevent such authentication being used. However, IPv6 includes IPsec by default, allowing stronger authentication methods to be used.

5. IPv6's Privacy Extensions enable a static host (e.g. workstation in the office) to use different IPv6 source addresses through time (e.g. a different IPv6 source address daily), allowing greater privacy for such non-mobile devices and users.

6. It is normal practice for IPv6 devices to have multiple addresses, where IPv4 devices usually have one address. It is thus possible for future IPv6 applications to use multiple (dynamic) IPv6 addresses, e.g. to reduce traceability in peer-to-peer applications.

7. Further research may introduce new classes of IPv6 addresses, for example cryptographically generated addresses. This is only possible with IPv6.

8. The EC IPv6 TF strongly recommends that vendors implement RFC3041 by default in all systems. The TF notes that some vendors have already done so.

9. There should be easy user-controllable mechanisms for RFC3041 to be enabled or disabled, per device/interface or per application. This could also be automatic depending on the initiated traffic (in bound or outbound), pre-configured by default or customized. These may require further work or research. Again, such enhancements are only possible with IPv6".

The EC IPv6 TF stated that "the privacy issue is one (important) piece of the larger chess-game of security, transmission, e-business, open government, law enforcement and even good governance. So in any intergovernmental recommendations on this area it would be useful to see a more interdisciplinary approach emerging in the future."

"The EC IPv6 TF believes that the new built-in properties in IPv6 provide a set of necessary and unique tools to empower a user's privacy in ways that are not possible in IPv4. The combination of the availability of IPSec support in full IPv6 implementations combined with these new properties makes IPv6 a potentially powerful tool to improve the possibilities for user privacy.

The EC IPv6 TF strongly recommends the implementation of RFC3041 by all IPv6 vendors. However it is clear that in any communication medium a balance needs to be struck between usability and privacy. For example, further work would be desirable on allowing user-controllable enabling of the IPv6 privacy extensions on a per-application basis".

In view of the above the EC IPv6 TF asked the Article 29 Working Party to reconsider its statement given the fact that IPv6 had significant improvement in relation to privacy in comparison to IPv4 and stated that a statement by them would be an important signal to the IPv6 community who had viewed the paper with some concern.

7.2 Meeting with Article 29 Working Party in Brussels on 25th February 2003

As stated above, after publishing this paper, the EC IPv6 TF went to Brussels to meet with the Internet Group of the Article 29 Working Party and after the meeting, the following joint document was approved.

The issue resulted from the publication of WP58 - Opinion 2/2002 published in May 2002 by the Article 29 Data Protection Working Group (Article 29 WG), which had had an impact in the IPv6 community worldwide as it had raised the issue of privacy concerns with the unique identifiers using IPv6 as the only example and the task was to clarify some issues raised.

This issue had been discussed by the International Working Group for Telecommunications at an international level and this Group had identified various issues such as the fact that unique identifiers could raise threats to privacy, there could be an increase in the profiling of individuals and there were issues with regard to the security of communications if many terminals had the same constant id. The Group had wanted to raise the issue so that a privacy default setting was high on the list for IPv6 implementations. These issues have been taken on board from a more European perspective in Article 29 WP Opinion 58.

The IPv6 Task Force Position

The IPv6TF presented its position (http://www.ec.ipv6tf.org/in/i-documentos.php) and gave a short overview of RFC3041. The EC IPv6 TF wanted to make clear that the following key considerations should be borne in mind when looking at the privacy implications of IP based communications both in IPv4 and IPv6.

1. IPv4 has privacy issues with static IP addresses being used as identifiers. These can be tracked just as other devices and items used by a person can be.

2. IPv6 by default where stateless autoconfiguration is used will construct IPv6 addresses that allow the correlation of activity where the same device is connected to different networks, because a constant identifier (based on hardware in the device) is embedded in the IPv6 address.

3. RFC3041 fixes the problems of correlation by allowing an IPv6 device to generate a random identifier to be embedded in the address.

RFC3041 was an implementation standard, which meant that it could be used by implementations (e.g. operating systems like Linux or Microsoft). It could be included in the operating system which would provide choice for the manufacturer to implement or not and for the end user to use or not. Therefore this addressed the WP58 Opinion paper concerns.

Discussion

It was generally agreed that the meeting of the EC IPv6 TF and the Article 29 Working Party had been a good step, that it was important to proceed together. The Article 29 Working Party was in principle willing to enter in a dialogue with the EC IPv6 TF as stated in the Opinion paper. The Article 29 Working Party offered to do some work in the Euro6IX project. There are two deliverables later this year and it was agreed that members of the Article 29 Working Party would have the opportunity of reviewing the document to reach a consensus with the EC IPv6 TF.

8. OTHER ISSUES

We have set out a technical solution to the issue of the unique identifiers in IPv6 addresses, which is the immediate concern regarding the successful deployment of IPv6 in Europe. We hope that it will be implemented in such a wide-scale manner, that it will become de facto mandatory and will solve the problem identified.

However we recommend monitoring this issue to determine whether there may be a need for further non-technical solutions or recommendations to compliment RFC3041. There are currently various recommendations about the roles of various actors in the Internet in relation to data protection and it may be necessary in due course review and update these in the light of the deployment of IPv6

Another area that needs to be reviewed is the applicability of RFC3041 to all types of Internet devices under IPv6 and in particular the issue of third generation cellular hosts. The current recommendation is that RCC3041 should be implemented but again we need to monitor to see whether this in fact occurs.

Finally there is a wider data protection debate than that of the dangers of unique identifiers. This relates to whether any amendments are necessary to the current data protection legislation to deal with the data generated by IPv6, as the Internet Protocol becomes the common communication technology. It may be that the traditional definitions and concepts of traffic and location data do not cover IPv6 (and the Internet's multi layered architecture) adequately. This will form the basis of our second deliverable due in December 2003.

9. SUMMARY AND CONCLUSIONS

The implementation of IPv6 is important to the technological competitiveness of Europe. However whilst the rapid deployment of IPv6 should be encouraged, this should not be at the expense of safeguarding certain important principles.

The right to privacy and the right to data protection are two fundamental rights enshrined in the EU Charter and legislation. The protection of these rights is of paramount importance. Technology moves at a fast rate but the European data protection legislation in place is intended to provide checks and balances to protect privacy whilst allowing the development and deployment of new technology.

On a general level, designers of new protocols are under a duty to bear the privacy and data protection principles in mind and to ensure that new protocols are privacy compliant. One aspect of privacy and data protection is to allow anonymity for citizens, although this principle of anonymity is balanced with the ability to identify people in order to prevent illegal activity.

On a more specific level there are particular rules in relation to the processing of personal data. Personal data means any information relating to an identifiable or identified person, such as for instance data relating to an identification number. It is accepted than an IP address is personal data.

Given that an IP address is personal data, the data protection legislation protects the rights and freedoms of individuals and in particular, their right to privacy with respect to the processing of the IP address.

The use of a unique identifier as part of the IPv6 IP address in stateless address autoconfiguration, without any safeguards would be a potential threat to privacy because the use of the unique identifier as part of the 128-bit address would be a constant identifier threatening the user's anonymity.

The designers of IPv6 foresaw this potential problem and therefore drafted a proposed standard (RFC 3041) as a technical solution. This provides for the unique identifier 64 bit part of the 128-bit address to be replaced by a random number in outgoing communications. This random number can be changed thus resolving the problem of a constant identifier linked to the interface.

This technical solution is a proposed Internet Standard and therefore the success of this technical solution depends on its widespread implementation by vendors. It has already been implemented in Windows XP where you get an RFC3041 addresses for outbound addresses and a global IPv6 address, which can be used to accept inbound connections.

It is strongly recommended that all vendors implement RFC3041 and the fact that some of the most important vendors have already implemented it creates strong peer pressure. Consumer pressure plays an important part in this process.

If the technical solution to the unique identifier provided above is implemented, the conclusion about IPv6 is that it is in many ways safer than IPv4 as it contains in built security systems (such as IPSec).

To ensure that the technical solution is implemented it is important that there is widespread dissemination of the solution in RFC3041 in order to create confidence amongst Europe citizens about the benefits of IPv6 which in turn will assist IPv6 being deployed rapidly in Europe.

Our next task after publication of this paper will be to implement the widespread dissemination of the above in order to promote IPv6 as a Protocol, which, in many ways, has greater privacy features than IPv4.