D2.1
User Requirements

Project number	611458
Project acronym	SECURED
Project title	SECURity at the network EDge
Project duration	36 months (1/10/2013–30/9/2016)
Programme	FP7 (Collaborative Project)

Deliverable type	**R** - Report
Deliverable number	D2.1
Version (date)	v1.1 (09.03.2014)
Workpackage(s)	WP2
Due date	31.01.2014 – M4

Responsible organisation	TID
Editor	Antonio Pastor
Dissemination level	**PU** - Public

Abstract	This deliverable describes the process that we followed for deriving requirements according to the stakeholders and users of SECURED. The main objective is to prepare a list of requirements to be used in the design phase of the SECURED architecture and its key components.
Keywords	Stakeholders, user requirements

(This page is left blank intentionally.)

Editor

Antonio Pastor (TID)

Reviewers

Marcelo Yannuzzi (UPC)

Diego Montero (UPC)

Contributors

Fulvio Risso (POLITO)

Roberto Sassu (POLITO)

Mario Baldi (POLITO)

Antonio Lioy (POLITO)

Adrian Shaw (HPLB)

Michael Georgiades (PTEL)

David Florez (TID)

Germán Martín (TID)

Francesca Bosco (UNICRI)

Diego Montero (UPC)

Marcelo Yannuzzi (UPC)

Mario Nemirovsky (BSC)

Jarkko Kuusijärvi (VTT)

Acknowledgement

This work was partially supported by the European Commission (EC) through the FP7-ICT programme under project SECURED (grant agreement no. 611458).

Change Log

Version	Date	Note	Author
v1.0	24.02.2014	Base version	A. Pastor
v1.1	09.03.2014	Quality control	A. Lioy

Executive summary

This deliverable collects the requirements of different potential users of SECURED. The main goals of this document are: a) to identify the different types of SECURED stakeholder, b) to report the outcomes of a survey made to understand the needs and interests of the different stakeholders, and c) to derive from the survey the list of requirements that will be used as a starting point in the design phase.

To be able to design a solution with high potential, the unanimous decision was to reach as many stakeholders as possible. An online questionnaire was selected as the best option for gathering information from a broad set of stakeholders – though this was not restricted to this sole source.

Five categories of stakeholders were identified: End Users, Corporate ICT Managers, Security Developers, Network/ISP Operators and Service Providers. Based on these categories, specific questionnaires were created for each of them and distributed via a web-based survey tool.

The questionnaire for End Users aimed at understanding their habit regarding mobility and device preferences, perception about the most important security risks, and attitude to the SECURED concepts.

The ICT Manager survey focussed on managers of corporations. Opinions related to network application-offloading were asked together with common problems that ICT managers will need to face upon any new technology, such as learning curves, complexity of configuration tasks, perceived cost or risks, etc.

For the Developers of Security Applications the questionnaire was oriented to their preferences in programming and system environments and platforms, and the kind of security applications that developers were interested in using.

The Network Operators questionnaire aimed at evaluating the interest that this type of stakeholder could have in hosting and deploying SECURED inside its own network, and offering it as a service. There were specific questions related to business opportunities and risk perception. Additionally, opinions about SECURED as a security service were asked to them.

Service Providers were asked about their support for a SECURED-like architecture, and if there was an interest to pursue this vision in their business models. Also, there were questions related to the potential impact on other SP services.

Invitations to the survey were distributed to interest groups (e.g. national and trans-national forums). Hard copies of the questionnaires were also distributed and processed. A total of 517 surveys were completed. Most of repliers were EU residents, and answered for the End User questionnaire. It is important to note that their experience level was mostly in the medium to high range.

The main conclusions drawn per stakeholder can be summarized as follows.

- The security-level and protection means for End Users strongly depend on the capabilities and performance of their specific device, which is prone to a number of threats in many cases. An opportunity to extend the current security offer is evident, especially in mobile environments.
- ICT Managers have several services protected with legacy technology, which could be offloaded to SECURED. While this approach would have clear implications in terms of cost and maintenance, it also raises strong concerns, especially, regarding third-party tools and security applications.
- Developers of security applications have more interest in x86 platforms and high-level languages, but their preference about particular security applications remains unclear. There was a positive perception among them about the SECURED concepts.
- Networks Operators have shown a strong interest in SECURED concepts, and they consider it as a business opportunity. They have shown concern about opening SECURED to third-party developers.
- Service Providers also recognize the opportunities of opening the platform to third-party developers, but they are concerned about potential tampering attempts.
- Additional aspects extracted from the survey include concerns about how to integrate SECURED in legacy environments, and how to comply with regulatory requirements.

Finally, a comprehensive list of requirements has been elaborated, the most relevant ones being:

- (End Users) mobility support, good performance, proportionate cost, transparency, and versatility;
- (ICT Managers) protection and policy enforcement support in roaming scenarios, assurance, applications for mobile devices, antivirus and firewalls, privacy and confidentiality of the traffic and user authentication;
- (Developers) support for high-level languages, rich APIs, a platform-independent deployment framework, guarantee of adequate performance and scalability, easy migration support and good documentation;
- (Network Operators) a flexible and scalable architecture, operation and monitoring support, SLA support, as well as security and support to categorize applications;
- (Service Providers) guarantees on end-to-end security, minimum supported user capacity, equivalent service performance in mobility, no third parties affection in existing services and Virtual Security functions support;
- (miscellanea) backward compatibility and regulatory/legal compliance.

As a conclusion, the final list of requirements seems well balanced and considers the general needs of each stakeholder, ensuring that none of the key stakeholders is left out of the SECURED design.

Contents

(This page is left blank intentionally.)

1 Introduction

The main objective of the SECURED project is the offloading of the multiple and heterogeneous security tools utilised by users in the form of home/office applications installed in their equipment, to a device placed at the network edge. This approach not only enables the harmonisation of security features in a transparent way, but also alleviates the users security responsibilities and scales much better as the number of gadgets and end devices per user increase. Also note that SECURED fosters in-network management, which can significantly improve the security and protection levels offered to the users.

It thus seems sensible to obtain first-hand opinions about the users involved and their security needs, especially, to understand under which conditions it would be desirable to move the security control from the end user device to the network, and therefore release the users from the burden of directly controlling and supervising their security on a per device basis. Take note too that the user concept covers a wide set of meanings within SECURED. A SECURED "user" refers to anybody who may have security requirements, from an average layman navigating the Internet, up to the Network Operator striving for securing its subscribers' communications.

In that sense, SECURED considers as one of its main goals to reach out to its potential beneficiaries and gauge their opinion and needs by distributing questionnaires. The answers will be then analysed in order to extract the requirements, which will subsequently drive the design and implementation activities, thereby composing the main lines of activity of the project. Since the SECURED "user" concept is a portmanteau[1] word, which hides a wide spectrum of phenomena, the first task will be to create a taxonomy of the potentially relevant stakeholders in the SECURED. This taxonomy will help to elaborate specific targeted questionnaires according to each user's profile.

The remainder of this document is structured as follows.

Section 2 explains the rationale for users questionnaires, defines the stakeholder taxonomy and briefly sketches what information will be queried in each stakeholder's questionnaire, as well as the description of the tools used in their dissemination and general statistic data about questionnaire's results.

Section 3 focuses on analysing the raw data collected from the questionnaires per stakeholder. The aim is the detection and extraction of general trends, which will serve as the seed of SECURED's requirements.

Section 4 describes the actual requirements per stakeholder. Each requirement is clearly defined, highlighting its repercussion on the originally intended SECURED concepts.

Section 5 contains a summary table of the requirements to ease future references.

Section 6 summarises the contents of this deliverable and enumerates the main conclusions.

Appendix A includes the full text of the distributed questionnaires, while Appendix B derives additional concepts (related to business interest). Finally, Appendix C lists the abbreviations used in this document.

[1] A portmanteau is a neologism created by combining two existing words, as explained by *Lewis Carroll* in *Through a Looking Glass [1]* .

2 User questionnaire's rationale

As explained in the introduction, the motivations behind the elaboration of SECURED's questionnaires lies on the data that will be obtained after distributing them to potential SECURED stakeholders. In this section, it will be first explained the rationale behind this method, and the stakeholder taxonomy. Individual questionnaires were composed for each stakeholder, and their contents and justification will be later on sketched (the full questionnaires can be found in Appendix A). To conclude this section, we shall describe the means for distributing the questionnaires (basically online as well as hard copies), and we will describe the basic statistics about respondents.

2.1 Why a user questionnaire?

As explicitly stated in the introduction, the main objective of SECURED is the offloading of security functionality from users' premises to the network, so the entire project (i.e. from requirements to testing) must be driven by the user aspirations and needs. It is true that the SECURED consortium consists of important stakeholders in security matters, coming from Academia, Manufacturing and Network Operation. With our experience, a complete and coherent specification of requirements could be elaborated in the traditional way, but it would be inevitably biased by the interests and prospects of our respective organisations and goals.

It is then necessary to get out our walled gardens and reach out for all the potential SECURED stakeholders, known or not, so the SECURED model is made from the start, to be as flexible, scalable and adaptable, as possible. The creation of questionnaires and its distribution through the appropriate fora seems then the right choice, especially because the partners' profiles in the SECURED consortium ensures that we could poll the opinion from disconnected users' populations, not at the reach of a single partner, and located in different countries in the EU area, including, Finland, Italy, Spain, UK, and others as well.

Note that we are talking of questionnaires, not a questionnaire. The multiplicity of potential user types needs to be polled with different sets of questions, which specifically address their roles and needs. The first task to be completed is the identification of these user types, which in our case consisted in creating a stakeholder taxonomy, and the sketch of what should be asked within each category.

2.2 Stakeholders' taxonomy

When talking about shifting security to the network edge, the first impulse would be to think of a layman navigating the Internet via a mobile terminal or a laptop who does not want to be concerned with the installation of complex security applications, which may or not be regularly updated or may be not fully protecting the user despite their advertising claims. However, it is not difficult to realise that other stakeholders are also interested in this security paradigm, even if they are not aware of it yet. One clear example is a company's ICT manager who may be interested in offloading either part or even the entire set of security procedures, as long as the risk of compromising relevant data is controlled. Clearly, this is just one example, but many others can be sketched.

It is then necessary to start by identifying those stakeholder types and their profiles. The different questionnaires are properly elaborated focusing on each user profile, thus ensuring that the collected data is definitively relevant. A brief survey of the potential market for SECURED has detected at least six stakeholder profiles, which are described hereafter.

End USR. An End User is any individual navigating the Internet, who may or may not have technical advanced knowledge beyond the use of simple applications, (e.g., a Web Browser.). Despite his technical prowess, he will be interested in ensuring his communication security, data integrity and personal privacy, but he would rather avoid complex and intrusive means of security enforcement.

ICT Manager. The ICT manager commonly is a high level technical expert in charge of managing the internet communications of an organisation, e.g., an enterprise, a public administration, and so on. Despite its degree of knowledge, the complexity of the security task an ICT Manager has to face will make him prone to

accept solutions which simplify/automate his daily work, with the provision that the organisation procedures are not compromised.

Developer of Security Applications. The target of an application developer is twofold. First, he would like his applications could be deployed on most commonly used OSs, aiming to reach wider swathes of public. Second, and specifically for security applications, this can only be achieved if the user is convinced somehow that the applications he is installing are really secure. In other words, they have been certified. In principle, a developer would be receptive to a platform like SECURED, which aims at compatibility and will put an extra effort in ensuring the legitimacy of any deployed application.

Network Operator/ISP. Network operators would not only benefit from protecting their subscriber from externals threats, so subscribers' QoE would be improved and loyalty ensured, but also from offering extra security features in the network edge nodes they manage, after being endowed with SECURED functionalities.

Service Provider. The service provider would be interested in protecting the products that they are offering from unauthorised access, as well as ensuring the integrity and confidentiality of the data provided by their users. Since keeping these functions in-home usually places considerable burden on the already stretched resources of a Service Provider, offloading them to the network edge would be a clear improvement.

2.3 Overview and rationale of questionnaires

In the following sections it will be discussed how the questionnaires have been composed and which relevant pieces of information they must and do contain.

It is important to specify, in the methodology, that the aim of this questionnaire is a qualitative assessment of needs more than a quantitative research; therefore. Therefore the sample was not scientifically identified, but it was selected on the basis of the network of each partner. Some respondents did not finish the whole questionnaire, but we decided to take into consideration their answers since they might give useful information for better understanding the end users' needs and possible attitude toward SECURED.

As we all know, there is always a small percentage of possible bias, but we can overall evaluate the answers given as genuine and sound.

2.3.1 End User

As explained in the Stakeholders' Taxonomy section, end users can have different knowledge levels. We attempt to divide the end users by their self-assessment, therefore 5 categories resulted: highly expert, expert, familiar, novice, unfamiliar. Since it is based on an auto perception and we did not include in the questionnaire any "control" questions, we decided to use the average as general background for the group, but not to make specific correlations with other questions.

The questionnaire for the end users tried to understand both the users' habits and behaviours with laptops/desktops and with mobile devices (smartphones and tablets), and their perception of risks, the countermeasures they put in place and their possible wishes regarding network security management. Then a relevant set of questions is dedicated to understand the possible users' attitude towards SECURED aim and specificities, looking into usefulness, costs, performances, ownership of security controls and configuration options. These elements are useful as a guiding principle to build users' requirements as a result of an analysis of their attitude in responding to the related questions.

2.3.2 ICT Manager

The purpose of the ICT manager questionnaire is to find out the opinions of managers and admins who protect corporate resources and handle security policies related to different corporate devices ranging from mobile devices to routers, servers, and so on. The questionnaire results are used to aid in deriving high-level stakeholder requirements for the ICT Managers group. Overall, the questionnaire covers questions about 1) background of the manager, 2) currently exposed services and user security measures, 3) security policies,

willingness to learn new ones and the configuration complexity related to them, and 4) opinions about "network application offloading" services in general and concerns related to them..

Enterprises and small businesses may find adoption of new kinds of network devices difficult within their existing network topology, depending on the number of available resources or due to other constraining factors, such as cost. Since the SECURED project introduces a new style of Network Edge Device (NED), it is important to understand the current flexibility of corporate environments, should they consider incorporating NEDs as part of their existing network infrastructure. We proposed to include a question about how easily existing network devices can be integrated, excluding the typical variance in software setup. As for the business side, we propose to include a question about what would the ICT managers be willing to pay for a "network application offloading" service, referring to the SECURED platform and NED.

Manageability is a primary concern within larger corporate environments. This ranges from the usability of management software to the scalability of the number of devices that can be managed. Furthermore, policies must be well understood by the network administrators, as well as easily deployable on large numbers of devices. If applied policies cannot be well understood by the administrators or auditors, then they will not prove particularly effect. Introducing new ways of expressing policies will often require substantial training cost on behalf of the business, especially if there are a large number of administrators involved. Since a number of existing systems (e.g. IPtables, SElinux, large XML-based schemas and others) require specific tools and training, it is reasonable to ask ICT administrators and managers whether learning a new policy language specifically for network devices will cause any difficulties. In addition, it would be beneficial to ask whether admins prefer simple or complex security configurations (taking into account that simple configurations might be less powerful because of coarse-grained expressions).

We proposed as part of the questionnaire, to ask the corporate admin about existing protection mechanisms that are already in the corporate environment, and ask whether there are any specific functionalities that may be more effective as part of the network edge. Since some ICT companies provide full, separate wireless networks for guests and for employees, we proposed the question that, given distributed network protection and complete compliance with company policies, whether they would feel more comfortable in sharing network resources between the guest and employee networks. This is an important question in order to understand if this factor can allow for improved consolidation of network resources and security management.

Due to the potential problem of inside attackers, who can gain physical access to employee devices, a number of technologies are in wide use in many businesses to help protecting personal data (e.g. disk encryption for endpoints) as well as managed firmware (e.g. secure boot). We proposed to ask the question to managers as to whether they are particularly worried about the threat of tampered network devices. This is an important question to ask, to test if assured firmware security is a major concern for network edge devices.

Since typical applications running on users' NEDs are expected to be Antivirus and some form of traffic inspection services, we also proposed to ask the ICT Managers how they feel about anonymous inspection of traffic for security monitoring purposes.

2.3.3 Developer of security applications

Developers of future security applications play an important role in SECURED, as the success of the project will be greatly dependent on the amount and the quality of the applications that can be executed in the NED. The success of the project depends on how the developer community embraces and leverages this new technology, and innovate the kind of user security applications to be deployed using the SECURED technology. In fact, the number of available applications is likely to be one of the parameters that can be considered by end users when they evaluate whether to migrate to the new platform or to stay with a more traditional paradigm. The quality of the applications (e.g., in terms of features, performance) represents an important parameter for end users as well as the operators, which would like to make sure that the applications are stable, trusted, and do not consume excessive resources of the NED.

For those reasons, the SECURED platform, which includes both the architecture and components, should be defined in a way that satisfies the requirements of the developer's community.

Therefore, the portion of the questionnaire specifically dedicated to developers has been designed with those objectives in mind, in particular to discover:

- preferences in terms of programming environment (operating systems, languages);
- classes of applications that most likely will be created;
- willingness to start developing for (yet another) platform (i.e., NED in addition to PCs, smartphones).

2.3.4 Network Operator / ISP

Network Operators/ISPs are stakeholders with great interest in SECURED, due to their preferential position as a hosting provider for the SECURED infrastructure. Several of the questions were oriented to discover the Network Operator/ISPs' attitude towards personal security applications running and interacting in a new way inside their networks.

Additional questions were made to seize the needs in the SECURED architecture for Networks Operators/ISPs. The subjects were related to third parties access, service availability and operational requirements.

Observe that a security application is a quite open concept that covers a lot of different services and applications, and it has a strong dependency on the person asked. In order to know what kind of application can be specified and developed for Network Operators/ISPs, and to make it possible in SECURED, a few questions were made about the types of security applications that were expected in the short and medium term.

In addition to the technical questions, others related to business opportunities and markets size were also posted, mainly with focus on exploitation opportunities.

2.3.5 Service Provider

For a Service Provider, it will be interesting to obtain sufficient feedback on how this segment feels about the introduction of NED-based security controllers. To achieve this, a large number of questions have been created to identify what an SP thinks about the feasibility of having an NED for security support, what an SP thinks about customised security support at the network edge, in order to get insight on whether SPs are worried about the idea of introducing an NED.

The questions asked targeting the SP segment included: identifying the willingness of a SP for supporting the deployment of NEDs; if they believe in its feasibility; willingness for customisable security features to be installed at the NED; number of user expectations; willingness to allow subscribers to define their own security functions at an NED; whether they believe that moving security functionality from users' devices to the network edge will affect services; and also, if this approach will create more business opportunities for them. To obtain clear statistics, a set of closed form questions was asked with the objective to limit responses to a pool of answers.

The answers of these questions will give an insight on whether an SP may fear whether its services will be in jeopardy. An SP could also decide to offer its own NED functionality for a particular service it provides to a set of customers. A use case scenario with SP providing specific security is worth investigating to obtain further requirements.

2.4 Tools and means of distribution

The survey has been created by using an open source tool, called Limesurvey (www.limesurvey.org), and has been hosted in a server at the Politecnico di Torino.

This tool is very flexible as it allows, through its Web front-end, to insert new questions by using predefined templates (list dropdown/radio, text box, multiple choice, etc.), so that the survey creator has only to choose the appropriate format and provide the question text as well as possible answers.

Another useful feature that has been employed to create the survey is the possibility to define conditions so that a question is displayed to the user only if the provided conditions are evaluated as true. For example, it is possible to display certain questions only if a user gave a specific answer on a previous question.

Since a survey could be filled by people from different countries, Limesurvey allows translating each question and their answers in one or more languages by keeping the same identifiers (so that statistics can be collected regardless of the language chosen). A user can answer questions in his native language by accessing the survey from a specific URL, which is composed by the main survey URL and the suffix "/lang-<language ID>".

Data analysis can be done while the survey is active (it has been published and made available by the survey creator) or when it is deactivated after the deadline providing answers passes. Limesurvey allows data to be processed in two ways: it allows exporting raw data so that they can be analysed by an external program (e.g., with Excel), or it can provide data statistics by itself with the percentage of answers for each question, and, eventually, a graph.

The survey has been made available in three languages: English, Italian and Spanish; the former at the URL http://survey.polito.it/31418/lang-en, and others at the same URL with 'en' replaced by 'it', and 'es', respectively.

The online questionnaire was conducted between 26/11/2013 and 15/12/2013. In addition to the online questionnaire, some paper questionnaires were distributed and filled (e.g. in FinnSec 2013 exhibition, http://www.messukeskus.com/Sites3/FinnSec/en/Pages/default.aspx), which were later stored to the online questionnaire to include the results into the main analysis results.

It is important to mention here that the online questionnaire was announced to several special interest groups to increase its visibility. Some examples are different units in some national Network Operators, National Network operators groups (e.g. ESNOG) or Trans-Europe forums like TERENA [2].

The questionnaire's paper version itself can be found in Annex A.

2.5 Questionnaire statistics: population and distribution

This section provides some information about the users that filled the survey. Since not all users finished answering all questions (223 surveys were filled partially), statistics are provided for both the completed surveys (294) and all surveys (517, completed + partials). Numbers and percentages for each source of information are separated through the slash character.

Regarding the results provided below there are two important remarks. First, since for some questions the answer is missing, the sum of percentages for statistics based on all surveys may be lower than 100 (the number of respondents that did not answer a question is not reported). Second, all the answers come from countries of the European Union. It must be noted that, since the statistics may vary between the two survey sets (only the completed ones or all), list items are ordered by considering numbers from the first set.

The survey targeted five main categories (Figure 1):

- End User: 231 (78,57%) / 386 (74,95%);
- Corporate ICT Manager: 11 (3,74%) / 29 (5,63%);
- Developer of Security Application: 30 (10,20%) / 49 (9,51%);
- Network Operator /ISP: 14 (4,76%) / 25 (4,85%);
- Service Provider: 8 (2,72%) / 16 (3,11%).
- Don`t Know / No Answer: 0 (0%) / 10 (1,94%)

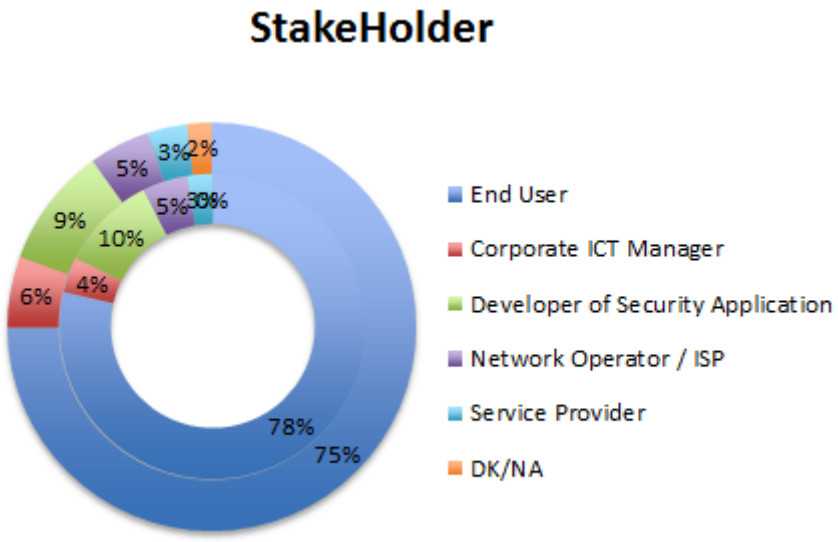

Figure 1: Stakeholder distribution

In the survey, it was inserted a question to distinguish, within the *End User* category, those with an advanced knowledge of computer and networks (those that gave the answer "Expert") from others. Statistics of answers to the question "**How would you characterise your experience level related to the use of computers and networks?**" are (Figure 2):

- Unfamiliar: 0 (0,00%) / 0 (0,00%);
- Novice: 9 (3,90%) / 10 (2,78%);
- Medium: 51 (22,08%) / 77 (21,39%);
- Very good: 94 (40,69%) / 146 (40,56%);
- Expert: 77 (33,33%) / 127 (35,28%).

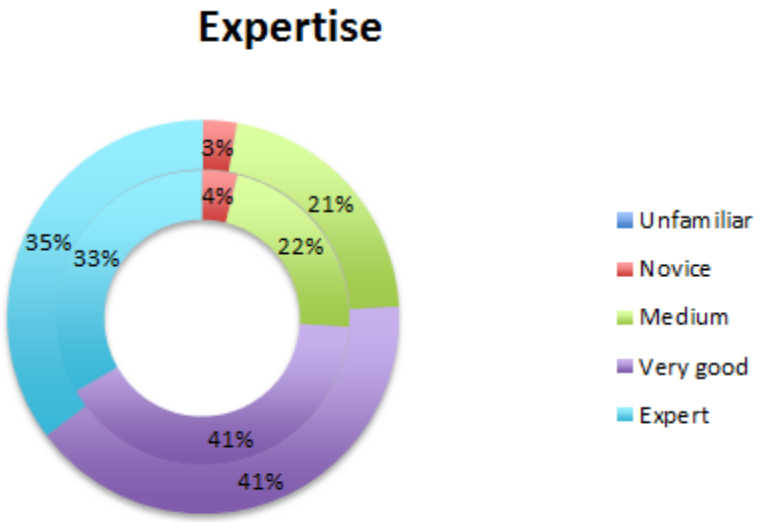

Figure 2: Expertise distribution

Finally, the following statistics give additional information about the respondents. The age distribution is shown in (Figure 3):

- up to 18: 1 (0,38%) / 3 (0,71%);
- 19-24: 80 (30,65%) / 145 (34,12%);
- 25-44: 145 (55,56%) / 237 (55,76%);
- 45-54: 23 (8,81%) / 25 (5,88%);
- 55-65: 9 (3,45%) / 10 (2,35%);
- over 65: 3 (1,15%) / 4 (0,94%).
- Don`t Know / No Answer: 0 (0%) / 1 (0,24%)

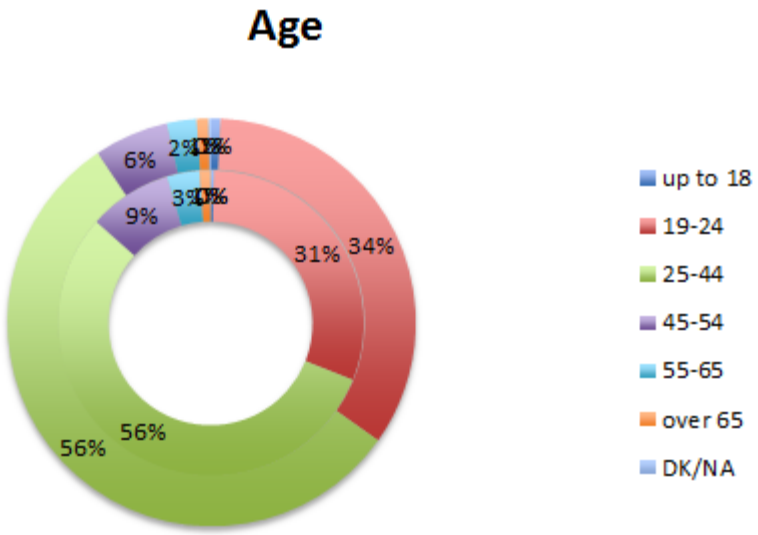

Figure 3: Age distribution

Regarding the *Developer of Security Application* category, the number of years they are programming (Figure 4):

- less than 1 year: 1 (3,33%) / 2 (4,26%);
- 1-5 years: 9 (30,00%) / 10 (21,28%);
- 6-10 years: 14 (46,67%) / 21 (44,68%);
- more than 10 years: 6 (20,00%) / 13 (27,66%).
- Don`t Know / No Answer: 0 (0%) / 1 (2,13%)

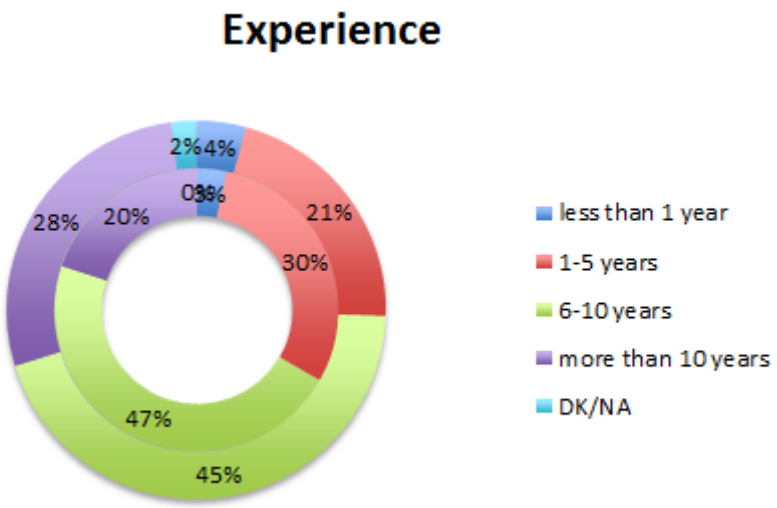

Figure 4: Programming Experience distribution

3 Questionnaire results' analysis

This section describes the analysis performed over the poll results, aiming to extract key information questionnaires' raw data. Besides several conclusions are listed, which will be listed the guide and support for the requirements definition (section 4). It is important to mention that this section will not list detailed information with raw data results of the questionnaires.

It is important to specify, in the methodology, that the aim of this questionnaire is a qualitative assessment of needs more than a quantitative research; therefore. Therefore, the sample was not scientifically identified but it was selected on the basis of each partner's network. Some respondents did not finish the questionnaire, but we decided to take these answers into consideration since they might give useful information for better understanding of the stakeholders' needs and because of the overall small complete answers in some stakeholder cases.

As we all know, there is always a small percentage of possible bias, but we can overall evaluate the answers given as genuine and sound.

An important statistic derived from the poll's results shows that respondents are mainly from different EU countries. This result allows us to have an accurate representation of different stakeholders' interest and obtain meaningful conclusions. Besides, most of the respondents' profiles were from medium to high experience level. This result makes sense considering that the survey was not public-oriented but ICT niche audience-driven.

The analyses of the results are classified based in the stakeholders' taxonomy defined in Section 3.2. In order to facilitate this distribution, the surveys included an initial question the querying the respondent to identify himself in one of the stakeholders group. Next subsections will describe main findings and conclusions.

3.1 End User

The category of End Users defines a regular, Internet surfer USR. The questionnaire targeting this stakeholder searches for information about the security risks perceived by them as well as the measures implemented for their personal protection in domestic activities (e.g. protected web browsing for kids) and in their working related activities (e.g. remote access to their working emails).

The first general observation rom the end users' behavior is that the primary devices used to connect to the Internet are high performance, comprehensive platforms (e.g. laptop and desktop pcs). Most of these platforms have an antivirus installed. On the other hand, since mobile platforms (e.g. smartphone, tablets) are becoming more powerful, they are being used as secondary devices to connect to the Internet. However,

mobile devices are not protected in the same way as primary platforms: In fact, from the results we obtained that 72% of the respondents using this kind of devices do not have an antivirus installed. Even if the smartphones are not adequately protected and they are mainly used for surfing the web (almost 53%), still social networking activities (41%) and, in a small percentage (14%), online banking, can provide fertile ground for possible threats. SECURED can be a key enabler for improving the protection of these devices since implementing it on mobile devices can result in performance degradation and excessive battery depletion.

As a side note, 64% of respondents disclosed that other people have access to the devices of which they are owner or main USR. These behaviours can clearly expose the devices to threats that the user might not have considered.

As a general remark, users do care about security when connecting to the Internet as it is confirmed by the answers to questions about the importance of privacy and the desire to use anonymizing services to protect it (over 75% of users express preferences in this direction).

The vast majority of the users protect their primary platform with an antivirus as viruses are seen as the most relevant Internet security threat. Users are also worried about theft of financial /identity information, privacy violation, network activity monitoring and phishing scam. Child online exploitation and grooming are also among the perceived worrying risks.

End users also try to protect themselves when they perceive a concrete risk of security breach. This is the case of protecting the wireless connection. Most users protect the access to their network with a password-based access control (e.g., WPA, WPA2).

From the results, we can derive that other threats are not considered critical. For example, respondents do not often use VPN to connect to their organization's network or other security measures when uploading content to their web site.

Users are in general satisfied about the security applications present in the market. However, since the percentage is not particularly high (about 60%), this suggests that there is a significant share of the potential users that could appreciate an extension to the current offer.

With regards to kids' use of the devices, more than 79% of the respondents do not have kids, but few respondents answered that they have parental control installed on TVs, tablets and desktops.

Among the security measures in place, users find useful that they are warned if they access a scam web page and more than 95% is interested also in checking blocked connections (due to suspicious behaviour of the remote peer). Users can also accept to prove their identity, provided that they can have an option to connect anonymously.

In support of the protection of several independent electronic devices, users find also useful a protection service that is device independent. This confirms that the SECURED proposal is aligned with the end user needs. In particular, most users (73%) agree on the importance of having the same kind of protection when switching from one network to another one and the 64% thinks that moving the security actions to the network edge would provide better security. Since the protection will be applied by network edge devices, it will be possible to increase the network security level for users that are not or only partially worried about the mentioned security threats (e.g. uploading of web content, connecting to the organization network) or capable of putting the right protections in place. Respondents revealed their conviction that if companies offered protection services that run on network edge devices, these services would gain acceptance in both business and residential environments, with a slight preference to the former.

One reason why the SECURED protection service would be adopted especially in the professional environment is that users are not willing to accept the overhead introduced by this service in terms of either cost (58%) or performance (51%). For those respondents that accept the overhead, the protection service should be accessible and the impact over the performance should be minimal.

Considering the effort required using a new protection service, 82% of end users have no problems to install new applications on their electronic devices, with however, there is less preference for doing it on smartphones (37%).

Regarding the security applications that should be executed on the network edge devices there is not a strong preference over common types (e.g., network security monitor, malware detection). Among other types of applications, users express preferences for those related with electronic identification, data processing and content filtering. In all cases, users agree on having options to configure applications and determine which ones are being deployed.

Specific considerations should be taken regarding the ownership of the security controls executed on network edge devices: while. While users would accept that network providers establish the security applications (66%) configured to handle their network traffic, however, a main concern is raised due to network providers would have too much control. It is very important for users to have visibility at any time onto which applications are being executed over their traffic.

In particular, users are concerned with the fact that network providers are inspecting the network traffic (87%), however, half of them would accept this for due to the additional security advantages it imposes. Only 10% of users would delegate the management of security services to any ISP while others need extra guarantees (29%), prefer a specific company (27%), or want to execute services on their own servers (16%). The perception that respondents revealed with respect to their traffic being processed by security applications running on network provider equipment (independently of whether such applications are chosen by the user or by the provider) demonstrates that an effort to properly educate and reassure end users might be essential to foster the SECURED solution acceptance.

3.2 ICT Manager

The ICT manager questionnaire contained 25 questions in the topics covered in Section 2.3.2**.** The types of questions used were: 1) interval scale 2) multiple choice, and 3) free text. Additionally, some questions allowed comments for additional opinions on the specific question. Most of the questions were five-level questions.

The services exposed to the Internet by the respondents are mostly web, database, FTP, and SSH services. 5% of the answers exposed VPN, remote desktop, SFTP and email services. It should be noted that many answered FTP (64%), while only one response said SFTP (5%) – the secure version of FTP. The network segments were protected mostly by firewalls (packet filters) and router/switch access control lists.

Concerning the subject of how difficult it is to incorporate new network edge devices into existing networks, the responses were overall mixed. It most likely depends on the size of the businesses, the administrative processes which are already in place, and overall costs. Still, 53% of the respondents answered that it would be manageable compared to the 35% that answered it would be somewhat difficult. In addition, there were more responses accepting to install third party software in company devices than declining, so it, thus there is a possibility to bring NED into the companies.

A new, policy specific language did not sway the decision of the respondents, who were overall in favour of the idea and did not express any particular concern over adaptability. There is no clear preference regarding whether managers prefer fine-grained (complex to use) or simple (less powerful) security configuration systems. The responses obtained are mixed, with slight preference over the simple configuration systems.

Network segmentation is a main concern for ICT Managers. There is a no clear preference in results in regard of whether they consider feasible of having different user profiles, e.g., guest users and employees, on the same network with different applied protection. This is either due to reduced complexity or because the lack of a detailed SECURED architecture.

Most managers were concerned about the potential threat of insiders tampering with network edge devices**.** After this questionnaire, there has been news about devices being bugged or trojanized in the factory or before delivery by third parties [3] to gain backdoor access, so this particular result might be an underestimate. Furthermore, around 68% of respondents expressed some concern over security of devices during an employee trip.

Almost all of the respondents (93%) are willing to pay for a “network application offloading” service, while both monthly flat-rate payment and per-user monthly payment got the same support. Therefore, there is some

business potential for some stakeholders providing the service. The willingness to pay for the service is supported by the results of IT Security Trends 2013 [4].

Most of the companies (79%) permitted some form of remote access (e.g., VPN, remote desktop, wireless, email) to the organization's network. Most of the respondents are willing to permit automatic but anonymous inspection of network traffic for security monitoring purposes (strongly agree 37% and somewhat agree 36%). Nevertheless, 36% are undecided whether they would trust delegating security controls to a third party (a broad question), while a small majority would trust to do it. When asked whether they would be interested in security applications being executed by their operator instead of having them in the client devices, 29% would accept it and 50% probably. Additionally, 64% of the responses were concerned about the theoretical possibility of network operator inspecting all of their network traffic.

The managers consider that protecting confidential information and mobility support (64% of respondents) are key aspects that their current network security systems require improvements. Next aspects are the level of security (55%), the application and modification of security policies (45%), and lastly cost (36%). In addition, 78% of the respondents recognize that their organization does not have a policy for mitigating information security risks in mobile devices. Antivirus and firewall security controls are commented as services that could be offloaded from the client devices into the network edge.

3.3 Developer of Security Applications

In the first part of the questionnaire, we asked to developers their preferred supporting platform (the one that will run developed security applications) and source code language in order to have a better idea of the features (hardware and software) the main device developed by SECURED (the Network Edge Device, NED) should offer. Indeed, one of the goal of SECURED is to encourage developers migrating their existing applications and developing new ones for the new platform so that the market will meet the demand for more security by end users.

From the statistics collected on this part of the questionnaire, we obtained two important pieces of information. First, from the results we can derive that developers feel more comfortable developing applications to be deployed (over which platform the application is going to run) in two x86 platforms, i.e., Linux/UNIX 63% and Windows 16%. Others platforms like Embedded ARM or Architecture specific are less attractive.

Second, most developers prefer to work with high-level (29%) and scripting languages (20%) than low level ones (19%). One reason for this result, as also confirmed from answers given to an open question, is that most high-level languages are platform independent (like JAVA, python) and, thus, hide to developers specific features of the platform their applications will run on.

Regarding which kinds of security applications are of interest to developers, statistics show the highest values for network security monitor (30%) and privacy protection (24%). There is still interest in developing applications for packet filtering (16%) and malware detection (13%) while less effort is concentrated on VPN clients (7%). These results help us understand which kind of information the NED should make available through its API to ease the task of developers working on this set of standard applications. SECURED should provide a mean to select the portion of data required by the application.

In the second part of the questionnaire, we asked to developers what they think about the approach chosen by the SECURED project about offloading network security applications to NEDs. From the technical perspective, we obtained positive results regarding the possibility that either developers port their existing applications to the new platform (48%) or develop new ones specifically to be executed on NEDs (63%). Also, we found that there is a high percentage of undecided (about 30%) but this is expected as, since the project is in an early stage, we were unable to provide more details about the platform and development tools we aim to offer.

From the business perspective, developers also believe that offloading network security applications would be an opportunity to make profits and their opinions about the main benefits in following this approach are aligned with considerations we made at the time of writing the SECURED proposal. Among others, we

recall the simplification of IT management, costs reduction and availability of security applications for a broader range of platforms.

Finally, we asked to developers which are the emerging technologies that would be helpful to develop new network security products, with the objective to use them in SECURED. The most relevant ones are also current research hot topics, such as cloud, virtualization [5] and SDNs. One result worth to notice is that several developers presented an interest in the privacy-protection topic matching the end users growing concerns about their privacy on the Internet.

3.4 Network Operator/ISP

Questionnaire results have revealed several underlying interests of Network Operators/ISP related to security services, Network offloading and kind of services.

ISP/Network Operators have a high interest in offer customizable security features integrated in the network and see it as a business opportunity (74%). Survey results show a clear interest in access to a new technology based in network that can offer security services on mobility and this kind of service will attract more clients to their networks.

This conclusion coincides with a public surveys conducted by F-Secure (an anti-virus, cloud content and computer security company) where 69% of people think it is the responsibility of their communications or Internet service provider to keep their digital life safe [6].

Security Service sizing is wide. A weighted average shows around 50.000 users sizing for Security Services. But there is a wide range of needs, between less than 100 users up to 100,000 or more users.

There is interest in allow user to have management preferences in the services. Customizable preferences by end-users in services help in market position and competitive advantage, and have being seen as a clear demand expressed in the surveys.

Opening the Network to third parties generates hesitation as expected in NO/ISP. It is produced mainly by two aspects. The first one is due to the offloading of end-user security services from end-devices to network nodes, which increases the security risk in the network operator. The second one is related to the security concerns raised because of the required access of third parties to network infrastructure in order to offer and host new security services. These concerns are similar to current Cloud services models [7].

There is not a type of security killer application in the NO/ISP results. No preferred application or service above the common ones has being discovered in from the results. On the contrary, there is interest in all of the security applications asked. Main interests are divided among 3 categories:

- network monitoring, where relevant applications interests are centre in DDoS protection and IDS/IPS;
- related to Malware security impacts, like spam e-mail generating or receiving, phishing web pages and campaigns' detections and blocking, or online antivirus protection;
- network filtering. Inside this category the most interest is packet filtering functions like Firewall protection and Parental control services.

This conclusion analysis shows a clear opportunity to offload classic security services on the network. Apart from that, most NO/ISP have a classic vision of security services, most of the time limited by their own knowledge of the state of the art in Security technology. Developing and exploitation of new disrupting security services is a clear opportunity for SECURED, where carrier-class quality services can be developed. Using new technologies aligned with standards like NFV [8] will help in these disruptive models to be successful.

Additional specific needs from NO/ISPs showed up. Encryption data for clients, privacy concerns on the data and the traffic, or cooperation between operators using services based in SECURED are the comments from the open questions.

3.5 Service Provider

Out of 294 questionnaires, 2.72% where completed by Service Providers (SP). From this the following conclusions have been realised.

An SP is concerned that none of its services are tampered from security control functions provided through the NED, mainly in third party participations.

An SP does not want end-to-end service provisioning to be jeopardised in any way.

An SP wants customers to be provided with seamless mobility if possible without affecting ongoing services or sessions while on the move. Hence the NED must provide the necessary interfaces to support security for intra- and inter-domain mobility support.

The SP may want to provide a particular in association with a particular service. E.g. a school online program together with associated NED features for parental control.

An SP is willing to accept that third party providers may provide security features at an NED.

An SP will benefit if a an end user is relieved from heavy duty security functions cause this will mean that thin client terminals could benefit of high demanding services and application without security processes adding additional load on the memory of the device.

SPs believe that better security could be provided through an NED rather than simply at the terminal alone. This is probably true a an NED will probably be located on a higher spec machine and can provide a suite of security features from different parties and offer options for utilising the best combination of these.

QoS is really important for the SP and the services provided. SPs worried about this probably worry about possible impact on the QoS of the services.

In terms of security functionality an SP has already deployed or would like to have in place is shown in the Figure 5.

It is clear that those working for a Service Provider already use or feel that having an Antivirus and Firewall systems installed are essential which probably comes down to personal usage on their own terminals. Beyond this only some Service Provider employees seem to place emphasis on other security mechanisms such as network security, spam protection, parental control etc. This is probably because people working for a SP may think that as things stand it is the job of the network operator or the end user to provide the majority of secure functionalities. However service providers focusing on a specific service that may need for example parental control may want to be aware for such support either by the NO/ISP or by a third party security function provider.

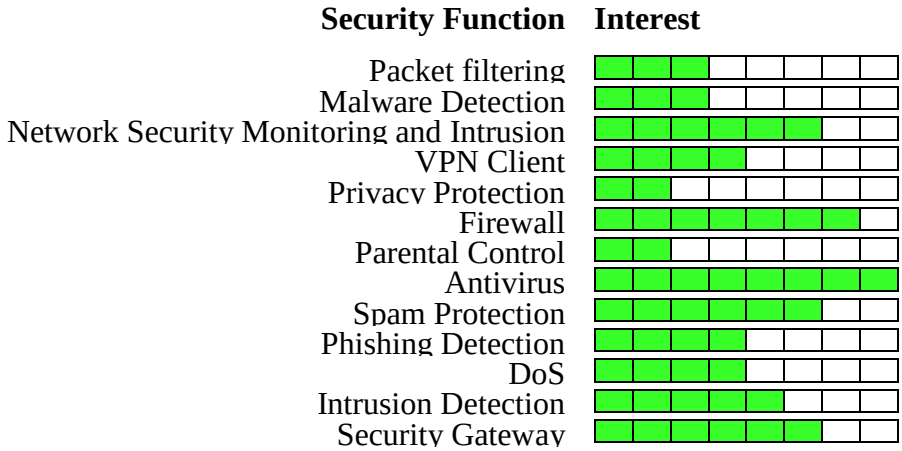

Figure 5: SPs Security Functions usage

3.6 Additional aspects

This particular section has been included to list additional conclusions obtained with other mechanism than surveys: mainly operational experience in Network Operators, partners' contributions and comments received by stakeholders.

One big nightmare for any business related stakeholder (Service providers, ISP, etc.) is to have malfunctions or service failures caused by versions incompatibility between applications (e.g. PSA) or the infrastructure components (PSC or NED). Stakeholders affected think that SECURED design must consider these demands, for example, guarantee backward compatibility in at least minor's release.

Any stakeholder with its own infrastructure is concerned with the difficulties involved in integrating a new technology in legacy network. These problems can appear in:

- Legacy technologies based in monolithic architectures. Help will be needed to adapt and understand SECURED model. For examples legacy Edge Routers are based in close Operative Systems and have limited programmatic interfaces, so the use of advance routing or state of the arts technologies like SDN could be necessary.
- IT systems used, such as Provision, billing, supervising, etc., have to be connected with new SECURED elements, like NEDs or policies controllers.

Some stakeholders are subject to regulatory and lawful requirements. Therefore some future service based in SECURED that will be executed as part of this stakeholder's product portfolio will be asked for these regulations. Most frequently mentioned by the stakeholders are Lawful Interception, data retention, personal data and privacy.

4 Requirements description

In this section, a set of requirements identified by each of the stakeholders is described. The same previous structure of subsections organized by stakeholder has been intentionally selected to try to focus on the key points identified by each of them in previous sections.

It should be noted that some of the Requirements might seem repetitive for different stakeholders. This situation is preferred in opposition to a summarized general requirement section, because this approach allows us to keep records with detailed expectations for each stakeholder, which will drive later on the design and implementation phase.

4.1 End User

4.1.1 USR.1 – Mobility/Independence

Users should have security protection while switching from one network connection to another and among personal devices.

4.1.2 USR.2 – Performance

The NED should ensure good quality and performance, and should not impact excessively on the delay experienced while accessing the Internet.

4.1.3 USR.3 – Cost

The NED costs should be proportional to the security benefits offered. A strong effort is needed to keep the costs low, especially when aiming at residential users, and to highlight the security benefits it can bring.

4.1.4 USR.4 – Transparency

Users are interested in knowing that the NED is active and functioning correctly, as well as the impact it might have on their network activity, and what applications is executing for protecting their traffic.

4.1.5 USR.5 – Versatility

The NED should support a broad range of security applications, possibly with different configuration options and with the capability of offering users control (possibly shared with the network provider) over which applications are being executed and with what configuration.

4.1.6 USR.6 – Simplicity

The NED should be characterized by simplicity as a key design element: configuring the security options should be user friendly.

4.1.7 USR.6 – Data Processing

The NED should be able to process data that would not be possible to process otherwise.

4.2 ICT Manager

4.2.1 ICT.1 – User protection and policy enforcement when roaming (on the move)

Corporate policies should be able to follow an employee between different networks when travelling, where an agreement has been made between the business and an external service provider/telecom provider.

4.2.2 ICT.2 – NED must provide assurance of correct firmware

A network edge device should be able to be challenged to see whether it is running the correct firmware, as well as being able to provide some level of assurance on what services are running on it. This is in order to help protecting users from connecting to a network edge device with unauthorised (and potentially malicious) software.

4.2.3 ICT.3 – Mobile device security

Mobility in general should be well supported. Malware for mobile devices is growing, and nowadays corporate data is being delivered to employees' mobile devices. Therefore, we should support the capacity to create Personal Security Applications (PSA) for protecting mobile devices, e.g., to check malware.

4.2.4 ICT.4 – Security configuration complexity

Users and ICT managers prefer both rich and fine-grained as well as simple systems for security configuration. SECURED must support these needs.

4.2.5 ICT.5 – Anonymous security monitoring

There should be support for creation of PSAs that allow conducting anonymous monitoring on network traffic for security purposes.

4.2.6 ICT.6 – Privacy and confidentiality

The SECURED architecture should be able to encrypt all the data so that outsiders cannot inspect the traffic.

4.2.7 ICT.7 – User authentication

The SECURED architecture must support different authentications models. Complex models where users should be authenticated multiples times, from network access authentication, to SECURED platform (NED, PSC) and final applications (PSA) must be supported but also avoided. Not all authentications processes needs to be applied in every case; in simple models anonymous usage should be possible or basic authentication is enough.

4.2.8 ICT.8 – Antivirus and firewall applications

There should be support for creation of PSAs that offer antivirus and firewall services.

4.3 Developer of Security Applications

One preliminary consideration about identifying requirements from this category of users is that with the survey we can infer only main interests of developers in terms of preferred platforms and languages. At this stage, we cannot collect detailed opinions about the development environment (for example, which functions should be exposed through an API) until the SECURED main architecture (hardware and software components) will be defined.

4.3.1 DEV.1 – High-level source code language

Given the strong preference among developers on high-level languages, as reported in Section 4.3, development tools to be delivered by SECURED could be based on one of them (for example JAVA or python), but not exclusively. Alternatively, main libraries could be written in a low level language like C and exported to high-level languages through bindings.

4.3.2 DEV.2 – API

To encourage developers porting their existing applications to the new SECURED platform, the latter should offer at least feature parity in terms of operating systems or upper layers functions that can be exploited by security applications. This objective could be satisfied by exposing a rich Application Programming Interface (API) to developers or reusing existing ones in virtualization or paravirtualization techonologies.

4.3.3 DEV.3 – Use of emerging technologies

In order to get the benefits from emerging technologies (e.g. cloud, virtualization and software defined networks), SECURED should allow developers to exploit the enhanced features introduced by these technologies when building new network security products.

4.3.4 DEV.4 – Platform-independent deployment framework

SECURED must provide to the developers a deployment framework that is platform-independent. This requirement is in concordance with the specifications of the project regarding that the security applications can either be deployed in a network device or in a virtual device and they should be able to move on-the-fly. Furthermore, the platform-independent requirement is bound with the requirement DEV.1.

4.3.5 DEV.5 – Security applications and NED's performance.

SECURED must both derive the user traffic towards the security application and guarantee that no latency is introduced by the system in order to avoid impacting on the traffic speed and user experience. From the survey results we obtained that, developers are working in different types of well-known security applications, which require fast and efficient access to the user traffic, minimally impacting the overall speed. Thus, these applications once deployed on SECURED must be able to process the traffic without affecting the speed, consequently, the user experience.

4.3.6 DEV.6 – NED scalability

The applications developed for the SECURED system should guarantee an appropriate in-line processing rate of packets in order to not affect the user experience. This requirement will have impact not only on the architecture but also on the deployment system, as it has to be adaptable and well dimensioned to handle the scale of users and their traffic.

4.3.7 DEV.7 – Ease migration of security applications

To encourage developers to adopt the proposed security-offloading scenario, SECURED should provide tools that facilitate the porting procedure of pre-existing applications. This requirement aims to simplify the porting of the source code into the SECURED environment, for example, making it platform independent in accordance with DEV.1 and DEV.4.

4.3.8 DEV.8 – Developer's documentation

SECURED must provide developers with detailed documentation regarding its development and deployment framework. This requirement is in concordance with DEV.1 and DEV.2.

4.4 Network Operator/ISP

4.4.1 ISP.1 – Flexible and Scalable Architecture

The SECURED architecture must be flexible and scalable (within each NED, in the number of NEDs, PSAs, Provisioning, Maintenance, etc.).

The proposed architecture should be scalable in hardware and software resources, applications, services and users levels to allow security services from dozens to thousands of users. At the same time, it should allow some degree of flexibility so as to facilitate customization and configuration of the resources and services according to the users, services, applications or ISP/NO needs.

Besides, SECURED's provisioning should be flexible enough to allow massive management from ISP/NO needs and from users' demands. It should be allowed to register, deregister or update users and services in a scalable way, so that the needs required by NOs/ISPs and end-users are covered.

On the other hand, connections between SECURED elements and NO/ISP IT Systems (provisioning, billing, monitoring, etc.) have to be assured as well as compatibility with previous versions between applications (PSA) and SECURED elements (PSC, NED, etc.)

4.4.2 ISP.2 – Capabilities to Operate and Monitor Services

It is required the inclusion of mechanisms for monitoring the services and triggering alarms in case of any incident or anomaly. A set of procedures on how to act in case of a service failure has to be defined to ensure greater availability.

The mechanisms for service restoration after a failure should be as fast as possible, so it would be useful to have a tool or user interface that allows to create, destroy, start, stop, and monitor the status of the involved resources (virtual machines, devices, services…), not only to facilitate service maintenance but also the provisioning tasks.

Redundancy or backup mechanisms for services brought to the edge of the network are needed to prevent users to be without security services.

It is needed to provide to the final users with a configuration interface (web portal, API or another mechanism) that allows them to easily set their preferences and make updates.

4.4.3 ISP.3 – Assurance of Network Operators/ISPs Service Level Agreements

Applications and services provided by SECURED should ensure the compliance with the SLAs provided by ISPs/Network Operators in terms of performance and QoS.

It is important that the NED does not jeopardise any SLAs agreed between the ISP and its costumer. The NED hence must not influence any QoS levels expected by the costumer.

4.4.4 ISP.4 – Strong security requirements

The questionnaire results show a concern for operators about installing applications provided by third parties. For this reason there must be strong security requirements.

The edge device must support the ability of isolating the SECURED applications (PSA) running on behalf of the different users. If necessary, the communications among the SECURED applications will be done using external interfaces.

Redundancy, high availability or backup mechanisms for services brought to the NED are recommended to prevent users to be without security services.

It is also necessary to have mechanisms to ensure trust between the user and the Network Edge Device that will be hosting their SECURED applications.

Moreover, the SECURED architecture must support the capability to encrypt the communications channel between SECURED applications and the end devices. Auditability capacity must be included as well, for special needs or particular services.

4.4.5 ISP.5 – Categorization of applications

Different types of categories of applications (packet filtering, malware, security monitoring, etc.) must be supported by the SECURED architecture for ISPs/NOs, in order to facilitate service management and marketing products creation.

4.4.6 ISP.6 – NED can accommodate multiple PSAs and allow for future installations

An NED may host a large number of PSAs. PSAs from multiple third party providers may be available with only some being used for a particular customer. However the NED must provide sufficient space for collocation and future installations and hence the ISP must provide sufficient resources to accommodate for this need.

4.4.7 ISP.7 – Secure communication channel between NED and customer devices

Allow for secure communication tunnels between NED and customer devices where necessary. These could end up being in the order of thousands and should not place a burden or affect expected QoS levels across these access links.

4.5 Service Provider

Based on the questionnaire results we are able to gather a number of requirements that need to be satisfied by the proposed solutions in SECURED. It has to be noted that it would be beneficial for an SP to consider all aforementioned requirements of all stakeholders when it comes to offering any kind of service and in particular its customers' needs. Hence, although the proposed solutions will aim to satisfy the different stakeholders' requirements, it is in the interest of the SP to especially focus on possible business opportunities based on the customers' demand, their requirements, and preferences in general.

4.5.1 SP.1 – Serve all customers being offered connectivity

A distinction needs to be made between the type of devices that the technology targets to support. For example 100 FTTB customers will have different demands to 10000 Sensors. However all customers served under a specific interface need to be supported with security control.

4.5.2 SP.2 – Ensure that end-to-end security is not jeopardised

"*Not jeopardising end-to-end security provisioning as provided*" seems to have received a very mixed response by the Service Providers illustrating the uncertainty in what SECURED might provide and if the proposed solutions will tamper with existing security provisioning offered by the SP. End-to-end security should not be jeopardised at all service levels. Introducing additional

security at the network edge or even moving security components to the edge to improve terminal performance should not leave any security holes on the access side.

4.5.3 SP.3 –Equal or better performance than existing service during end-user mobility

The majority of Service Provider indicate that they are optimistic and that they think it is possible to provide network edge security that can support seamless mobility. The requirement here will be to place at least lower burden to service/session performance than existing methods.

4.5.4 SP.4 –Offer Virtual Network Security functions

The majority of the Service Providers show high interest in the provisioning of Virtual Network Security Functions and could hence be considered as a requirement. This is an option of interest rather than a requirement but since more or less all SPs support this it could be treated as requirement in the system design.

4.5.5 SP.5 – Allow third party security function providers to easily provide their own standalone packages

It is a requirement that the controller is flexible enough to allow for third party security components, packages, agents or drivers to be added seamlessly to the controller system.

4.5.6 SP.6 – Third party customised features should offer additional security functionality without affecting existing security services offered by the SP

Based on the questions related to offering customisable services it seems that the SPs are mainly worried that third parties customisable features will place a burden on the security services provided by them. To avoid this, it is required that third-party security features provide additional security and not jeopardise security services offered by the SP.

4.5.7 SP.7 – A security function must offer a complete standalone solution for a specific threat at the network edge

This is to say that a particular security function should offer a standalone solution and not be split (e.g. between the terminal and network edge).

4.6 Miscellanea

We list here requirements deduced from conclusions described in additional aspects in section 3.6.

4.6.1 MISC.1 – Backward compatibility

The SECURED design must guarantee backward compatibility between different versions. As a basic requirement, minor release changes in the software in any of the elements must guarantee that SECURED services remain running correctly. Only drastic changes could admit incompatibilities with older versions.

4.6.2 MISC.2 – Regulatory or legal compatibility

The SECURED architecture must be sufficiently flexible and extensible to suit into different national regulations, and types of stakeholders, like a Network Operator, a SME or an end user. Some examples can be:

- an ISP may be forced to apply lawful interception of the traffic in a user application;
- an SME must enforce a national law on personal data.

This does not mean that the SECURED architecture must consider all EU, national or regional regulations, on the contrary, what this requirement collects is the need for a configurable and flexible solution that may fit different regulations.

5 Summary of requirements

This section enumerates the list of requirements in order to improve the readability. The Table 1 is organized with three columns: assigned ID, stakeholder and requirement summary.

ID	*stakeholder*	*system requirement*
USR.1	End User	Mobility/Independence
USR.2	End User	Performance
USR.3	End User	Cost
USR.4	End User	Transparency
USR.5	End User	Versatility
USR.6	End User	Simplicity
USR.7	End User	Data Processing
ICT.1	ICT manager	User should have protection and policy enforcement when roaming (travel)
ICT.2	ICT manager	NED must provide assurance of correct firmware
ICT.3	ICT manager	Mobile device security
ICT.4	ICT manager	Security configuration complexity
ICT.5	ICT manager	Anonymous security monitoring
ICT.6	ICT manager	Privacy and confidentiality
ICT.7	ICT manager	User authentication
ICT.8	ICT manager	Antivirus and firewall applications
DEV.1	Developer	High-level source code language
DEV.2	Developer	Rich API
DEV.3	Developer	Use of emerging technologies
DEV.4	Developer	Platform-independent deployment framework
DEV.5	Developer	Security applications and NED performances
DEV.6	Developer	NED scalability
DEV.7	Developer	Easy migration of security applications
DEV.8	Developer	Developer’s documentation
ISP.1	NETOP / ISP	Flexible and scalable architecture
ISP.2	NETOP/ ISP	Capabilities to operate and monitor services
ISP.3	NETOP / ISP	Assurance of Network Operators/ISPs Service Level Agreements
ISP.4	NETOP / ISP	Strong security requirements
ISP.5	NETOP / ISP	Categorization of applications
SP.1	SP	Serve all customers being offered connectivity.

SP.2	SP	Ensure that end-to-end security is not jeopardised.
SP.3	SP	To allow for at least equal or better service performance than existing service during end-user mobility.
SP.4	SP	To be able to offer Virtual Network Security Functions.
SP.5	SP	Allow Third Party Security Function providers to easily provide their own standalone packages.
SP.6	SP	Third party customised features should offer additional security functionality without affecting existing security services offered by the SP.
SP.7	SP	A security function must offer a complete standalone solution for a single type of attack or thread at the network edge.
MISC.1	miscellanea	Backward compatibility
MISC.2	miscellanea	Regulatory or Legal compatibility

Table 1: User requirements summary

6 Summary and conclusions

The main objective of this deliverable encompasses different aspects aiming to define the user requirements for the SECURED project. The exercise executed to gather these requirements includes the definition of user taxonomy, the creation of different questionnaires targeting each stakeholder and the dissemination of them. Finally, based on the results from the survey, the requirements are defined, specifying each one according with the stakeholder.

The problem of defining the user requirements was approached by first defining the concept of "user" within SECURED. A SECURED user may be client surfing the Internet, a developer who is working in a new security application or a network operator who uses the technology to provide security to its clients. Thus, a deep analysis of all possible users was driven which focused on how each user may adopt or leverage the SECURED technology for their benefits. As a result, a user taxonomy definition was agreed between the partners. This taxonomy classifies the users in six groups: End Users, ICT Managers, Developers of Security Applications, Network Operators and Service Providers.

First thing it was discovered was that regardless the technical prowess of the partners in the SECURED consortium, coming from Academia, Manufacturing and Network Operation, it was necessary to get out of their respective walled gardens and reach out for a wider audience to avoid the SECURED project going astray. The raw material used in the requirements would be extracted from the result of questionnaires, so the actual needs and preferences of the potential SECURED users would be accurately gauged. Laterally, it was also discover that it could not be possible to talk about a single questionnaire but questionnaires, since there exists different user profiles with wide apart sets of targets and requirements.

Next, based on the classification of user profiles, the requirements definition task was split by considering the requirements of each stakeholder. To this end, a questionnaire targeting each profile was formulated. These questionnaires where disseminated by two main means: through an on-line web application and through print-out to be distributed in specific events, in. In order to maximise penetration in some partners' countries, they were written in three different languages: Spanish, Italian and English. As expected, most of the answers were received from the End User category (79% from the completed surveys, and 75% from the not completed ones). This is easily explainable by the specialised character of some of the stakeholder categories, which radically restricts the available population pool. Consequently, even if the population sample is small for some of the questionnaires, it is still representative.

After data collection and analysis, it was possible to define 7 requirements per each user profile, mainly 7 End User requirements, 8 for ICT Managers, 8 for Developers of Security Applications, 5 for Network Operators, and 7 for Service Operators. The final collection seems to be well balanced, with a slight bias to

those stakeholders which will effectively offload their security tools from their premises (home or enterprise) to the network edge or will be involved in the development of the security applications populating the SECURED nodes.

In summary, the requirements gathered from the different stakeholders are essential information that will drive the design of the SECURED architecture. Considering different stakeholders in this process of requirements definition have let us learn about different perspectives, expectations and opinions regarding this new security paradigm. Therefore, the SECURED architecture design should be as flexible, adaptable and scalable as possible with the clear aim of covering these requirements.

7 References

[1] L. Carroll, “Through a Looking Glass”, MacMillan, 1871

[2] The Trans-European Research and Education Networking Association, http://www.terena.org/

[3] Covert monitoring of devices, http://arstechnica.com/security/2014/01/nsa-uses-covert-radio-transmissions-to-monitor-100000-bugged-computers (accessed on 16/1/2014)

[4] IT Security Trends 2013, http://searchsecurity.techtarget.com/feature/IT-Security-Trends-2013-Mobile-security-concerns-tops-the-list (accessed on 16/1/2014)

[5] R. Bhadauria, S. Sanyal, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques”, International Journal of Computer Applications, Vol. 47, No. 18, June 2012, pp. 47-66

[6] U. Tovainen, “Championing Security over Crimeware: F-Secure, Nokia Solutions and Networks Join Forces”, http://www.f-secure.com/en/web/corporation_global/news-info/product-news-offers/view/story/1356578/Championing%20Security%20over%20Crimeware:%20F-Secure,%20Nokia%20Solutions%20and%20Networks%20Join%20Forces

[7] J. Raj, P. Subharthi, “Network Virtualization and Software Defined Networking for Cloud Computing: A Survey”, IEEE Communication Magazine, Vol. 51, Nov 2013, pp. 24-32

[8] “Network Functions Virtualisation (NFV), Architectural Framework”, ETSI GS NFV 002, v1.1.1 (2013-10) http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf

[9] F-Secure Freedome, http://freedome.f-secure.com/en/home.html#security (accessed on 16/1/2014)

Appendix A. Final questionnaires

This section includes the actual questionnaires as they were distributed among the relevant stakeholders

A.1 End Users

Q1. Select the category you belong to

- ☐ 1. End User
- ☐ 2. Corporate ICT Manager
- ☐ 3. Developer of Security Application
- ☐ 4. Network Operator / ISP
- ☐ 5. Service Provider

Q2. Which age range do you belong to?

- ☐ 1. Up to 18
- ☐ 2. 19-24
- ☐ 3. 25-44
- ☐ 4. 45-54
- ☐ 5. 55-65
- ☐ 6. Over 65

Q3 - In which country do you live?

Q4. How would you characterize your experience level related to the use of Internet?

- ☐ 1. Unfamiliar
- ☐ 2. Novice
- ☐ 3. Medium
- ☐ 4. Very good
- ☐ 5. Expert

Q5. How would you characterize your experience level related to the use of computers and networks?

- ☐ 1. Unfamiliar
- ☐ 2. Novice
- ☐ 3. Medium
- ☐ 4. Very good
- ☐ 5. Expert

Q6. Which device you normally use for Web navigation?

- ☐ 1. Desktop
- ☐ 2. Smart Phone
- ☐ 3. Tablet

- ☐ 4. Laptop

Q7. Which additional devices do you also use for Web navigation?

- ☐ 1. Desktop
- ☐ 2. Smart Phone
- ☐ 3. Tablet
- ☐ 4. Laptop
- ☐ 5. Other

Q9. Which sort of network access do you primarily use to connect to the Web?

- ☐ 1. WiFi (public hotspot)
- ☐ 2. WiFi (at work)
- ☐ 3. Wired access at home – fiber/cable/modem (e.g. DSL)
- ☐ 4. Wired access at work (E.g. Ethernet)
- ☐ 5. Mobile

Q10. Which sort of network access do you alternatively use to connect to the Web?

- ☐ 1. WiFi (public hotspot)
- ☐ 2. WiFi (at work)
- ☐ 3. Wired access at home – fiber/cable/modem (e.g. DSL)
- ☐ 4. Wired access at work (E.g. Ethernet)
- ☐ 5. Mobile

Q11. Which environment do you primarily leverage on to connect to the Web?

- ☐ 1. Home
- ☐ 2. Enterprise
- ☐ 3. Public place

Q12. Which other environments do you leverage on to connect to the Web?

- ☐ 1. Home
- ☐ 2. Enterprise
- ☐ 3. Public place

Q13. Which are the risks you perceive as most worrying when surfing online? Please, rate the following risk from least worrying (1) to most worrying (5)

- ☐ a. Virus (spyware/adware)
- ☐ b. Phishing scam
- ☐ c. Identity theft
- ☐ d. Financial information theft
- ☐ e. Grooming (minors)

- ☐ f. Child Online Exploitation (minors)
- ☐ g. Privacy violation
- ☐ h. Monitoring (by third parties)

Q14. Would you like to restrict access to some Internet pages when navigating from your home? (for you or any of your relatives)?

- ☐ 1. Yes
- ☐ 2. No
- ☐ 3. Don’t know

Q15. Would you like to be warned/asked a password if you are about to open a scam web page or a web page that might infect your device with a virus or malware?

- ☐ 1. Yes
- ☐ 2. No
- ☐ 3. Don’t know

Q16. Which are the activities you usually carry out with your smartphone? Please, rate the following activities from least used (1) to most used(5)

- ☐ a. Surfing the Web
- ☐ b. Online Banking
- ☐ c. Social networking
- ☐ d. Online gaming
- ☐ e. Secure communication (e.g. encrypted communication)
- ☐ f. Shopping online
- ☐ f. I don’t use smartphone

Q17. Does your computer have anti-virus software installed?

- ☐ 1. Yes
- ☐ 2. No
- ☐ 3. Don’t know

Q18. Does your mobile/tablet have anti-virus software installed?

- ☐ 1. Yes
- ☐ 2. No
- ☐ 3. Don’t know

Q19. How often is your anti-virus software updated (e.g., new version loaded, new virus definitions downloaded)

- ☐ 1. Every day
- ☐ 2. Every week
- ☐ 3. Every month

☐ 4. Don’t know

Q20. Are all your Internet-connected devices (e.g., smart tv, iptv, gaming console, tablet, home automation, etc.) protected from Internet threats?

☐ 1. Yes

☐ 2. No

☐ 3. Don’t know

Q21. Would you like to be able to define by yourself how your different Internet-connected devices (e.g., smart phone, smart tv, gaming console) are protected (e.g., what a certain device can do in the internet)?

☐ 1. Yes

☐ 2. No

☐ 3. Don’t know

Q22. Would you like to check the security status (e.g., blocked connections, number of blocked suspicious applications) every now and then? Please, answer this question if you check options ‘4-Very Good’ or ‘5-Expert’ in questions Q3 or Q4

☐ 1. Yes

☐ 2. No

☐ 3. Don’t know

Q23. Do you use peer-to-peer file sharing software/programs (such as BitTorrent, Direct Connect, eDonkey, eMule, Napster, Kazaa, etc.)?

☐ 1. Yes

☐ 2. No

If you check ‘Yes’, please specify

Q24. Do you use remote access (e.g. dial-in, wireless system, cable, satellite) to access the network of your employer externally (e.g. from home or while travelling?

☐ 1. Yes

☐ 2. No

If you check ‘Yes’, please specify

Q25. If you use a wireless network at home, have you configured it in a secured way (e.g. encryption enabled or password-based access control)?

☐ 1. Yes

☐ 2. No

If you check ‘Yes’, please specify

Q26. If you work from home, do you use a VPN (Virtual Private Network) to connect to your organization’s network?

☐ 1. Yes

☐ 2. No

Q27. Do other people (your spouse, family, friends, etc.) sometime use your own devices?

☐ 1. Yes

☐ 2. No

Q28. If you upload information (files etc.) to the Internet (your website, your webpage, your blog, your company's network, etc.), do you use a secure (encrypted) connection?

☐ 1. Yes

☐ 2. No

If you check 'Yes', please specify

Q29. How concerned are you about your privacy in the internet?

☐ 1. Strongly concerned

☐ 2. Somewhat concerned

☐ 3. Neutral

☐ 4. Marginally concerned

☐ 4. Not concerned

Q30. How much important is for you the possibility to connect to the network in an anonymous way?

☐ 1. Very much

☐ 2. Somewhat

☐ 3. Undecided

☐ 4. Not really

Q31. Would you feel comfortable in a scenario where you must always prove your identity (i.e. authenticate yourself) before connecting to the network?

☐ 1. Yes

☐ 2. Yes, but I would like to have an option to connect to the network in an anonymous way

☐ 3. Neutral

☐ 4. No, unless I have strong guarantees about my privacy

☐ 5. No, I would not accept this

Q32. If you have kids, do you have any restriction or ad-hoc protection software for the Internet explored by your kids? And on which device?

☐ 1. Yes

☐ 2. No

☐ 3. No, I don't have kids

If you check 'Yes', please specify

Q33. Are you concerned about network security when accessing Internet while travelling?

- ☐ 1. Very much
- ☐ 2. Somewhat
- ☐ 3. Indifferent
- ☐ 4. Not really
- ☐ 5. Not at all

Q34. Would you like to have a protection service that moves with you and is independent of the device that you use to access the network?

- ☐ 1. Very much
- ☐ 2. Somewhat
- ☐ 3. Undecided
- ☐ 4. Not really
- ☐ 5. Not at all

Q35. Would you be willing to allow your Network provider to provide security applications for your network connection(s) instead of installing security applications onto each of your devices?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q36. Do you find it difficult to install and configure security applications in your devices (e.g. anti-virus)?

- ☐ 1. Very much
- ☐ 2. Somewhat
- ☐ 3. Neutral
- ☐ 4. Not really
- ☐ 5. Not at all
- ☐ 6. I did never install security applications

Q37. Would you be willing to install new applications (or update existing ones) on your devices to support new security services?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q38. Suppose that you have the possibility to remove all your security software (antivirus, firewall…) from your personal electronic devices (PC, smartphone, …) and demand all protection to your Internet provider or network device. How much additional delay for your Internet operations would you tolerate or expect?

- ☐ 1. Almost none
- ☐ 2. 1-2 seconds
- ☐ 3. 3-9 seconds
- ☐ 4. 10+ seconds

Q39. Would you be willing to have third party's security software installed on your smartphone?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no
- ☐ 6. I don’t use a smartphone

Q40. Would you accept that your Internet provider handles the majority of network security operations for you?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably n0
- ☐ 5. Definitely no

Q41. Would you be willing to pay for the new security services?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably n0
- ☐ 5. Definitely no

Q42. Would you be willing to pay your Internet provider for added-value security features?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably n0
- ☐ 5. Definitely no

Q43. How would you find the idea of having the same kind/level of protection while switching from one

network connection to another or changing your personal device?

- ☐ 1. Strongly agree
- ☐ 2. Somewhat agree
- ☐ 3. Neutral
- ☐ 4. Somewhat disagree
- ☐ 5. Strongly disagree

Q44. How satisfied are you with the current security applications available in the market for your electronic device? Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4

- ☐ 1. Very much
- ☐ 2. Somewhat
- ☐ 3. Undecided
- ☐ 4. Not really
- ☐ 5. Not at all

Q45. Would you be willing to allow for the Internet provider to handle network security at the "edge of the network" (e.g. at DSL routers or public wifi access points) for improved performance?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q46. Do you think that moving security filters (e.g. packet filtering functions) from your personal device to the network edge could provide better security support? Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q47. Would you be willing to permit automatic but anonymous inspection (i,e, users are not tracked) of network traffic for security monitoring purposes? Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q48. A common trend nowadays is "network application offloading", that is implementing some applications into the network rather than on end-user devices. In this scenario, would you be concerned that your Internet provider could theoretically inspect all your network traffic when providing these additional services? Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4

- ☐ 1. A lot
- ☐ 2. Yes, but I can accept this risk given the advantages I get
- ☐ 3. Neutral
- ☐ 4. I don't think this is a big issue
- ☐ 5. Not an issue

Q49. Are you willing to delegate additional network security services to your Internet provider, or do you prefer to delegate these services to a different entity (e.g., a company that you trust)? Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4.

- ☐ 1. Any ISP/company is fine, as it would be the best from the performance point of view
- ☐ 2. Any ISP/company is fine, but I need specific additional guarantees (e.g., trusted computing)
- ☐ 3. Neutral
- ☐ 4. I would prefer a specific company that I trust
- ☐ 5. I require that the "network application offloading" is implemented on my own servers

Q50. Given the "network application offloading" mechanism in place, would you use it for "professional" services (e.g., trusted connections to/from your corporate network) or "domestic" services (e.g., protecting you and your family from Internet threats)? Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4

- ☐ 1. Only "professional" services
- ☐ 2. Mostly "professional" services
- ☐ 3. Both "professional" and "domestic" services
- ☐ 4. Mostly "domestic" services
- ☐ 5. Only "domestic" services

Q51. As a domestic user, how much would you be willing to pay for protection implemented as a "network application offloading" service? Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4

- ☐ 1. > 10€/month per user
- ☐ 2. Between 5 and 10€/month per user
- ☐ 3. Between 2 and 5€/month per user
- ☐ 4. Less than 2€/month per user
- ☐ 5. No fee

Q52. Beside security applications, do you foresee additional applications that may be usefully implemented in a "network application offloading" scenario? Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4

Q53. What kind of security application are you interested in? (Multiple choice) Please, answer this question if you check options '4-Very Good' or '5-Expert' in questions Q3 or Q4

- ☐ 1. Packet filtering
- ☐ 2. Malware detection
- ☐ 3. Network security monitor and intrusion detection
- ☐ 4. VPN client
- ☐ 5. Privacy protection
- ☐ 6. Other

If you check 'Other', please specify which

Q54. Would you prefer configuration options to be available for each of the following security services:

a) To define privacy and anonymity levels

- ☐ 1. Strongly Disagree
- ☐ 2. Somewhat Disagree
- ☐ 3. Neutral
- ☐ 4. Somewhat Agree
- ☐ 5. Strongly Agree

b) To define access control to web pages with different categories (child-safe, commercial)

- ☐ 1. Strongly Disagree
- ☐ 2. Somewhat Disagree
- ☐ 3. Neutral
- ☐ 4. Somewhat Agree
- ☐ 5. Strongly Agree

c) To block certain web pages (blacklisting)

- ☐ 1. Strongly Disagree
- ☐ 2. Somewhat Disagree
- ☐ 3. Neutral
- ☐ 4. Somewhat Agree
- ☐ 5. Strongly Agree

d) To block certain IP addresses or network protocols

- ☐ 1. Strongly Disagree
- ☐ 2. Somewhat Disagree
- ☐ 3. Neutral
- ☐ 4. Somewhat Agree
- ☐ 5. Strongly Agree

e) To deny network access for certain applications installed on your device

- ☐ 1. Strongly Disagree
- ☐ 2. Somewhat Disagree

- ☐ 3. Neutral
- ☐ 4. Somewhat Agree
- ☐ 5. Strongly Agree

f) To define what are the acceptable web pages (whitelisting)

- ☐ 1. Strongly Disagree
- ☐ 2. Somewhat Disagree
- ☐ 3. Neutral
- ☐ 4. Somewhat Agree
- ☐ 5. Strongly Agree

A.2 Corporate ICT Managers

Q1. Select the category you belong to

- ☐ 1. End User
- ☐ 2. Corporate ICT Manager
- ☐ 3. Developer of Security Application
- ☐ 4. Network Operator / ISP
- ☐ 5. Service Provider

Q2. Which age range do you belong to?

- ☐ 1. Up to 18
- ☐ 2. 19-24
- ☐ 3. 25-44
- ☐ 4. 45-54
- ☐ 5. 55-65
- ☐ 6. Over 65

Q3. What countries does your company operate in?

Q3.1. How many employees work in your company?

- ☐ 1 – Less than 50
- ☐ 2 – 51-100
- ☐ 3 – 101-500
- ☐ 4 – 501-1000
- ☐ 5 – More than 1000

Q4. Which services does your company expose to Internet

- ☐ 1 - Web
- ☐ 2 - Database
- ☐ 3 - FTP

- ☐ 4 - SSH
- ☐ 5 - Other

If you check ‘Other’, please specify

Q5. Which technology is in place to protect network segments from hostile traffic?

- ☐ 1 – Firewalls (packet filter)
- ☐ 2 - Router/switch ACLs (Access Control List)
- ☐ 3 - Host-based IP filters
- ☐ 4 - Filters
- ☐ 5 – Reverse proxy
- ☐ 6 - Other

If you check ‘Other’, please specify

Q6. Do you permit remote access (e.g dial-in, wireless, cable, satellite) to your organization’s network for employees working externally (e.g. from home or while travelling)?

- ☐ 1 - Yes
- ☐ 2 - No

If you check ‘Yes’, please specify

Q7. Does your organization have policies and procedures in place to mitigate the Information Security risks associated with the use of the mobile devices (e.g., tablets and smartphones)?

- ☐ 1 - Yes
- ☐ 2 - No

If you check ‘Yes’, please specify

Q8. Would you be willing to learn a new policy language (I.e. a language to configure network security controls) to achieve better security?

- ☐ 1 - Definitely yes
- ☐ 2 - Probably yes
- ☐ 3 - Undecided
- ☐ 4 - Probably no
- ☐ 5 - Definitely no

Q9. How difficult would it be to adopt new edge devices (e.g. new types of switch, router or wireless access point) into your existing infrastructure?

- ☐ 1. Very difficult
- ☐ 2. Somewhat difficult
- ☐ 3. Manageable
- ☐ 4. Easily
- ☐ 5. Frictionlessly

Q10. A common trend nowadays is "network application offloading", that is implementing some applications into the network rather than end-user devices. Do you believe that moving applications from clients to network edge devices (that is "network application offloading") will make IT management more difficult?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q11. If better protection and multitenancy support would be available for network resources, then would you be willing to share your network infrastructure with guest users?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q12. Are you concerned about insiders tampering with network edge devices?

- ☐ 1. Yes
- ☐ 2. No

Q13. Would you accept to have third party's security software installed in your company devices?

- ☐ 1. Very much
- ☐ 2. Somewhat
- ☐ 3. Undecided
- ☐ 4. Not really
- ☐ 5. Not at all

Q14. Would you be interested in your network provider to execute security applications on its core network devices rather than having security applications installed to each end-user device?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q15. In a “network application offloading” scenario, would you be concerned that your network provider could theoretically inspect all your network traffic when providing these additional services?

- ☐ 1. A lot

- ☐ 2. Yes, but I can accept this risk given the advantages I get
- ☐ 3. Neutral
- ☐ 4. I don't think this is a big issue
- ☐ 5. Not an issue

Q16. Are you willing to delegate the "network application offloading" service to your network provider, or do you prefer to delegate this service to a different entity (e.g., a company that you trust)?

- ☐ 1. Any ISP/company is fine, as it would be the best from the performance point of view
- ☐ 2. Any ISP/company is fine, but I need specific additional guarantees (e.g., trusted computing)
- ☐ 3. Neutral
- ☐ 4. I would prefer a specific company that I trust
- ☐ 5. I require that the "network application offloading" is implemented on my own servers

Q17. How much would you be willing to pay for the "network application offloading" service for your company and its employees?

- ☐ 1. >10€/month per user
- ☐ 2. Between 5 and 10€/month per user
- ☐ 3. Between 2 and 5€/month per user
- ☐ 4. Less than 2€/month per user
- ☐ 5. Less than 1000€/month (flat rate)
- ☐ 6. More than 1000€/month (flat rate)
- ☐ 7. No fee

Q18. Beside security applications, do you foresee additional applications that may be usefully implemented in a “network application offloading” scenario?

Q19. Would you feel comfortable in a scenario where your employees must always prove their identity (i.e. authenticate themselves) before connecting to the network?

- ☐ 1. Yes
- ☐ 2. Yes, but I would like to have an option to connect to the network in an anonymous way
- ☐ 3. Neutral
- ☐ 4. No, unless I have strong guarantees about my privacy
- ☐ 5. No, I would not accept this

Q20. Would you be willing to permit automatic but anonymous inspection (i.e. employees are not tracked) of network traffic for security monitoring purposes?

- ☐ 1. Strongly agree
- ☐ 2. Somewhat agree
- ☐ 3. Neutral
- ☐ 4. Somewhat disagree
- ☐ 5. Strongly disagree

Q21. Would you prefer to have a rich and fine-grained system (but complex to use) for security configuration or more simple but less powerful one?

- ☐ 1. Strong preference for the simple one
- ☐ 2. Mild preference for the simple one
- ☐ 3. Neutral
- ☐ 4. Mild preference for the complex one
- ☐ 5. Strong preference for the complex one

Q22. Would you trust delegating your security controls to a cloud service?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q23. What aspects of your current network security process would need improvements? (Please provide also a comment)

- Costs
- Level of security
- Mobility support
- Applying and modifying security policies
- Protecting confidential information

Q24. Which of the previously described aspects could be improved by offloading of network security features from end-user devices to internal network devices?

Q25. What are the main network security controls that you are willing to invest in?

Q26. What is the feedback from your employees about your current network security services?

Q27. Which of your corporate network security controls would you be willing to offload from employee devices to your internal network devices?

A.3 Security Developers

Q1. Select the category you belong to

- ☐ 1. End User
- ☐ 2. Corporate ICT Manager
- ☐ 3. Developer of Security Application
- ☐ 4. Network Operator / ISP
- ☐ 5. Service Provider

Q2. Which age range do you belong to?

- ☐ 1. Up to 18
- ☐ 2. 19-24
- ☐ 3. 25-44
- ☐ 4. 45-54
- ☐ 5. 55-65
- ☐ 6. Over 65

Q2.1. How long have you been programming?

- ☐ 1. Less than 1 year
- ☐ 2. 1-5 years
- ☐ 3. 6-10 years
- ☐ 4. More than 10 years

Q3. In which country do you live?

Q4. If you would develop a security application for a new generation network device, which kind of platform would you prefer to work on?

- ☐ 1. Complete Windows x86 platform
- ☐ 2. Complete Linux/UNIX x86 platform
- ☐ 3. Embedded ARM platform but with OS support (Linux or Windows)
- ☐ 4. Architecture specific platform
- ☐ 5. Other

If you check 'Other', please specify

Q5. Which programming framework(s) do you prefer?

- ☐ 1. Low Level programming language
- ☐ 2. High Level programming language
- ☐ 3. Scripting language
- ☐ 4. SDK (software development kit)
- ☐ 5. API (Application Programming Interface)
- ☐ 6. Other

If you check 'Other', please specify

Q6. What kind(s) of security application are you designing or working on? (multiple choice)

- ☐ *1. Packet filtering*
- ☐ *2. Malware detection*
- ☐ *3. Network security monitor and intrusion detection*
- ☐ 4. VPN client

- ☐ 5. Privacy protection
- ☐ 6. Other

If you check ‘Other’, please specify

Q7. Which kind(s) of security application for network filtering are you designing or working on? (multiple choice)

- ☐ 1. Firewall (packet filtering)
- ☐ 2. Parental Control
- ☐ 3. Other

If you check ‘Other’, please specify

Q8. What kind(s) of security application for malware detection are designing or working on? (multiple choice)

- ☐ 1. Antivirus
- ☐ 2. Spam protection
- ☐ 3. Phishing detection
- ☐ 4. Other

If you check ‘Other’, please specify

Q9. What kind(s) of security application for network security monitor and/or intrusion detection are you designing or working on? (multiple choice)

- ☐ 1. Denial of Service / Distributed Denial of Service protection
- ☐ 2. Intrusion Detection System / Intrusion Prevention System functions
- ☐ 3. Security Gateway
- ☐ 4. Other

If you check ‘Other’, please specify

Q10. A common trend nowadays is "network application offloading", that is implementing some applications into the network rather than on end-user devices. In this scenario, some selected applications run in a "network edge device", such as router or wireless access point. Costs aside, would you be willing to port your existing security application(s) to run on a network edge device?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q11. Would you be willing to expand your security applications and services towards the network application offloading scenario?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes

- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q12. In your opinion, what aspects of offloading network security from end-user devices to network edge devices would enhance your business?

Q13. In your opinion, what will be the preferred technologies to implement network security products in the future?

A.4 Network Operators/ISP

Q1. Select the category you belong to

- ☐ 1. End User
- ☐ 2. Corporate ICT Manager
- ☐ 3. Developer of Security Application
- ☐ 4. Network Operator / ISP
- ☐ 5. Service Provider

Q2. Which age range do you belong to?

- ☐ 1. Up to 18
- ☐ 2. 19-24
- ☐ 3. 25-44
- ☐ 4. 45-54
- ☐ 5. 55-65
- ☐ 6. Over 65

Q3. In which country do you live?

Q4. Would you be willing to offer to your subscribers seamless security services on the move within your network?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q5. Do you consider feasible the implementation of a new network technology that supports seamless end-user mobility on your access network?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no

☐ 5. Definitely no

Q6. Would you be willing to offer to your subscribers (both home and corporate users) customizable security features integrated in your network?

☐ 1. Definitely yes
☐ 2. Probably yes
☐ 3. Undecided
☐ 4. Probably no
☐ 5. Definitely no

Q6.1. Willing to offer a security-on-the-edge service to your customers, how many users do you expect to be supported by the device which provides the service?

☐ 1. Less than 100
☐ 2. 100 – 1,000
☐ 3. 1,000 – 10,000
☐ 4. 10,000 – 100,000
☐ 5. More than 100,000

Q7. Do you believe that you would be able to attract more subscribers by offering them enhanced security features?

☐ 1. Definitely yes
☐ 2. Probably yes
☐ 3. Undecided
☐ 4. Probably no
☐ 5. Definitely no

Q8. Would you be willing to allow your subscribers to define their security features according to their preferences? (related to Q3)

☐ 1. Definitely yes
☐ 2. Probably yes
☐ 3. Undecided
☐ 4. Probably no
☐ 5. Definitely no

Q9. Do you think that moving security support from end-user devices to network edge devices (e.g. routers, wireless access points) would jeopardize end-to-end network security provisioning?

☐ 1. Definitely yes
☐ 2. Probably yes
☐ 3. Undecided
☐ 4. Probably no
☐ 5. Definitely no

Q10. Do you think moving security support from end-user devices to network edge devices would create further business opportunities for an ISP?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q11. How difficult do you think would be to offer personalized security services at the edge of the network?

- ☐ 1. Very difficult
- ☐ 2. Somewhat difficult
- ☐ 3. Undecided
- ☐ 4. Not really difficult
- ☐ 5. Not difficult at all

Q12. Would you be willing to offer virtual network security functions provided by third parties?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q13. Do you think that moving security packet filtering functions from end-user devices to network edge devices would provide better security support?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q14. Would you accept to install third party's security applications (trusted and certified) into your network?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q15. Which kind(s) of security application have you implemented or are you planning to implement in the

next couple of years? (Multiple choice)

- ☐ 1. Packet filtering
- ☐ 2. Malware detection
- ☐ 3. Network security monitor and intrusion detection
- ☐ 4. VPN client
- ☐ 5. Privacy
- ☐ 6. Other

If you check 'Other', please specify

Q16. Which kind(s) of security application for network filtering have you implemented or are you planning to implement in the next couple of years? (Multiple choice)

- ☐ 1. Firewall
- ☐ 2. Parental Control
- ☐ 3. Other

If you check 'Other', please specify

Q17. Which kind(s) of security application for malware detection have you implemented or are you planning to implement in the next couple of years? (Multiple choice)

- ☐ 1. Antivirus
- ☐ 2. Spam protection
- ☐ 3. Phishing detection
- ☐ 4. Other

If you check 'Other', please specify which

Q18. Which kind(s) of security application for network security monitoring and intrusion detection have you implemented or are you planning to implement in the next couple of years? (multiple choice)

- ☐ 1. Denial of Service / Distributed Denial of Service protection
- ☐ 2. Intrusion Detection System / Intrusion Prevention System functions
- ☐ 3. Security Gateway
- ☐ 4. Other

If you check 'Other', please specify which

Q19. Moving security functions to a network edge device is part of a common trend towards "network application offloading", that is implementing some applications into the network rather than on end-user devices. How would you see this approach fit with the future Internet architecture?

A.5 Service Provider

Q1. Select the category you belong to

- ☐ 1. End User
- ☐ 2. Corporate ICT Manager
- ☐ 3. Developer of Security Application

- ☐ 4. Network Operator / ISP
- ☐ 5. Service Provider

Q2. Which age range do you belong to?

- ☐ 1. Up to 18
- ☐ 2. 19-24
- ☐ 3. 25-44
- ☐ 4. 45-54
- ☐ 5. 55-65
- ☐ 6. Over 65

Q3. In which country do you live?

Q4. Would you be willing to offer to your subscribers seamless security services on the move within your network?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q5. Do you consider feasible the implementation of a new network technology that supports seamless end-user mobility on your access network?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q6. Would you be willing to offer to your subscribers (both home and corporate users) customizable security features integrated in your network?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q6.1. Willing to offer a security-on-the-edge service to your customers, how many users do you expect to be supported by the device which provides the service?

- ☐ 1. Less than 100
- ☐ 2. 100 – 1,000

- ☐ 3. 1,000 – 10,000
- ☐ 4. 10,000 – 100,000
- ☐ 5. More than 100,000

Q7. Do you believe that you would be able to attract more subscribers by offering them enhanced security features?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q8. Would you be willing to allow your subscribers to define their security features according to their preferences? (related to Q3)

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q9. Do you think that moving security support from end-user devices to network edge devices (e.g. routers, wireless access points) would jeopardize end-to-end network security provisioning?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q10. Do you think moving security support from end-user devices to network edge devices would create further business opportunities for an ISP?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q11. How difficult do you think would be to offer personalized security services at the edge of the network?

- ☐ 1. Very difficult
- ☐ 2. Somewhat difficult
- ☐ 3. Undecided

- ☐ 4. Not really difficult
- ☐ 5. Not difficult at all

Q12. Would you be willing to offer virtual network security functions provided by third parties?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q13. Do you think that moving security packet filtering functions from end-user devices to network edge devices would provide better security support?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q14. Would you accept to install third party's security applications (trusted and certified) into your network?

- ☐ 1. Definitely yes
- ☐ 2. Probably yes
- ☐ 3. Undecided
- ☐ 4. Probably no
- ☐ 5. Definitely no

Q15. Which kind(s) of security application have you deployed or planning to deploy? (Multiple choice)

- ☐ 1. Packet filtering
- ☐ 2. Malware detection
- ☐ 3. Network security monitor and intrusion detection
- ☐ 4. VPN client
- ☐ 5. Privacy protection
- ☐ 6. Other

If you check ‘Other’, please specify

Q16. Which kind(s) of security application for network filtering have you deployed or planning to deploy? (Multiple choice)

- ☐ 1. Firewall
- ☐ 2. Parental Control
- ☐ 3. Other

If you check ‘Other’, please specify

Q17. Which kind(s) of security application for malware detection have you deployed or planning to deploy? (multiple choice)

- ☐ 1. Antivirus
- ☐ 2. Spam protection
- ☐ 3. Phishing detection
- ☐ 4. Other

If you check ‘Other’, please specify which

Q18. Which kind(s) of security application for network security monitor and/or intrusion detection have you deployed or planning to deploy? (Multiple choice)

- ☐ 1. Denial of Service / Distributed Denial of Service protection
- ☐ 2. Intrusion Detection System / Intrusion Prevention System functions
- ☐ 3. Security Gateway
- ☐ 4. Other

If you check ‘Other’, please specify which

Appendix B. Business interest

From the questionnaires and the corresponding analysis for each stakeholder it is possible to gather more than just requirements and this additional input is included here for future use within the project. Here certain statistics are captured and presented to illustrate the NO/ISPs interest and willingness in deploying the proposed technology.

Figure 6 (a) is a plot of the responses of whether an ISP is willing to incorporate customizable features in its network with Figure 6 (b) showing whether ISPs feel they will attract more subscribers by doing so. Clearly the majority of ISPs are willing to offer customizable features (61%) with a large number undecided or being uncertain. Similarly the majority of ISPs feel they could attract more customers (51%) with a large number being uncertain (44%). This could be due to the fact that the technology has not been developed yet hence the confidence is low.

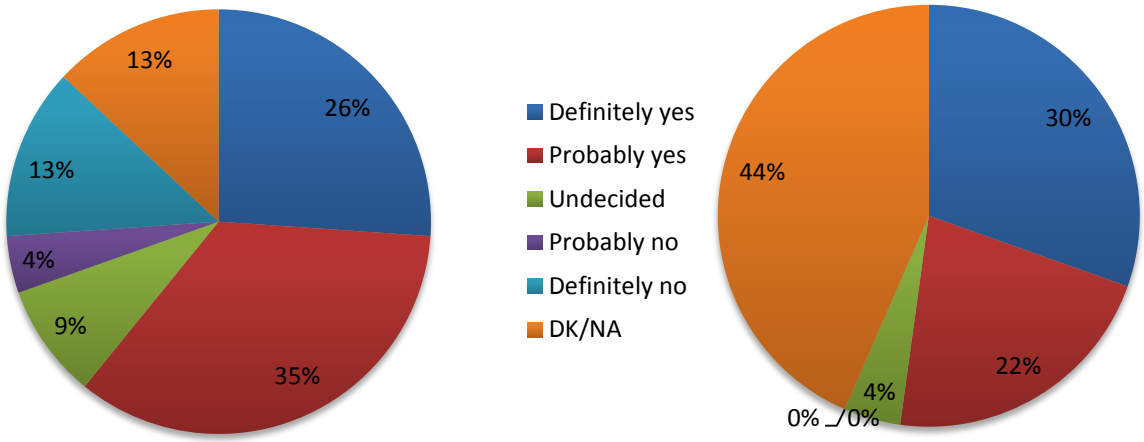

Figure 6 (a) Q. Would you be willing to offer to your subscribers (both home and corporate users) customizable security features integrated in your network? (b) Q. Do you believe that you would be able to attract more subscribers by offering them enhanced security features?

Figure 7 (a) shows whether ISPs are confident enough to allow for customers/subscribers to define their own security features. A large number said yes (39%), with a high percentage being uncertain. Figure 7 (b) illustrates clearly the belief that having NED security provisioning will open business opportunities for ISPs with 61% saying yes to the corresponding question. Figure 8 (a) and (b) Illustrate that a large number of ISPs are willing to offer third party service provider Virtual Network Security Functions as well as installing third party Security Applications with a fairly large number not being certain. The latter could be due to lack of knowledge on the deployment options and the clear placeholders of such technology.

A clear business model example is F-Secure who has published a security application (VPN application) in which the user's traffic is inspected in F-Secure's cloud to block attacks, e.g. malware [9].

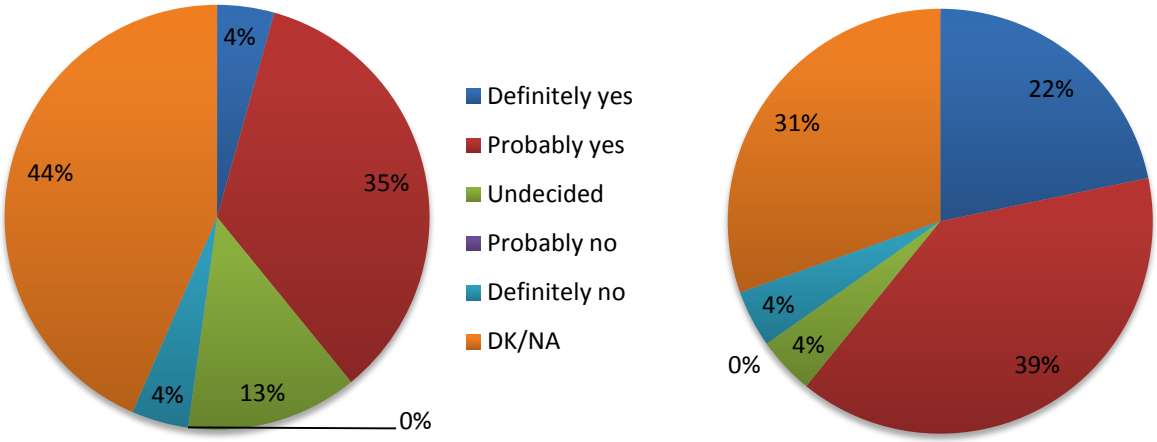

Figure **7** (a) Q. Would you be willing to allow your subscribers to define their security features according to their preferences?, (b) Q. Do you think moving security support from end-user devices to network edge devices would create further business opportunities for an ISP?

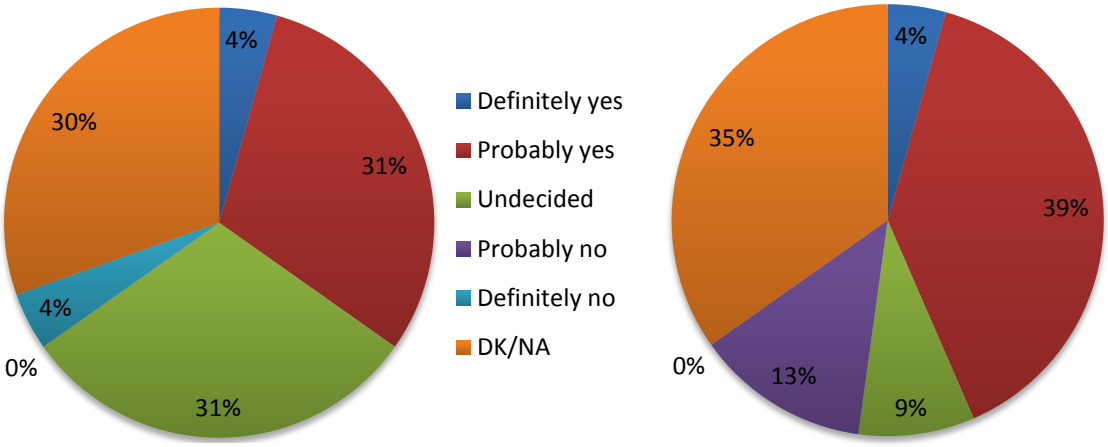

Figure 8 (a) Q. Would you be willing to offer virtual network security functions provided by third parties? (b) Q. Would you accept to install third party's security applications (trusted and certified) into your network?

Appendix C. Abbreviations

DDoS	Distributed Denial of Service
ESNOG	España Network Operators Group
FTP	File Transfer Protocol
ICT	Information and Communications Technology
IDS/IPS	Intrusion Detection/Prevention system
ISP	Internet Service Provider
NED	Network Edge Device
NO	Network Operator
PC	Personal Computer
PSA	Personal Security Application
PSC	Personal Security Controller
QoE	Quality of Experience
QoS	Quality of Service
SDN	Software-defined Networking
SECURED	Security at the Network Edge
SFTP	SSH File Transfer Protocol
SLA	Service Level Agreement
SP	Service Provider
SSH	Secure Shell
STREP	Specific Targeted Research Projects
TERENA	Trans-European Research and Education Networking Association
URL	Uniform Resource Locator
VPN	Virtual Private Network
XML	Extensible Markup Language