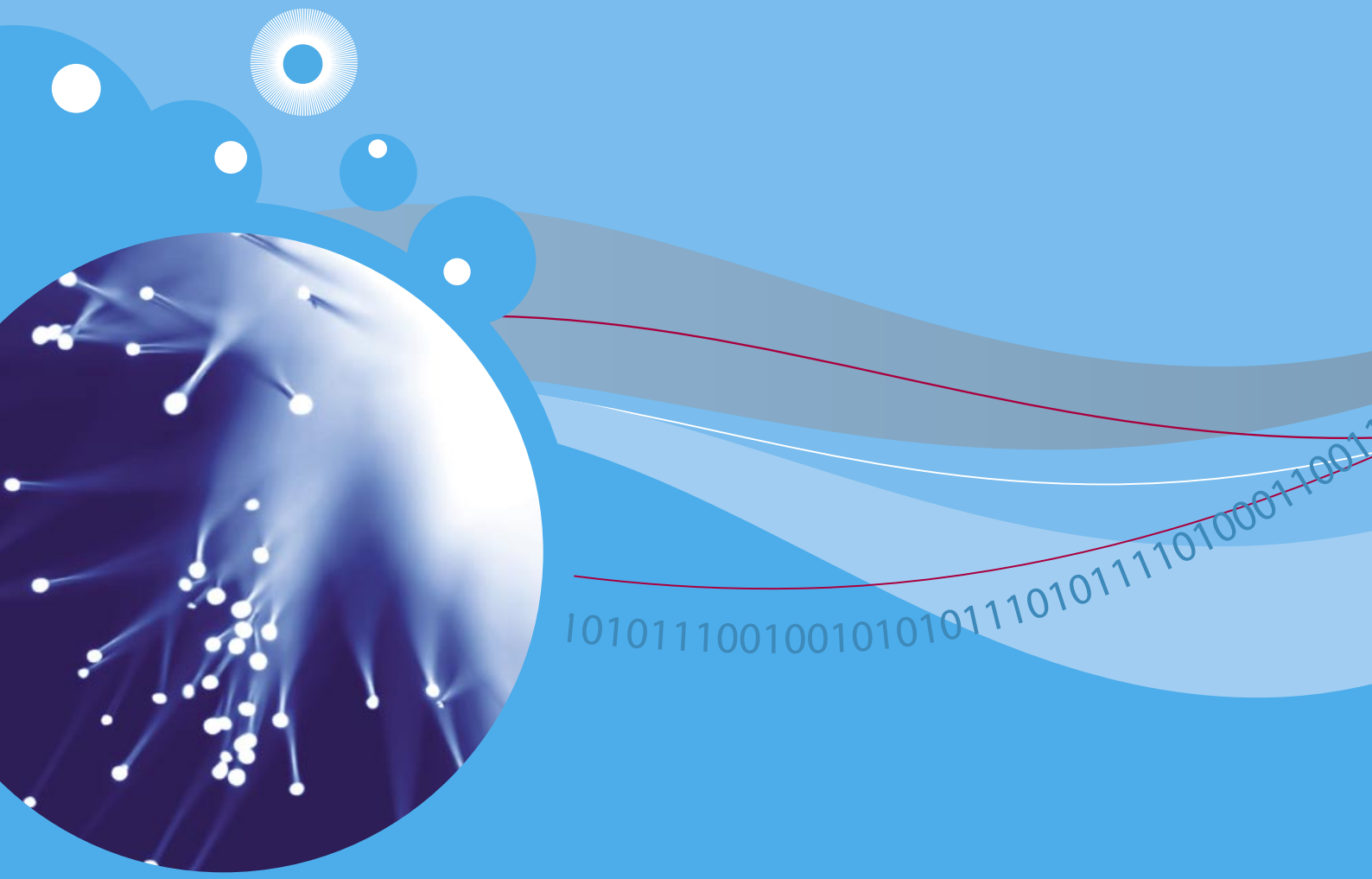


enisa
European Network and Information Security Agency

STOCK TAKING REPORT ON THE TECHNOLOGIES ENHANCING RESILIENCE OF PUBLIC COMMUNICATION NETWORKS IN THE EU MEMBER STATES

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for enquiries on this study, please use the following details:

Technical Department, Security Tools and Architectures Section

Email: sta@enisa.europa.eu

Internet: http://www.enisa.europa.eu/sta/

This study has been prepared by the Security Tools and Architectures Section of ENISA in collaboration with TeraTel GmbH http://www.teratel.ch/ that conducted on behalf of ENISA the data collection activity.

Acknowledgments

The authors would like to express their gratitude to all of the people and organisations that have participated in the various meetings, survey and interviews and without those contributions and dedications this report would not have been completed.

Our appreciation is also extended to the members of the Working Group of leading experts who contributed throughout this activity.

List of abbreviations

ARECI – Availability and Robustness of Electronics Communications Infrastructures

ATM – Asynchronous Transfer Mode

CoS – Class of Service

CPNI – Centre for the Protection of National Infrastructure

DNSSEC - Domain Name System Security Extensions

ENISA – European Network and Information Security Agency

IPTV – Internet Protocol Television

IPv6 - Internet Protocol version 6

KPI – Key Performance Indicator

MPLS - Multi Protocol Label Switching

MTP - Multi-annual Thematic Program

NAT – Network Address Translation

NRA - National Regulatory Agencies

QoS – Quality of Service

SDH – Synchronous Digital Hierarchy

SLA – Service Level Agreement

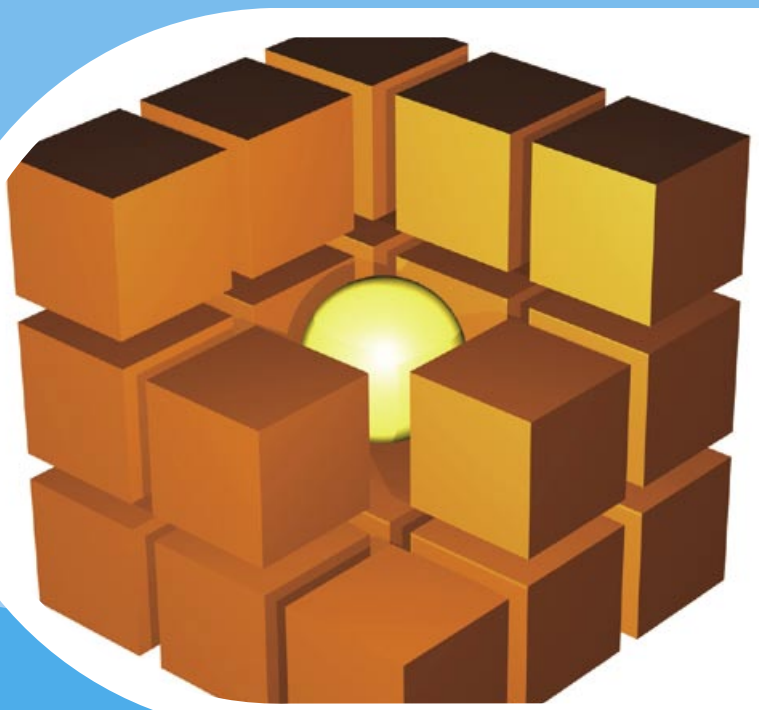
TAR – Trusted Anchor Repository

TLD – Top Level Domain

VPN – Virtual Private Network

WDM – Wavelength Division Multiplex

Contents



1 Executive Summary

1 Executive Summary

Resilience and security of communication networks and services that they support is an issue of critical importance to the EU economy and its citizens as it impacts day-to-day operation of businesses and affecting daily lives of EU citizens. In its reform proposals amending the current regulatory framework[1] (eCommunications Directive) the European Commission recognising the importance of resilience of communications networks and services proposed increased responsibilities for network operators through stronger obligations to ensure security and integrity and the mandatory requirement for breach notifications to National Regulatory Agencies (NRA) and consumers.

Resilience of public communications network is expected to play a major part in driving forward the growth of the EU economy. The ICT sector contributes 25% to the EU's GDP growth and 40% to its productivity growth[2]. In this light, it is of strategic importance to work towards securing European ICT infrastructures in support of EU development priorities. All efforts should be made in order to ensure that growth of the European industry will not be hindered by unreliable and unsecure network access to infrastructures. This is likely to happen if Europe does not put effort in the development and deployment of new, emerging technologies and architectures.

ENISA, the European Network Information Security Agency, recognised this need and launched a programme[3] with the ultimate objective to collectively evaluate and improve the resilience of public communications networks in Europe. In terms of technologies, the deployment of existing and emerging technologies as Internet Protocol version 6 (IPv6), Domain Name System Security Extensions (DNSSEC) and Multi Protocol Label Switching (MPLS) are promising for providing increased network resilience and therefore are under investigation in this survey.

This report presents the results of a survey conducted to a number of service providers in the EU (Annex 2: Interviewee Data) on the state-of-the-art of deployment of those technologies and their impact on improved network resilience. The report also addresses open issues identified by the representatives of the service providers interviewed.

The field of Network Resilience has been attracting increasing attention because it greatly contributes to the quality of services and to the business continuity of systems and processes. Many good practices, regulations and recommendations underline the importance of network resilience for all organisations, especially for those which rely on connectivity of IT systems to implement their business processes.

The purpose of this document is to provide information on and raise awareness of the important topic of network resilience and secure connectivity. Our main objective is to offer a state-of-the-art survey about the plans to deploy and/or experienced and applied impact in terms of network resilience in relation to three technologies, namely IPv6, DNSSEC and MPLS. The following general observations of applied network resilience have been encountered during the survey process:

- missing experience from commercial operation on the features and applications of IPv6 and DNSSEC improving network resilience;
- absence of operational best practices and recommendations in the area of applied network resilience in particular for the upcoming new technologies DNSSEC and IPv6 to facilitate secure communication and connectivity and;

[1] http://ec.europa.eu/information_society/policy/ecomm/library/proposals/index_en.htm

[2] "The Role of ICT in the Economic Growth and Productivity of Andalucia", JRC Scientific and Technical Report, EUR 22781EN – 2007, European Commission, DG JRC-IPTS, http://ftp.jrc.es/EURdoc/22781-ExeSumm.pdf

[3] http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_desig_ver_2008.pdf

- lack of management and coordination between stakeholders, missing information security policies, guidelines and management principles in particular for deployment of DNSSEC.

Based on the survey overview and results presented in this report it is recommended that ENISA:

Ensure resilient connectivity of European organisations. If badly prepared, the integration of the technologies without best practices and expertise on features improving network resilience will present a risk, hinder European growth and therefore reduce the competitiveness of its industry.

Exploit European expertise, best practice and operational experience allowing European industry to benefit from improved resilience ensuring new business opportunities created by the technology integration.

Ensure existence of European trained experts that will allow organisations to benefit from the state of the art innovations in a fair and competitive environment, network resilience being a path to a stabilised and secured Internet and intra-company connectivity while opening the door to a range of new secure applications.

2 About the study

2 About the Study

In the context of its Multi-annual Thematic Program (MTP)[4] the European Network and Information Security Agency (ENISA) http://www.enisa.europa.eu/ aims to evaluate and contribute in the area of resilience of public eCommunications in Europe[5].

In this light, during 2008 ENISA carried out an assessment of the effectiveness of three current and/or emerging technologies, namely MPLS, DNSSEC, IPv6 that have been identified[6] as having the potential to improve the stability and integrity of public eCommunication networks. In addition, a number of deployment success stories were identified and presented.

In order to assess the effectiveness of the above mentioned technologies as well as problems and gaps that could potentially compromise the availability of networks and services, at first instance a number of interviews of network operators in EU Member States were carried out. The analysis of the inputs collected is expected to become input to the preparation of guidelines on the effectiveness of these three technologies especially in terms of their potential to improve the resilience of public networks (but also highlighting their shortcomings). The guidelines produced in the course of 2009 will be primarily addressed towards National regulators and policy makers but also network operators.

The process was carried out in direct consultation with a group of leading experts representing both industry as well as academia and research organisations. The members of the group have contributed to the stock taking through the identification of the main issues, the preparation of the questionnaire and the list of network operators to be interviewed. They also participated in the preparation of the main conclusions of the study on emerging technologies and standards that could potentially improve the resilience of public networks.

The working group comprised of the following members:

Michael Behringer	Cisco Systems
Philippe Bereski	Alcatel-Lucent France
Anne-Marie Eklund Lowinder	.SE
Bosco Fernandes	Nokia Siemens Networks
Thrasivoulos Griparis	WIND
Christian Jacquenet	France Telecom
Dimitrios Kalogeras	National Technical University of Athens
David Kennedy	Eurescom GmbH
Latif Ladid	IPv6 Forum
Richard Lamb	ICANN/IANA
Athanasios Liakopoulos	GRNET
John Markoulidakis	Vodafone Group

[4] http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_desig_ver_2008.pdf

[5] Electronic communications networks used wholly or mainly for the provision of publicly available electronic communications services. Directive (2002/21/EC) on a common regulatory framework.

[6] http://www.enisa.europa.eu/doc/pdf/resilience/ENISA_Workshop_Report_final.pdf

Bertrand Marquet	Alcatel-Lucent France
Arno Meulenkamp	RIPE-NCC
Kari Ojala	Ministry of Transport and Communications, Finland
George Polyzos	Athens University of Economics
Neeli Prassad	CTiF - Aalborg University
Michel Riguidel	ENST – Département Informatique et Réseaux
Christos Siaterlis	European Commission - JRC
Kostas Strakadounas	FORTHNET
Franck Veysset	France Telecom R&D
Theodore Zahariadis	Technical Educational Institute of Chalkida

This study was initiated and supported by the members of the Security Tools and Architectures Section (http://www.enisa.europa.eu/sta/) Slawomir Gorniak, Panagiotis Saragiotis and Demosthenes Ikonomou

3 Survey Methodology

3 Survey Methodology

Unlike consumer surveys, where a sample large enough for statistical analysis is used, in our case we are limited in size of "population" (number of operators) that have different scope of network security issues. Hence, much attention has been drawn to survey planning and development achieving the right coverage, in particular to

- **sample design** (selected operators)
  with respect to the scope of business
- **questionnaire design**
  with focus on few questions with successful answers
- data collection method / interviews
  such as face-to-face meetings, online questionnaire and conferencing.

A specific methodology for this kind of survey was designed covering mainly three phases:

- **survey planning and development** including well defined pre-test in order to achieve high data quality at low risk
- **survey implementation and data collection** including survey and data quality control and if necessary fine-tuning and revision
- data analysis and presentation final reporting including presentation of recommendation.

Phase I: Survey Planning & Development:

The questionnaire (Annex 1: Questionnaire) itself was designed using open questions, giving the interviewed persons the possibility to contribute essentially to the scope of the survey. A first draft of the questionnaire was prepared by ENISA and was used as a basis for discussion within the Working Group. Having received the comments by the members of the Working Group the final version of the questionnaire was prepared by the TeraTel GmbH that also carried the data collection activity on behalf of ENISA.

The operators identified for the interview (Annex 2: Interviewee Data) have been selected on the basis of maximising the coverage of the survey in terms of services offered (wireless fixed, telecommunications, data services, etc.), coverage (operating in more than one countries) and customer base (both corporate and consumer markets). Attention was also given in selecting from the operators interviewed executive decision makers, technology influencers as well as innovators and researchers. In many occasions the members of the Working group provided valuable help in identifying the relevant contact persons and/or through suggestions on operators that could be interviewed.

Phase II: Survey Implementation and Data Collection:

Survey implementation and data collection focused on the execution and operational part of the survey. Starting with operational planning, this phase highlighted data collection and management. Prior to the survey execution, pre-testing of questionnaire was applied in order to assure quality of questionnaire. Another main task for quality assurance was performed using data and sample quality control mechanism.

Phase III: Data Analysis and Presentation:

Data analysis and presentation were mainly focused on data processing and preparation of charts, graphs and tables with the results. Data quality assurance in terms of consistency and integrity was applied.

Within the data analysis itself different methods of evaluating answers have been used. Enumerationand quantification methods have been used as well as weighting methods, quantifying different possibilities by their weight for the interviewee.

4 On Network Resilience

4 On Network Resilience

Any component of a networked service may fail due to equipment failure, human error, or deliberate malice. The growing complexity and inter-dependency of modern network services results into individual failures having widespread and unanticipated results.

BY THE TERMS RESILIENCE WE REFER TO THE ABILITY OF A SYSTEM TO PROVIDE & MAINTAIN AN ACCEPTABLE LEVEL OF SERVICE IN FACE OF FAULTS (UNINTENTIONAL, INTENTIONAL, OR NATURALLY CAUSED) AFFECTING NORMAL OPERATION.

In this context, the main objective of a resilient communications infrastructure is that faults are "invisible" to users in the sense that it may result to degradation in terms of Quality of Service (QoS) but within an accepted predefined range of values that are described in the Service Level Agreement (SLA) between the service provider and the user. The Centre for Protection of National Infrastructure (CPNI) of the UK has published a good practice guide on telecommunications resilience[7].

We can identify five categories of incidents as posing risks to the resilience of communications network:

- ***Flash crowd events:*** Events or situations where large surge of traffic are observed. According to reports by networks operators in the UK the bad weather conditions in the UK early in 2009 led to an increase of mobile network traffic of about 73% while the demand for fixed broadband was also up by 20%.
- ***Cyber attacks***.
- ***Outages to other services affecting the network:*** Among them power and air-conditioning are the most prominent.
- ***Natural disasters***.
- ***System/Logical failings***: The addition of features to the network equipment although improving network maintenance and management increases complexity to a level where the reduced impact of failure of a single component is outweighed by the increased likelihood of failure of the complex whole.

The availability of the underlying transmission and switching/routing equipment is clearly important to the resilience of network services. In this context, a resilient network should aim at removing single points of failure in transmission media and switching/routing equipment. Network availability is thus a risk management issue, as well as involving technical measures such as:

- ***Resilient design:*** Providing multiple paths through networks through the exploitation of mesh networking technologies, the availability of spare capacity via the use of redundant links, load balancing techniques, etc. In all cases, maintaining network visibility and controllability to higher levels is of high importance since network operators need continuously to monitor and manage all the individual paths and components of the network.

[7] "Good Practice Guide To Telecommunications Resilience", March 2006 http://www.cpni.gov.uk/docs/re-20040501-00393.pdf

- ***Resilient transmission media:*** It may sound simple however in many occasions accurate information about physical routing of cables is very hard to obtain. In many cases cross-selling of fibre and ducts is common leading to a situation that it is hard to ensure that paths that in theory are geographically separated are not, in fact, at risk from the same localised incident.
- ***Resilient equipment:*** It is common place for today's high-end switches and routers to include resilience enhancing features such as backup power supplies and in-service ('hot') re-configuration.
- ***The use of technologies that have the potential to improve resilience:*** ENISA has recently published a study on the "Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios"[8]. The study provides an overview of the characteristics of the selected technologies as well as an analysis of their public communication network's resilience enhancing features. Furthermore, a number of deployment scenarios for the technologies are presented.

Finally, the project on the "Availability and Robustness of Electronics Communications Infrastructures (ARECI)[9]" funded by the European Commission investigated the availability and robustness of electronic communications infrastructures.

[8] "Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios", 2008 http://www.enisa.europa.eu/sta/files/resilience_features.pdf

[9] "Availability and Robustness of Electronics Communications Infrastructures (ARECI)", Final Report, March 2007 http://www.publicsafetycommunication.eu/index.php?id=librarypublic&filename=PSCE-RD-024_Annexes.pdf&dir=Reference_documents&task=download&mountpoint=6

5 Network Resilience - Key Survey Findings

5 Network Resilience - Key Survey Findings

5.1 Overview of Interviewees

The selection of interviewed service providers was mainly based on covering a wide and sufficient sample to cope with the requested topics of network resilience focusing on the three technologies IPv6, DNSSEC and MPLS.

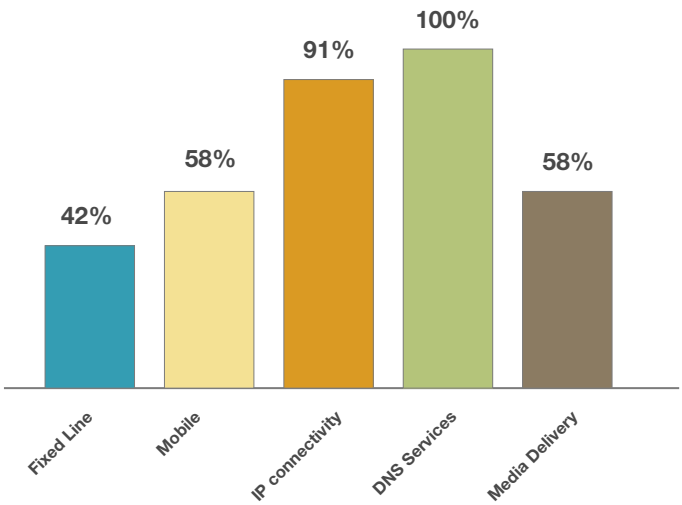
To that respect, the survey was focused on large service providers that have a big footprint in the European telecommunications landscape (and beyond) such Vodafone, WIND, Orange Group – France Telecom, Telenor, Portugal Telecom, OTE, etc. But also innovative and advanced service providers, successful in commercial data network provisioning market targeting for business customers, such as NFSi Telecom, Elisa, .SE, Netnod, and research and academic network providers such as the UK's Education Research Network Ja.net, were interviewed.

Four of them are present in more than 15 countries as well as participate in various associations, partnership programmes and joint industrial/investment ventures in many other countries offering services to a total customer base in the excess of 700 million subscribers. Five of the interviewed operators are extended beyond Europe with presence in North and South America, Asia, Africa and Australia.

Looking over the market profile of the interviewee at a glance, their coverage in terms of markets is presented below

- 42% coverage of fixed line market
- 58% coverage of mobile market
- 91% coverage of IP connectivity provisioning market
- 100% coverage of DNS service provisioning market
- 58% coverage of Media delivery

Figure 1 – **Interviewee profile**



With respect to the customer base of those interviewee, a balanced mix of service providers was selected with a large number of customers (more than 500'000), medium (with less than 500'000 customers) as well smaller (with less than 100'000 customers).

Summarising the mix of customer base, the sample of selected interviewee is represented by

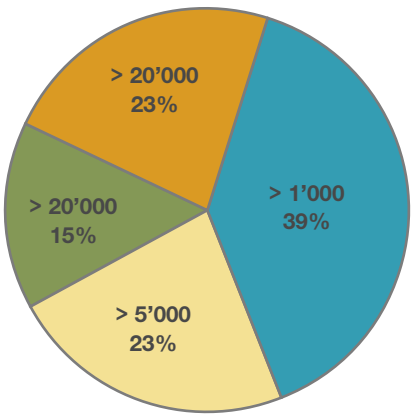
- 58% of operators have a customer base equal or larger than 100'000 subscribers
- 42% of operators with a customer base smaller than 100'000 subscribers

Another criterion used in the selection of the sample of network operators and service providers for the survey was also the number of employees. In this context, particular attention was given to large service providers that employ more than 5,000 employees aiming to obtain feedback from the large players in the telecommunications market.

In this light, the survey sample categorised by number of employees has the following distribution

- 15% of the service provider employ more than 20'000 employees
- 17% employ between 20'000 and 5'000 employees
- 25% employ between 5'000 and 1'000 employees
- 42% employ less than 1'000 employees

Figure 2 – **Interviewee profile**



The sample used in this survey represents a balanced selection of service providers and fulfils all initial requirements for the collection of information.

The interviewed service providers are key players in their markets, leading technology innovation as well as having an influential role in the market evolution.

5.2 Survey Findings on MPLS

The MPLS part of the survey aimed at receiving input on its deployment and use. The latter was investigated in terms of impact on network resilience as well as corporate network resilience strategies. Particular attention was given to:

Deployment status: what is the deployment status of MPLS?

Key driver for deployment: what were the key drivers for MPLS deployment and what were the business drivers for this decision?

Deployment options: which features are used in order to improve network resilience?

Key Performance Indicator: which are the Key Performance Indicators (KPIs) monitored in order to assess the impact of MPLS in terms of network resilience?

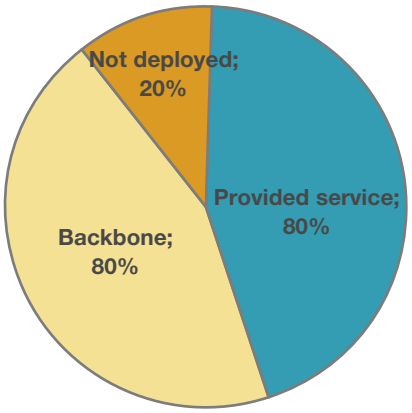
Challenges: what are the challenges posed by MPLS to the networking infrastructure in terms of resilience?

Customer reaction: what are the customers reactions to the introduction of MPLS?

5.2.1 Interviewee Profile & Deployment Status

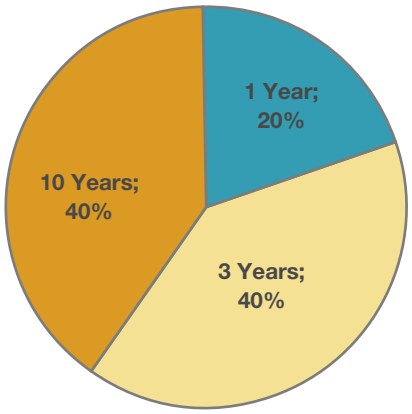
Concerning the market profile of the interviewed operators, almost all of them (91%), as expected, provide IP connectivity to their customers. From those, 80% deploy MPLS in their network infrastructure and at the same time are offering MPLS services to their clients in the form of VPN's (Virtual Private Network) for intra- and intercompany connectivity or WAN (Wide Area Network).

Figure 3. – **MPLS deployment be the surveyed operators**



The majority of the interviewed operators have deployed MPLS for a considerable amount of time. In this context, 40% of them have deployed MPLS for 10 years and another 40% have deployed MPLS for 3 years, while 20% have recently deployed MPLS.

Figure 4 – **Years of experience in MPLS deployment between the surveyed operators**



MPLS IS A WELL DEPLOYED TECHNOLOGY AMONG THE OPERATORS PROVIDING IP CONNECTIVITY

5.2.2 Deployment Options

According to our survey the commercial MPLS service offering is made following different deployment options.

- MPLS deployment over optical WDM (Wavelength Division Multiplex) or GigE (Gigabit Ethernet) backbone
- MPLS deployment using traditional SDH transmission backbone

MPLS can be used to improve resilience in conjunction with other technologies, used to provide protection in all protocols layers. With respect to the lower layer protection scheme most operators depend on the provided transmission network by third party carriers for the planned connectivity. Hence, all possible protection schemes are deployed, such as

- Synchronous Digital Hierarchy (SDH) protection or
- Metro Ethernet protection.

Those protection schemes are used without any preferences depending on the connectivity architecture and available transmission infrastructure. Mostly, underlying transmission protection schemes are used on the basis of Service Level Agreements (SLA) without any knowledge about the scheme.

Furthermore, several MPLS features such as

- Class of service (CoS) tagging and prioritisation
- Fast Reroute
- Traffic Engineering or
- Diffserv aware MPLS Traffic Engineering

that have the potential to enhance the resilience of the provided service are used by operators, although no real preference could have been identified in the course of the interviews.

Some of the operators prefer to apply intensive traffic engineering including Diffserv aware traffic engineering. These are mainly the operators which have already established traffic demanding services, such as IPTV (Internet Protocol Television).

Other service providers, in particular those which are new in the market or do not yet provide traffic demanding services, stated their intention of not to invest significantly in the traffic engineering while putting emphasis on other resilience features.

Fast reroute is used commonly by the operators providing IP connectivity services for corporate customers to meet high SLA requirements.

5.2.3 Key Drivers for MPLS Deployment

With respect to large deployment of the MPLS technology an interesting question remains:

"What are the key drivers for MPLS deployment and whether network resilience is one of them?"

On the basis of the survey, three such key drivers have been identified:,

- Providing in particular to corporate customers their own distinguished WAN-based non-overlapping VPN services.
- Providing distinguished customer networks with various types of service levels through a single platform with lower operating and transmission costs compared to older Asynchronous Transfer Mode (ATM) or Frame Relay platforms.
- Offering high level of security and network resilience by various types of implemented features.

5.2.4 Key Performance Indicators

Key performance indicators have been investigated throughout the performed interviews. Main attention has been drawn to KPIs of improvement of the network resilience in terms of service availability, security and guarantied quality of service.

Most of the surveyed operators use the overall network availability over one month period in order to assess their networks. During the survey we experienced difficulties in obtaining data concerning network availability since most corporate policies forbid the disclosure of such information mainly due to marketing reasons. During the study all interviewed service providers stated that they have observed:

- Increased network security for their corporate customers
- Increased MPLS dependent service availability
- Increased service guaranty up 99.999% (target 99.99999 %)
- Decreased round trip time for their networks leading to improved performance for applications and less timeouts occurring in the network, thus, improving network resilience.

MPLS DEPLOYMENT SIGNIFICANTLY INCREASES THE RESILIENCY OF NETWORKS

5.2.5 Challenges

The interviewed operators were also asked about the challenges they are confronting in relation to the deployment of MPLS and using its resilience enhancing features.

In this context, all interviewees stated that they do not see any major challenges to the networking infrastructure. In this light, MPLS is considered as a mature technology in particular in relation to its features enhancing resilience.

5.2.6 Customer Reaction

During the interviews, the interviewees presented their experience with MPLS service delivery to the customer. In common agreement all interviewed operators stated that:

- business customers demand MPLS in order to receive improved resilience and security
- customer feedback is positive, judging from the reduced numbers of complains being submitted and "trouble ticketing" reported.

5.2.7 Conclusions

Based on the aforementioned results on interviews with network operators about the subject of improved network resilience in IP networks by deploying MPLS, it is possible to draw the following conclusions:

- MPLS is deployed already for some years and is well known and established technology.
- MPLS improves network resilience significantly.

MPLS deployment is mainly driven by customer demand for improved resilience

5.3 Survey Findings on IPv6

On the subject of IPv6, the survey aimed at receiving information as well as concrete figures about the deployment and usage of IPv6. In terms of usage the survey investigated the impact of IPv6 on network resilience as well as corporate network resilience strategies. In this light, the survey comprised of the following sections:

- **Deployment status:** what is the deployment status and, in the case it is not yet deployed, what are the future plans for deploying IPv6 technology;
- **Key driver for deployment:** what are the key drivers for IPv6 deployment and the business rationale that leads to this decision;
- **Deployment options:** what kind of transition scenario(s) are envisaged for IPv6 deployment and what kind of architecture is used;
- **Key Performance Indicators:** what are the KPIs identified in order to assess network performance in terms of its resilience;
- **Customer reaction:** what is the customer reaction to the introduction of IPv6.

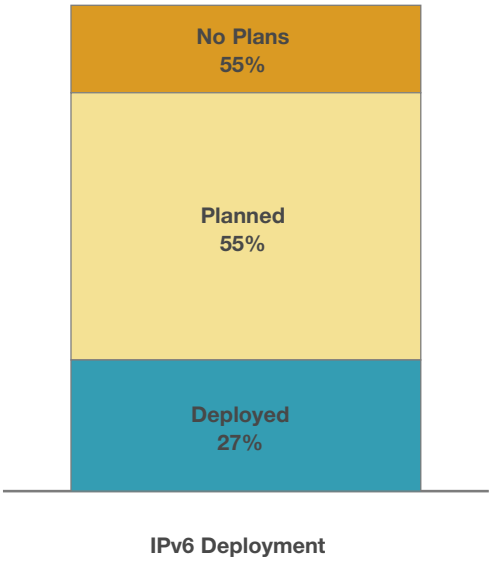
5.3.1 Interviewee Profile & Deployment Status

The survey indicated that all of the interviewed service providers are familiar with IPv6, although significant differences were observed in their perception of the opportunities given by this technology and their future plans either in deploying it or in testing in laboratory environment.

Some of the interviewed service providers have concrete plans of using IPv6 in their internal networks (or are already doing so), while others plan to connect new customers exclusively through IPv6 in the near future (by 2010).

The decision by service providers to deploy IPv6 is driven by a variety of, sometimes contradictory, reasons. Their approach differs in the way of considering IPv6 – where some of them have concrete time aligned projects, other monitor their competitors and wait for them to make the first step..

Figure 5 – **IPv6 deployment status**



The result of the survey and the analysis that followed indicates that:

27% of interviewed service providers already offer commercial IPv6 network services and use IPv6 in their internal network.

55% plan to deploy it commercially within 3 years.

18% declared no interest in IPv6 technology within 3 years.

82% HAVE ALREADY DEPLOYED OR DO HAVE PLANS TO DEPLOY IPV6

Most IP-service providers either already deployed or consider deploying IPv6 technology in their networks within the next three years.

5.3.2 Key Drivers for IPv6 Deployment

It is broadly known that the introduction of IPv6 was planned a decade ago because of the shrinking of available address space. In the meantime turnarounds such as Network Address Translation (NAT) entered into broad usage alleviating, at least temporarily, the pressure of Internet users to adopt the new technology.

In the context of the survey, four main drivers for the introduction of IPv6 have been identified by the interviewed service providers. These are:

- the increasing demand on IP address space;
- customer demand for IPv6 (based on providers' poll results);
- improvement on network resilience; and
- introduction of technical innovations.

"IPV6 DEPLOYMENT TODAY IS MAINLY DRIVEN BY INCREASING DEMAND ON IP ADDRESSES SPACE"

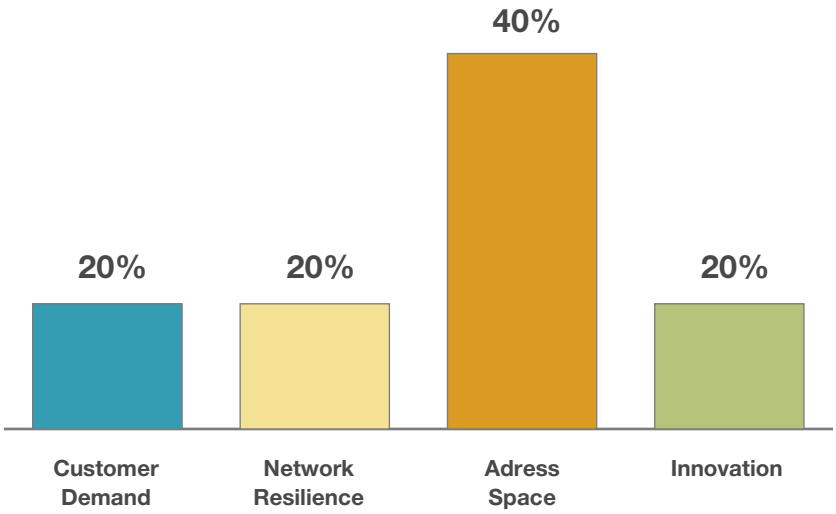
It is of worth to point out that in this part of the survey only the answers of service providers that are deploying IPv6 or plan to do it in the next 3 years were taken into account. Moreover, service providers were allowed to identify more than one "key driver" in their responses. In this light it has been found that:

60% of respondents indicated that the main driver for introducing IPv6 is the reduction of available IPv4 address space.

20% received a positive input or even demands of customers for introducing IPv6.

For 20% an important reason was enhanced network resilience, and the same amount of respondents indicated introduction of technical innovation.

Figure 6 – **IPv6 deployment drivers**



The responses to our survey clearly indicate that improved network resilience through the introduction of IPv6 is not perceived as a business driver by the majority of service providers. Most service providers do not focus on improving network resilience with IPv6, do not put any emphasis on its resilience improving features or even do not have any operational experience to what extent network resilience can be improved through its introduction.

Moreover, customers demand for IPv6 technology is not yet about to reach the critical mass for operators. New IPv6 services and benefits to the users are not really seen by the interviewed companies.

The main driver behind the introduction of IPv6 remains the demand of additional IP address space.

5.3.3 Deployment Options

The deployment of IPv6 in the backbone network can be performed following different technical approaches.

Following on non quantitative interviews in this area it was discovered that responders have shown specifically three deployment options already used or considered:

- Dual stack routers/links;
- Tunnelling IPv6 over IPv4/MPLS;

In most cases the chosen option is the use of dual stack routers throughout the network. However, service providers that have extensive MPLS deployments, choose to use dual stack routers on the edges and tunnel IPv6 in the core of their network.

5.3.4 Key Performance Indicators

Key performance indicators (KPI) have been investigated during the performed interviews. Main attention was placed at identifying KPIs which do improve network resilience

The responses of the interviewees indicated that:

- No real improvement in terms of network resilience is expected;
- KPIs for resilience in IPv6 networks were not considered so far due to the lack of operational experience;

- KPIs for resilience in IPv6 networks are not measured because there was no such focus during the planning and deployment process (no need of doing so).

Still the deployment of IPv6 is at the very early stage and operational experience is not established yet. Hence, KPIs for improving network resilience are not measured and are not really the focus of today's IPv6deployment.

Furthermore, features of IPv6 for improving network resilience are not really known nor do have service providers the experience or need to use those features at operational level. A significant number of service providers do not notice the added value of IPv6 in respect to the resilience of the network.

5.3.5 Customer Reaction

During the survey, the interviewed service providers presented their experience with IPv6 service delivery to their customers. The results of the interviews showed that:

- Customer polls conducted by network operators indicate that the number of customers asking for IPv6 services is estimated below 40%;
- There is no real customer feedback, neither positive nor negative, concerning improved resilience of their network using IPv6.

"IPV6 INTRODUCTION LACKS OF CUSTOMER DEMAND"

Because of the low number of commercial customers with IPv6 implementations, it is not possible to accurate classify and quantify their feedback at the moment.

5.3.6 Challenges

While the survey focused on investigating the perception of the service providers on network resilience enhancement through the deployment of IPv6, several interviewees identified challenges to the deployment that are worth to mention.

Management of the security in an environment where end-to-end connectivity has been restored is a challenge. Although as already identified in the drivers for IPv6 deployment section, the restoration of end-to-end connectivity will enable new and innovative services to operate efficiently.

Another challenge is the lack of experience in running IPv6 networks in comparison with the more than 20 years of experience with IPv4, depicted in IETF Request for Comments (RFC) and standards. That experience helps in identifying and resolving problems and keeps the internet running.

5.3.7 Conclusions

Based on the aforementioned results on interviews with service providers about the subject of increasing public eCommunication networks resilience in upcoming or already commercialised IPv6 service networks, we can draw the following main conclusions:

- IPv6 deployment is on track with EU initiatives on IPv6;
- IPv6 deployment is mainly driven by the increasing demand on IP address space;
- Network resilience is not the business driver for the introduction of IPv6;
- No improvement of resilience has been observed after introducing IPv6;
- No KPIs have been defined;
- The introduction and deployment of IPv6 lacks of experienced best practice;
- Customer demand for IPv6 is at a low level.

5.4 Survey Findings on DNSSEC

The aim of the interviews was to gather information as well as concrete figures about the deployment and usage of DNSSEC. In terms of usage we mainly investigated the impact of DNSSEC on public eCommunication networks resilience as well as corporate network resilience strategies. In this respect the main interests of the interviews conducted were the

Deployment status: what is today the level deployment of DNSSEC and, if not yet deployed, what are the future plans.

Key driver for deployment: what are the key drivers behind the decision to deploy DNSSEC, including business drivers.

Deployment options: in which services of the DNS has DNSSEC been deployed or is planned to be deployed and what policies have been implemented.

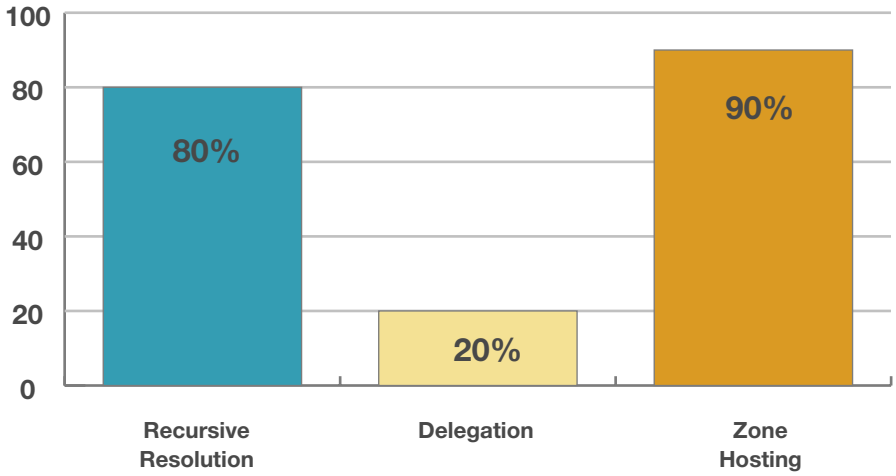
Key Performance Indicator: what are the Key Performance Indicators (KPI) measured and what is the experience in terms of improving or not the resilience characteristics of networks.

Challenges: what are the new challenges to the networking infrastructure in terms of resilience.

Customer reaction: what is the customer reaction to the introduction of DNSSEC.

5.4.1 Interviewee Profile & Deployment Status

Figure 7 – **DNS services offered by interviewees**



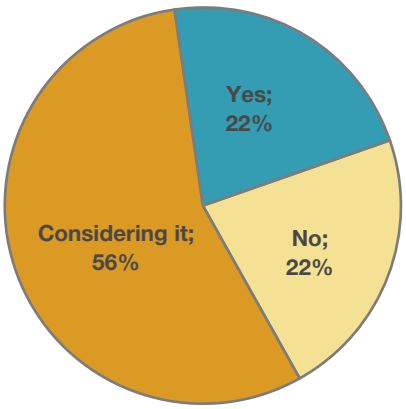
Concerning the profile of the interviewed operators, all of them, as expected, provide DNS services to their clients. DNS is a fundamental service in internet communications and it is used practically in every initiation of communications. The differentiation occurs on the specific DNS services offered by the surveyed operators that are aligned with their main line of business.

In this light, 80% of the interviewed operators provide Recursive Resolution of domain names to their clients, a typical task of internet service provider and every operator that provides IP connectivity to their client. Zone hosting is offered by 90% of the interviewees. This service is offered either as an autonomous one or in combination with other services like web-hosting. Most of the surveyed operators have such a service offering. Delegation is a service

that is provided by specialised companies that are most of the time registries of a Top Level Domain (TLD). 20% of the interviewees provide delegation DNS services.

The sample of the operators interviewed covers the full range of services that are provided through DNS. The distribution of the operators ensures the neutrality of the results in regard to polarisation due to specific service offerings.

Figure 8 – **Deployment of DNSSEC between operators**



From the interviewed operators, 22% do not plan to deploy DNSSEC in the next 3 years. The main reason for this decision seems to be the lack of customer demand for the service. Other reasons are the cost of deployment and the on-going costs for running the service. The immaturity of the technology was also mentioned as a potential reason with a negative effect in terms of the resilience for the DNS service currently offered by operators. Finally, one other reason against the deployment of DNSSEC is the lack of requirement set to operators by National regulators.

On the other hand, 22% of the operators participating in the survey have already deployed DNSSEC in their DNS services while the majority of the interviewed sample, 56%, is considering deploying it within the next three years. The main driver for deploying it as well as for considering its deployment is the improvement in the resilience of DNS. The introduction of DNSSEC is expected to build reliability in the systems as well as to enable the detection of cases where someone is tampering the DNS information. In this context, all the operators interviewed expressed their commitment to provide secure services that their clients can depend on. The early adopters among them were also driven by their desire or drive to advance the state-of the-art of the technology offered to consumers and to contribute to its establishment.

78% OF THE OPERATORS HAVE PLANS TO PROVIDE DNSSEC SERVICES WITHIN THE NEXT 3 YEARS

5.4.2 Key Performance Indicators

Key performance indicators have been investigated during the interviews with the providers. Particular attention was given to the KPIs which indicate improvement of network resilience in terms of security and service availability.

On DNSSEC the majority of the interviewee stated that

- KPIs for resilience in DNSSEC service provision were not considered so far due to the lack of operational experience.

- KPIs for resilience in DNSSEC service in particular security issues such as avoided attacks are hard to measure.
- KPIs regarding the resilience of the DNS service are expected to improve through the introduction of DNSSEC.
- Regarding the overhead that the technology is putting to the DNS infrastructure, there was a small decrease observed in the performance of the service due to the increase of the amount of the data transferred.

The operational experience of DNSSEC deployment is pretty scarce. In this context, best practices are not established yet. The interviewed operators that either deployed or consider deploying DNSSEC agree that the resilience of the DNS service is expected to increase.

Since the deployment of the technology is in its early stages, some operators are still at the phase of gathering statistics on the existing islands where DNSSEC is deployed and on the number of the resolvers that try to validate zones.

5.4.3 Challenges

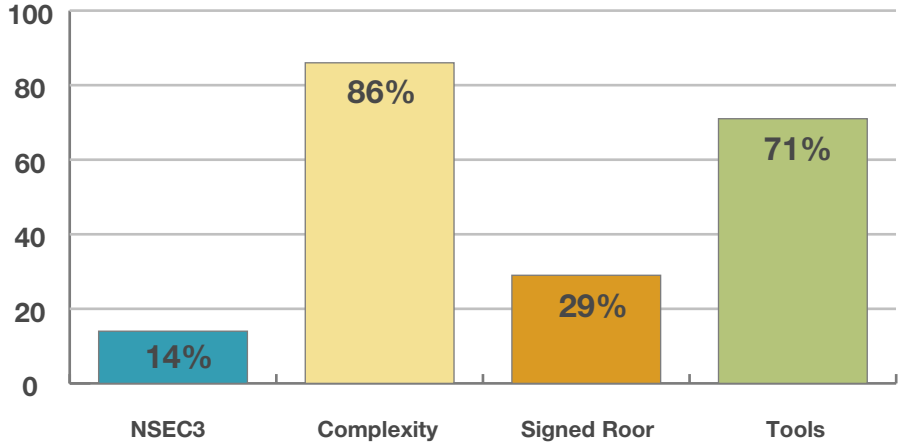
In this part of the survey the service providers were asked on barriers they have faced or are expecting to face in relation to the deployment of DNSSEC. In the context of this question, the impact of DNSSEC on network resilience in its wider sense was discussed.

All interviewee providing or considering DNSSEC as a potential future service have identified:

- Problems with the complexity of Key Management and Key Rollovers.
- Lack of supporting tools for Key Management as well as operational management of DNSSEC servers.
- Problems with increased system complexity of DNSSEC servers. In this respect, it has also been noted that in some cases equipment vendors deliver unstable products for DNSSEC support.
- Essential lack of key management policies as well as in a wider scope lack of information security policies with focus on DNSSEC and security management guidelines.
- Lack of end user awareness on the benefits provided by DNSSEC and the security it provides.
- There are no widely used applications that are supporting DNSSEC.
- The root of the DNS is not signed. This breaks the hierarchy of DNS and Trust Entry points (Trust anchors) have to be configured to the recursive resolvers.
- The distribution and update of the trust anchors is not standardised and there are no common policies and procedures yet in place.
- There is lack of standardisation in the transfer of the key material from the child domains to their parents.
- There is lack of tools notifying the user when the domain they are using is securely validated.
- The inherent feature of DNSSEC for authenticated denial of existence allows an abuser to enumerate the contents of a zone. The adoption of a variation of the protocol, named NSEC3, by the product vendors is required.

"BESIDES CLEAR NETWORK RESILIENCE IMPROVING FEATURES, DNSSEC IS STILL AT THE BEGINNING OF DEPLOYMENT AND LACKS TOOLS AND POLICIES"

Figure 9 – **Challenges to the deployment of DNSSEC**



Summarising the feedback received by the interviewees we observed that 86% of them have identified the complexity of deploying DNSSEC as a challenge. The complexity for the operators of signed zones and delegating services comes from the lack of tools for automating their operation. For those that provide internet connectivity and validating resolution services, the complexity comes from the lack of a signed root combined with the lack o common policies for Trust Anchor distribution and update.

71% of the interviewees identified the lack of tools for both operators and end users as a challenge for its deployment while 29% identified the lack of a signed root as a barrier. The deployment of DNSSEC in the root is also seen as a major driver for the wide deployment of the technology.

Finally, 14% of the operators are seeing the delay in the introduction of NSEC3 as a challenge to the deployment of DNSSEC. NSEC3, which prohibits the enumeration of the zone, is seen as a prerequisite for the deployment of the technology in registries where a provision against zone enumeration is in place.

5.4.4 Customer Reaction

During the interviews, the service providers discussed their experience with DNSSEC service delivery to their customers. The consensus view was that,

- There is no customer awareness of improved resilience in particular in terms of security;
- In most cases customers adopted the DNSSEC service quickly and easily once they became familiar with its benefits;
- Tools and applications are missing to support the customers daily operational work;

"DNSSEC IS STILL AT AN EARLY STAGE OF CREATING CUSTOMER AWARENESS AND DEMAND"

DNSSEC is well on track for wide deployment but the number of signed zones is not significant enough to make a difference by the security and trust offered by those zones. The number of deployments by customers as well as customer demand for it is not very high mostly due to the lack of customer awareness. DNSSEC needs to receive more attention and visibility in order to be deployed massively.

5.4.5 Conclusions

Based on the aforementioned results of the interviews with operators in regards to improving the resilience of public eCommunication networks with upcoming or already deployed DNSSEC extensions to the DNS service, we are driven to the conclusion:

- Operators agree that the deployment of DNSSEC provides essential improvement to network resilience and in particular to network security.
- Information security policies focusing on DNSSEC security guidelines, key management and recommendations are missing.
- Tools are missing for easy deployment of DNSSEC on all services that comprise the DNS.
- Customers adopt easily and quickly DNSSEC after getting familiar with its improved resilience features.

5.5 Survey Findings on Regulations

In parallel with investigating the views of European service providers on the potential of MPLS, IPv6 and DNSSEC to improve the resilience of communications networks infrastructure, this survey aimed at gathering information on the regulatory environment and incentives given to service providers in regard to the deployment of these technologies. In this context, a particular interest to this part of survey presented:

Regulatory requirements: what are the regulatory requirements on within their home country as well as in other EU member-states?

Effectiveness of regulations: are the existing regulations in their views sufficient, to what extent further incentives are needed?

5.5.1 Regulatory Requirements

The consensus among the interviewed service providers is that there is no need for a regulatory intervention for the deployment of any of the three technologies of interest.

The survey responses clearly indicate that a healthy and competitive electronic communications market can only exist with a minimum regulatory intervention.

Against this background, the most frequent responses received by the interviewed service provided are summarised below:

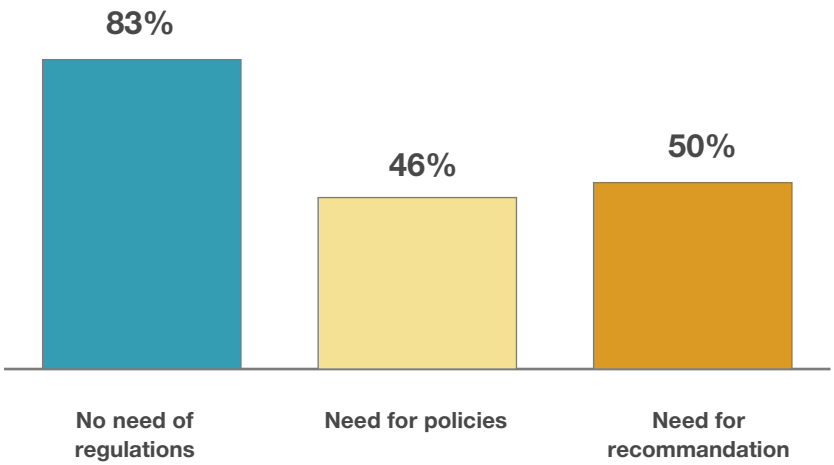
- Regulations only where and if necessary;
- Minimum intrusive regulation with minimum regulatory costs;
- Regulation respecting competition laws, opting for ex-post instead of ex-ante regulation;
- Regulatory interventions must promote investment and innovation.

"THE INTERVIEWED SERVICE PROVIDERS AGREE THAT FOR THE TECHNOLOGIES UNDER INVESTIGATION IN THIS SURVEY REGULATORY INTERVENTION IS NEITHER NEEDED NOR JUSTIFIED."

The interviewed service providers consider that guidelines on deployment and operational management practice (please refer to the previous sections with the survey findings on DNSSEC, IPv6 and MPLS) might, in some cases, help network operators with the introduction of these technologies in their networks.

5.5.2 Incentives, Policies and Recommendations

As already mentioned in the previous section, the majority of the interviewed service provider stated that there is no need for further regulatory intervention.



At the same time a significant number of the surveyed service providers identified the need for further policy actions as well as guidelines and recommendations relating to the deployment of especially DNSSEC and IPv6. In particular

46% of the interviewees identified the need for policy actions in favour of the deployment of DNSSEC as well as information security policies for upcoming security management.

54% of the interviewees identified the need for recommendations, security practices and best practice guidelines relating in particular to IPv6 as well as DNSSEC deployment, management and operation.

"A SIGNIFICANT NUMBER OF THE SURVEYED SERVICE PROVIDERS IDENTIFIED THE NEED FOR FURTHER POLICY ACTIONS AS WELL AS GUIDELINES AND RECOMMENDATIONS RELATING TO THE DEPLOYMENT OF ESPECIALLY DNSSEC AND IPV6"

5.5.3 Conclusions

Based on the aforementioned results on interviews with service providers about the subject of network resilience in upcoming or already commercialised IPv6, MPLS and DNSSEC service networks, it possible to draw the main conclusions:

- Regulatory intervention either at national or EU level was not considered necessary.
- Existing regulatory environment is seen to be adequate
- The need for information security policies, security practices and best practice guidelines relating in particular to IPv6 as well as DNSSEC deployment, management and operation was identified.

6 Recommendations

6 Recommendations

6.1 IPv6

The shortage of available public addresses is a fact concerning Internet Protocol version 4. Although expert views on the date when shortage of available IPv4 addresses will occur varied over time, there is now a consensus predicting that this will occur by 2011-2012.

Among the variety of possible options, the one aiming at supporting the IPv6 adoption in Europe through a set of measures is the one which is likely to bring the greater benefits for Europe for both the economy and society. These actions should address: common IPv6 connectivity availability, awareness of IT managers, network security during the integration, availability of a sufficient pool of trained people and proper exploitation of European expertise.

A more pro-active solution is the launch of the targeted actions by ENISA aimed at supporting and encouraging resilient IPv6 networks in Europe. Such a solution would allow a broader range of actions to be encouraged at various levels. Referring to the survey results mentioned in previous chapters as well as the operational objectives of ENISA, the most prominent directions and recommendations are listed below:

- Ensure that service providers, network operators and IT managers are made aware of the resilience features of IPv6;
- Ensure existence of a sufficient pool of IPv6 trained people;
- Encourage proper exploitation of European expertise on IPv6 resilience features, in particular in best practice and operational excellence on network resilience

6.2 DNSSEC

DNS is one of the essential protocols on the Internet. It is used in almost every interaction that uses names and identifiers: Email, Web, SIP based Voice over IP, Spam filtering, Instant messaging, and many more. Yet the DNS system has not been designed with security in mind; over 3 decades ago, availability and scalability where the important components to focus on. Given that the DNS is the largest distributed database on the Internet one could claim that the protocol designers were successful.

The fact that essential components in the DNS architecture called caches are subject to so called "poison attacks" has been known for almost 2 decades now. As a result of a cache poisoning attack, malicious web sites can be presenting at the request of well known site, e-mails can be redirected and copied before they are delivered to their final destination, voice over IP calls can be tapped by third parties, and - given the circular dependency of the certification on the DNS - SSL certificates may not be as protective as one would hope.

DNSSEC can deal with cache poisoning and a set of other DNS vulnerabilities such as "man-in-the-middle" attacks and data modification in authoritative servers. Its major objective is to provide the ability to validate the authenticity and integrity of DNS messages in such a way that tampering with the DNS information anywhere in the DNS system can be detected. Unfortunately it is because of the distributed nature of the DNS that DNSSEC needs to be deployed by a significant number of DNS zones before it becomes useful. Custodians of the DNS infrastructure such as Top Level Domain registries and the root zone should provide a breeding ground on which DNSSEC can take off, while ISPs and enterprise DNS administrators prepare their DNS infrastructure to validate signed data.

Obviously this is not going to be a project with immediate return on investment; it is a long term strategy to allow us to increase the trust in the Internet.

In 2009, ENISA will continue investigating possible ways for enhancing the resilience of public eCommunication networks, not limiting itself to technologies, architectures and protocols. In this context, incentives (on market and/or policy related aspects) will also be considered with a view on their impact on business practices and the associated regulatory framework.

Referring to the survey results mentioned in previous chapters as well as the operational objectives of ENISA, some directions and recommendations are detailed here:

- Ensure that service providers and network operators are made aware of the resilience features of DNSSEC;
- Ensure existence of a sufficient pool of DNSSEC trained people;
- Encourage proper exploitation of European expertise on DNSSEC resilience features, in particular in best practice and operational excellence on network resilience;
- Encourage key management policies as well as in a wider scope;
- Ensure information security policies with focus on DNSSEC security guidelines and security management principles;
- Promote coordination and alignment of security management between service provider within the EU member states;
- Encourage the development of DNSSEC deployment recommendations;
- Promote distribution of best practice and operational experience in DNSSEC business.

7 Case Studies of Deployment Scenarios

7 Case Studies of Deployment Scenarios

During the survey, the interviewed service providers were also asked whether concerning any of the three networking technologies under investigation (i.e. MPLS, DNSSEC, IPv6) in this study they could identify one or more issues (success or even failure story) that in their opinion could be the subject of a case study.

In this context, the surveyed service providers were requested to highlight how the introduction of any of these three technologies improved the operation of their networks and as a consequence created new business opportunities by improving their market offer.

7.1 .SE - DNSSEC Deployment in Sweden

As the world's very first Top Level Domain, Sweden offered DNSSEC as a service10 for the .se ccTLD. In 1999 they started by running a project that led to signing the .se zone in September 2005. After a quiet period of three months, they released several test domains with signed delegations. Since everything proceeded as planned, the key administration was gradually integrated into the existing registry system, and domain name holders were themselves able to administer their DNSSEC keys through "Keyman", a secure key management system developed in-house.

In February 2007, DNSSEC was launched as an additional service to domain holders through services from some of .SE's registrars. The aim was that .SE's DNS service should be not only highly robust and available, but also trustworthy. .SE's vision for 2011 is that DNSSEC shall be a natural part of the DNS, used by all important .se domains and supported by several applications.

Systems, security policies, and routines for key management and signing of the DNS data, have to be developed. When .SE developed its service, the main goal was to maintain the high availability on its ordinary DNS services and at the same time get a highly secure new DNSSEC service. Since no suitable software was available for key management and zone signing at that time, .SE was forced to develop its own system.

Another challenge for .SE – being a pioneer in this area - has been to get the market for DNSSEC started. Back in 2006, .SE did a market survey among .SE registrants and found a very positive attitude towards the use of DNSSEC technology. This attitude has been confirmed in the ongoing contacts and discussions with registrants since then.

In the beginning of 2009, .SE introduced a new business model for the domain name registration, starting by providing the DNSSEC service free of charge. This new model, among other things, raised the number of signed zones in the registry[11] to more than 1500. The number of registrars that offer the service rose to 11 and the majority of the large service providers are validating signatures in their resolvers.

The real value of DNSSEC is obtained when Internet users actually validate answers from DNS lookups, to ensure that they originate from the right source and have not been altered in transit. Validation can be handled in different ways. A common alternative is that the validation should be performed by the end user's application and that the end user should be informed of the result -- similar to the small padlock icon that is shown in the web browser, when a secure SSL session is established. Already applications exist that perform DNS lookups together with DNSSEC validation, but DNSSEC is not yet supported by most widely adopted applications.

[10] http://www.iis.se/en/domains/sednssec

[11] http://www.iis.se/en/domains/statistics

.SE will continue its work on making DNSSEC a natural part of DNS, used by all important .se domains and supported by useful applications. In an effort to achieve this, they continue contributing to the development of the market, systems and applications. The market development comprises of activities stimulating their registrars to offer DNSSEC services and to promote the use of DNSSEC tools among DNS Name Service Providers. Together with other TLDs, they will also continue their system development, with the aim to make key management and the zone signing process easier and more effective. Finally, they also promote applications that benefit greatly from using DNSSEC.

AS ONE OF THE VERY EARLY ADOPTERS OF DNSSEC, .SE PURSUED THE DEPLOYMENT OF THE TECHNOLOGY IN SWEDEN AND SUCCEEDED IN HAVING THE MAJORITY OF THE LARGE ISPS VALIDATING SIGNATURES.

7.2 France Telecom-Orange – IPv6 Deployment

Orange[12] is the key brand of France Telecom, one of the world's leading telecommunications operators.

The Group has a customer base of more than 182 million customers in 30 countries. Orange, the Group's single brand for Internet, television and mobile services in the majority of countries where the company operates, now covers 123 million customers. At the end of 2008, the Group had 122 million mobile customers worldwide and 13 million broadband internet (ADSL) customers in Europe.

France Telecom-Orange is the number three mobile operator and the number one provider of broadband internet services in Europe and, under the brand Orange Business Services, is one of the world leaders in providing telecommunication services to multinational companies.

The Group's strategy, which is characterized by a strong focus on innovation, convergence and effective cost management, aims to establish Orange as an integrated operator and benchmark for new telecommunications services in Europe. Today the Group remains focused on its core activities as a network operator, while working to develop its position in new growth activities. To meet customer expectations, the Group strives to provide products and services that are simple and user-friendly, while maintaining a sustainable and responsible business model that can be adapted to the requirements of a fast-paced and changing eco-system.

The group has more than 10 years of experience through experimental deployment of IPv6. They have started back in 1995 with the first available routers and host software. In 1997 they got their first interconnection through 6bone. An IPv6 prefix has been enquired and allocated to them by RIPE13. In 2005, they have started experimenting with the French interconnected IPv6 backbone. Their main target was to evaluate the different available tunnelling techniques in order to decide the one they will use to provide services to their customers.

FT-Orange is now deploying IPv6 having two main drivers. Their first driver is the depletion of IPv4 addresses and the impact it will have on their business. Their second driver is their internal corporate network connectivity. The group has many affiliated companies and they want every employee, wherever he/she gets stationed, to be able to connect to the corporate network and services without any constraints posed by the infrastructure. This will happen by restoring the end-to-end connectivity of the network and removing gateways like NATs.

FT-ORANGE WILL PROVIDE BY 2010 INTERNET CONNECTIVITY, VOIP AND IPTV OVER IPV6.

Taking into account their existing infrastructure, they shaped their deployment strategy which will be rolled out in three phases starting in 2008. By the end of 2010 they will offer internet connectivity, VOIP and IPTV over IPv6. FT-Orange has already deployed MPLS in its core network and thus chose to use 6(V)PE with dual stack routers to provide IPv6 connectivity to their customers over their MPLS backbone. CPE devices will be assigned with global IPv6 prefixes and will also be able to dynamically allocate private IPv4 addresses to IPv4-only terminals. Connectivity with the global IPv4 internet will be achieved through carrier grade NAT (Network Address Translation) devices.

FT-ORANGE WILL BUILD ON THEIR EXISTING INFRASTRUCTURE TO PROVIDE THEIR SERVICES OVER IPV6.

[12] http://www.orange.com/en_EN/

[13] http://www.ripe.net/

FT-Orange's IPv6 deployment program.

- Phase 1, "Introduction", started 2008: Basic design recommendations for addressing, management policies, forwarding and routing policies for network devices and customers. Also, they will assess the impact of introducing IPv6 on their information system. The offering at the end of this phase will be restricted to the Internet service.
- Phase 2, "Migration", 2009 - 2010: They will investigate the IPv6 instantiation of the whole range of advanced service offerings, including VOIP and IPTV.
- Phase 3, "Production", 2010 and beyond: Every new customer will be provisioned with an IPv6 prefix and all their offered services will be provided over IPv6.

8 Annex 1: Questionnaire

8 Annex 1: Questionnaire

Introduction

Name of your organization:

Country:

Contact person:

Email:

Phone:

Number of employees: ○ < 1.000 ○ < 5.000 ○ <10.000 ○ <20.000 ○ >20.000

Number of employees in R&D department: ○ < 100 ○ < 1.000 ○ <5.000

Do you operate in several countries through subsidiaries, participation in other operators?

○ Yes

○ No

If yes, in how many countries do you provide services?

How many subscribers does your organization have? ○ <100.000 ○ <500.000 ○ >500.000

Services provided by your organization:

☐ Fixed Telephony

☐ IP connectivity

☐ DNS Service

☐ Mobile communications

☐ Media delivery (e.g. IPTV)

☐ Other. Please specify:

8.1 Regulations

<table>
<tr><td colspan="2">In your home country, are there any regulatory requirements or/and incentives for the deployment of any of the three technologies of interest to this study?

○ Yes. Please elaborate:
○ No.</td></tr>
<tr><td rowspan="2">Yes</td><td>Do you consider that these regulatory requirements or/and incentives were effective?

○ Yes.
○ No. Please describe:</td></tr>
<tr><td>In case you serve more than one country, have you identified, in terms of resilience of network operation/services, any regulatory requirements and/or incentives that are similar between member states?

○ Yes, please explain:
○ No.</td></tr>
<tr><td>No</td><td>Would it in your opinion be of value to introduce common regulatory requirement or/and incentives across EU MS in terms of communication networks resilience?

○ Yes, please explain:
○ No.</td></tr>
</table>

Case Studies

In any of the three networking technologies under investigation (i.e. MPLS, DNSSEC, IPv6) in this study can you identify one (or more) issue (success or even failure story) that could in your opinion be the subject of an in depth case study? Please note that the technologies under investigation in this study are considered in terms of their potential to improve the resilience of a public communications infrastructure.

In this light, you proposal for a case study should clearly highlight how the introduction of any of these three technologies improved the operation of your network and as an extension opened new business opportunities by improving your market offer.

8.2 IPV6 Section

In the next 2-3 years, do you intend or are you in the process of deploying an IPv6 infrastructure? ○ Yes, will deploy in the next 2-3 years. ○ Already deployed for ☐ years. ○ Deployed in a trial testbed but have no concrete plans for deployment. ○ No.	
What led you to this decision? (customer demand/ relevant advantage/ technology limitations/ new service provision/ etc.)	
Deployed or will deploy	How would you describe your IPv6 backbone deployment? ○ Dual-stack routers and links. ○ IPv6 (and IPv4) on a separate link layer. ○ IPv6 on the edges, and tunnels to traverse the IPv4 backbone. ○ Other, please elaborate.
	What percentage of your network traffic is (or is estimated to be) in IPv6?
	Which metrics (Key Performance Indicators) have you defined and monitor (or will monitor) in order to assess the impact of IPv6 to the provided services in terms of resilience?
	How have these metrics differentiated from their corresponding IPv4 metrics? or how do you expect them to differentiate after the implementation of IPv6?
	Do you expect that (or has) the introduction of IPv6 introduce(d) some new challenges in terms of resilience to your networking infrastructure? ○ No. ○ Yes, in terms of co-existence of IPv4 and IPv6 networks. Please describe: ○ Other. Please describe.
Deployed	What was the reaction of your customers to the introduction of IPv6 technology? Have they noticed differences in the provided services in terms of resilience?

8.3 MPLS Section

<table>
<tr><td colspan="3">Do you provide IP connectivity to your customers as a service?</td></tr>
<tr><td rowspan="8">Yes</td><td colspan="2">Do you utilize any lower layer protection schemes?
○ SDH protection.
○ Metro Ethernet protection.
○ Other. Please Specify:</td></tr>
<tr><td colspan="2">Which is your organization network resilience policy?
○ Network protection (extra network resources reservation).
○ Network restoration (dynamic route selection).</td></tr>
<tr><td colspan="2">Have you implemented MPLS or do you plan to implement it in the next 2-3 years?
○ Yes, already deployed for ☐ years.
○ Will deploy in the next 2-3 years.
○ Deployed in a trial testbed but have no concrete plans for deployment.
○ No.</td></tr>
<tr><td colspan="2">What led you to this decision? (customer demand/ relevant advantage/ technology limitations/ new service provision/ etc.)</td></tr>
<tr><td rowspan="4">Deployed or will deploy</td><td>Is your MPLS implementation used for forwarding both IPv4 and IPv6 traffic?</td></tr>
<tr><td>Which of the following features of MPLS have you implemented or plan to implement?
☐ Class of service (CoS) tagging and prioritization.
☐ Traffic Engineering.
☐ Fast Reroute.
☐ DiffServ aware MPLS Traffic Engineering.</td></tr>
<tr><td>Which metrics (Key Performance Indicators) have you defined and monitor (or will monitor) in order to assess the impact of MPLS and each of the specific features to the provided services in terms of resilience?</td></tr>
<tr><td>How did these metrics changed after the implementation of MPLS? or how do you expect them to change after the implementation of MPLS?</td></tr>
<tr><td>Deployed</td><td>What were the reactions of your customers to the introduction of MPLS technology?
Have they noticed differences in the provided services in terms of resilience?</td></tr>
</table>

8.4 DNSSEC Section

Do you provide DNS services to your clients?		
Yes	Which of the following services do you provide? ☐ Recursive name servers. ☐ Zone delegation. ☐ Zone Hosting. ☐ Primary name service ☐ Secondary name service	
	How do you handle flash crowd events to the provided service due to line outages?	
	Have you implemented DNSSEC or do you plan to implement it in the next 2-3 years? ○ Yes, already deployed for ☐ years. ○ Will deploy in the next 2-3 years. ○ Deployed in a trial testbed but have no concrete plans for deployment. ○ No.	
	What led you to this decision? (customer demand/ relevant advantage/ technology limitations/ new service provision/ etc.)	
	What barriers, if any, do you/did you see for DNSSEC deployment? (e.g., zone walking NSEC/NSEC3, key management complexity, cost, lack of signed root zone)	
	Deployed or will deploy	In which of the following services have you implemented or plan to implement DNSSEC? ☐ Validating recursive name servers. ☐ Zone Signing. ☐ Delegation of signing authority.
		Have you defined a key management policy? ○ Yes. Please elaborate: ○ No.
		Which metrics (Key Performance Indicators) have you defined and monitor (or will monitor) in order to assess the impact of DNSSEC to each of the provided services in the context of resilience?
		How did these metrics changed after the implementation of DNSSEC? or how do you expect them to change after implementing DNSSEC?
	Deployed	What were the reactions of your customers to the introduction of DNSSEC technology? Have they noticed differences in the provided services in terms of resilience?

9 Annex 2: Interviewee Data

9 Annex 2: Interviewee Data

Interviewee	Ove Tøien
Company	Telenor
Position title	Head of Network Engineering
Task and Responsibilities	Network Engineering and Service Provisioning

Interviewee	Lei Wang
Company	Telenor
Position title	Manager Network Engineering
Task and Responsibilities	Network Engineering and Service Provisioning

Interviewee	Andrew Cormack
Company	JANET
Position title	Chief Regulatory Advisor
Task and Responsibilities	Network Regulations and Service Provisioning

Interviewee	Anne-Marie Eklund Lowinder
Company	.SE
Position title	Quality and Security Manager
Task and Responsibilities	DNSSEC and IPv6 Service Provisioning

Interviewee	Kurt Erik Lindqvist
Company	NetNod
Position title	CEO
Task and Responsibilities	Provisioning of DNSSEC, IPv6 and interconnectivity

Interviewee	Yannis Markoulidakis
Company	Vodafone Group
Position title	Head of Strategic Planning R&D - Technology Division
Task and Responsibilities	Mobile Network Service Provisioning

Interviewee	Kostas Strakadounas
Company	FORTHNET SA
Position title	Core Network Manager
Task and Responsibilities	IP and MPLS Service Provisioning

Interviewee	Achilles P. Voliotis
Company	OTEnet SA Internet Service Provider
Position title	Network Planning & Development Manager
Task and Responsibilities	Network Service Provisioning

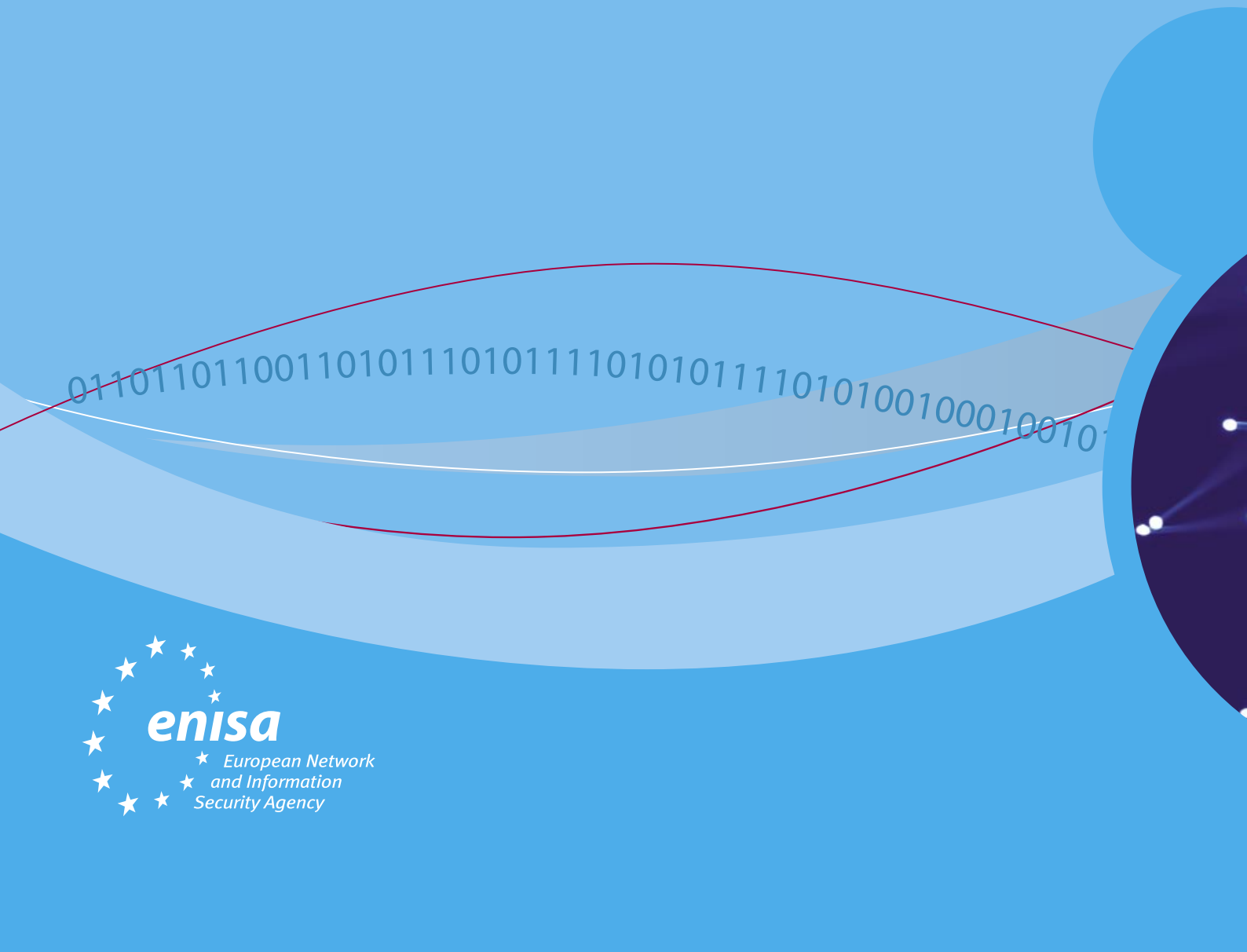
Interviewee	Thrasivoulos Griparis
Company	WIND
Position title	Advisor to the CTO
Task and Responsibilities	Mobile Network Service Provisioning

Interviewee	Christian Jacquenet
Company	Orange Group – France Telecomm
Position title	Head of Strategic Programs for IP Networks
Task and Responsibilities	IP & MPLS Network Service Provisioning

Interviewee	Mário Almeida
Company	Portugal Telecom
Position title	
Task and Responsibilities	IP,MPLS & DNS Network Service Provisioning

Interviewee	Nuno Vieira
Company	NFsi Telecomm
Position title	CTO
Task and Responsibilities	IP,MPLS & DNS Network Service Provisioning

Interviewee	Kalle Lehtinen
Company	ELISA Oyj
Position title	Head of IP Networks
Task and Responsibilities	Production, Planning and Optimization



enisa
European Network and Information Security Agency

P.O. Box 1309 71001 Heraklion - Crete - Greece
Tel: +30 28 10 39 1280, Fax: +30 28 10 39 1410
Email: resilience@enisa.europa.eu