EISPP Results

Identifier: **EISPP-D6-003-TR**

Version 1.0

Date 2004/05/11

Table of Content

Glossary

ASP	Application Service Provider
BoF session	"Birds of a Feather" session. During the annual conference of the FIRST, the "BoF sessions" are special meetings dedicated to hot topics
BT	British Telecom
CCIT	Chambre de Commerce et d'Industrie de Toulouse
CEISNE	Co-operative European Information Security Network of Expertise
CERT	Computer Emergency Response Team [1]
CLUSIx	This acronym is derived from French (CLUb de la Sécurité des Systèmes d'Information) and is the name of several European Information Security Associations in the field of IT-security promotion: CLUSIF (France), CLUSIB (Belgium), CLUSIT (Italy)
CoC	Chamber of Commerce
CSIRT	Computer Security Incident Response Team [2]
CVE	Common Vulnerability Exposure. CVE is a de-facto standard to assign a unique reference number to each vulnerability (see http://cve.mitre.org for further information)
DTD	Document Type Definition
EC	European Community
EISPP	European Information Security Promotion Programme
EISPP CERT	A CERT which joined the EISPP project and gets access to the exchange infrastructure
EU	European Union
FIRST	Forum of Incident Response and Security Teams
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP / HTTPS	Hyper Text Transfer Protocol. HTTP is the default transport protocol for the Web. HTTPS is a secured version of HTTP
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IS	Information Systems
ISP	Internet Service Provider
IST	Information Society Technologies
IT	Information Technologies
NAI	Network Associates Inc.
PCC	Progress Coordination Committee

[1] In the present document, CERT and CSIRT are considered synonymous terms

[2] Same as above

PKI	Public Key Infrastructure
ROI	Return On Investment
SME	Small to Medium size Enterprise
S/MIME	Secure/Multipurpose Internet Mail Extension
SMTP	Simple Mail Transport Protocol. The standard protocol used to transport e-mails over Internet
TERENA	Trans-European Research and Education Networking Association
TF-CSIRT	Task Force for Computer Security Incident Response Team
UK	United Kingdom
WP	Work Package
WPi	Work Package #i
XML	eXtended Markup Language
xSP	Service Provider on Internet

Related documents

Applicable Documents

Ref.	*Title*	*Version*	*Date*
AD01	CONTRACT No IST-2001-35200 and Annexes		
AD02	Project Consortium Agreement		
AD03	Annex 1 - Description of Work	6.0	2003/03/20

Reference Documents

Ref.	*Title*	*Version*	*Date*
RD01	Evaluation methodology and Criteria EISPP-D6-001-TR	1.2	2003/04/10
RD02	EISPP Project Report EISPP-D6-002-TR	1.0	2004/01/28

1. EXECUTIVE SUMMARY

The European Information Security Promotion Programme (**EISPP**) strives to set up a network of expertise with the aim of providing European SMEs with those IT Security services that give them the necessary trust in e-commerce to develop their businesses in that direction. EISPP is a project funded by the EU through the fifth European Framework Program within the thematic program Information Society Technologies (IST). The project started in June 2002 and ended in January 2004.

EISPP pursued the following secondary objectives:

1. to set up a network of expertise among the European CERTs which will allow them to share and enhance their own prevention material and to "open" it to the other CERTs and organisations involved in prevention;
2. to provide SMEs with adapted, useable and efficient services;
3. the dissemination of project results to the European SMEs and to the other key players.

The present document gives an overview over the complete EISPP project. It describes management and coordination of the EISPP project, reviews EISPP's objectives and methodology, presents the results and achievements of EISPP, and provides an outlook over follow-up actions initiated through the EISPP project. The results, achievements, and positive outlook demonstrate that –within the limitations applying to a take-up action between partners present within five European countries– EISPP has achieved its objectives and prepared the ground for further work. Thus, EISPP will continue to influence the European IT security landscape long after the end of the project.

2. MANAGEMENT AND COORDINATION

2.1. The consortium

The project consortium is constituted of seven participants that bring a good level of knowledge in the project context and a complementary approach.

It gathers different types of actors that can have to play a role in providing IT Security services to SME. The consortium is constituted of:

- four CERTs of different types (self-financing units or internal teams),
- a Security Services and Products provider,
- a CLUSIx, IT security promoter,
- and a xSP, Service Provider on Internet.

The consortium also brings the points of view from **5** different European countries: France, Germany, Italy, Spain and Sweden.

Project participants**:**

CERT-IST ***Project Coordinator***
Computer Emergency Response Team - Industrie Services et Tertiaire.
(FRANCE)
The Cert for France Industry, Services and Tertiary sector. Cert-IST is a not for profit association. Its goal is to provide to its members prevention services and assistance for incident handling. Cert-IST is a center for alert and reaction to computer attacks dedicated to French enterprises.
Cert-IST services are provided by **Alcatel CIT**
http://www.cert-ist.com/

esCERT
Universitat Politécnica de Catalunya (UPC)
(SPAIN)
The esCERT is the Cert managed by the Polytechnic University of Catalonia in Spain. By providing security services to its community, it aims at helping the management of security incident by providing expertise to estimate, prevent and solve security issues in information systems connected to Internet.
http://escert.upc.es/

SIEMENS-CERT
SIEMENS
(GERMANY)
Siemens CERT is the internal Cert of Siemens AG. It provides security services to its constituency; in particular, Siemens CERT operates an advisory service tailored to its constituency's needs.
http://www.siemens.com/

CLUSIT

ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA
(ITALY)
CLUSIT constitutes the Italian counterpart of other European Information Security Associations (Clusix) such as CLUSIB (B), CLUSIF (F), … Clusix have the mission to be the reference regarding Information Security in their country and have the objective to promote and improve awareness, education and information sharing at national and international levels.
http://www.clusit.it/

I.NET

(ITALY)
I.Net is the first Italian Application Infrastructure Provider. Its offering is articulated in two key areas: Managed Internet Connectivity and Web Farm Services, including value added services ranging from messaging, security, monitoring & reporting to management services and data back-up.
http://www.inet.it/

CALLINEB CONSULTING

(SWEDEN)
Callineb is an independent private CERT in Sweden that provides advanced IT security consultancy.
http://www.callineb.se/

INETSECUR

(SPAIN)
InetSecur is a company that provides a comprehensive security solution to its customers by providing security products and various security services.
http://www.inetsecur.com/

2.2. Coordination

The coordination of the consortium was done on a regular base through Progress Coordination Committee meetings (PCC meetings).

From the quality audits that occurred during the project, we can also highlight some points to consider for IST projects:

- As a website is important for the project, whether it is for its public part in order to make dissemination activities or whether it is for its private part in order to ease project communication, the website design, update and maintenance need to be considered as a full project task in the project design phase.
- The risk management is not really developed in the regular reports of IST projects but a risk management, even a very simple one, could bring a better control on project coordination.

3. OBJECTIVES AND METHODOLOGY

The main objective of the European Information Security Promotion Programme is to set-up a European framework aimed at providing European SMEs with the necessary IT Security services in order to give them the necessary trust in e-commerce which is important in developing their businesses. This objective can be achieved through a set of secondary objectives:

1. to set up a network of expertise among the European CERTs which allows them to share and enhance their own prevention material and to "open" it to the other CERTs and organisations involved in prevention;
2. to provide SMEs with adapted, useable and efficient services. Distributing a sole advisory does little to improve the security of any given organisation. A comprehensive accompanying set of services like security vulnerability monitoring plus patch impact on operational platforms, up to remote administration, is often sought, but rarely offered. A model of such a comprehensive set of services has to be set up, and defining a funding model to do business with it must be one the objectives of the project;
3. last but not least, the dissemination of project results to the European SMEs and to the other key players in this area will be sought.

To achieve these objectives, the EISPP project has been split into 6 distinct WPs (WP1, WP2, WP6). WP1 and WP6 are "utilities" WPs: they ensure that the project runs correctly. WP1 is the "Project Management" and WP6 is the "Measurement and evaluation of the project results". The other WPs have been specifically defined to meet the EISPP requirements. These WPs are described below in dedicated chapters.

3.1. WP2: Project Result Dissemination

To be successful, the EISPP project must consolidate and disseminate the lessons learned from the best practice actions that have been done through the project; that is why a separate WP was identified that will include all the Centres of expertise involved in the project, one of them assuming a co-ordinator role for this WP.

A certain number of existing forums/conferences were already identified at national, European and international level, which were used to promote this dissemination; they are:

- IT Security national conferences (Eurosec, …);
- TF-CSIRT Conference (which regroups other European CERTs) organised by TERENA;
- FIRST Conference (which concerns more than one hundred worldwide members).

Each Centre of Expertise has been responsible for addressing those national conferences, whereas the European and world dimension were taken care at a group level. Most of the Centres of expertise are members of FIRST and TF-CSIRT.

On top of that, a dedicated workshop was organised at European level, where SMEs, Chambers of Commerce, as well as European CERTs and service providers (which were likely to be interested in supplying the services which have been tested in the other WPs) were invited to participate.

3.2. WP3: Shared Advisory Infrastructure

To provide European SMEs with the necessary IT Security services they require to run their business, one has to be aware of those vulnerabilities which may endanger SMEs electronic activity if they are not protected against them; that is to collect all the vulnerability related information that are discussed in the various open (or underground) forums, assess them and make that information on the vulnerabilities and means of prevention known to the end users, and those service companies that supply the "computing and networking" facilities to SMEs.

In Europe, a few CERTs had already started this activity but this was done on a "national level" and each of them replicated the same effort (of collecting and assessing), when a lot of savings could be achieved through sharing data and expertise.

The objectives of this WP were then:

- to experiment this sharing by standardising an advisory exchange format;
- to allow each Centre of expertise to "cross access" all the participant vulnerability data bases;
- and to prepare an extension of the number of European CERTs which will be invited to join this "network" (**C**o-operative **E**uropean **I**nformation **S**ecurity **N**etwork of **E**xpertise).

There were four Centres of expertise involved in this WP, based in four different countries (France, Germany, Spain and Sweden), to tackle the language issue which is one of the key components of a security advisory. One of the other key component of a security advisory is the "amount of expertise" that has gone into it: since at least four Centres of expertise have had a chance to assess the same material and agree on its risk level, this has added a lot of credibility for the targeted end users.

All the other Centres of expertise which were part in the project have had access to the various vulnerability data bases which were "opened" as a result of this WP, particularly those which are part of WPs 4 and 5.

3.3. WP4: Advisory distribution to SMEs

EISPP WP4 aims at distributing the advisories produced by WP3 to the SME community. For that, those advisories must be packaged in such a way that they are of use by the recipients. The WP consisted then of experimenting various ways of distributing such information, to take into account the way SMEs are "equipped" to make use of such information:

- directly for those SMEs which are staffed with the technical ad hoc staff to apply the advisory to the information system;
- through Chambers of Commerce and Industry to use a proven dissemination infrastructure;
- through Service Providers (ISPs or ASPs) which already supply basic network services to SMEs.

On top of that, dissemination techniques (mail "push", or web based) were experimented. Trials were set up that experimented different "targets" and different distribution techniques.

The outcomes of this WP are a summary of advantages and disadvantages of distribution targets and techniques, and are also the construction of a funding model to carry such a business, for each of the experimented cases.

3.4. WP5: Deployment and integration of ICT security products

To help SMEs reach and maintain the level of security they need in order to carry their business with the minimum risks when they make use of public networks (Internet), one must ensure that the necessary steps to secure an IT architecture have been and are continuously taken. As for WP4, the same applies, that is, SMEs most of the time cannot dedicate specialised personnel to the maintenance of their IT system, hence the idea to provide a "comprehensive package" to help them, which encompasses the services of WP4 and a deployment and integration of ICT security products.

WP5 uses the results of the previous WP and bundles it into a complete service package for SMEs. EISPP aims to be useful to SMEs and by integrating advisory dissemination (from WP4) with other established security services such as virus management, the resulting service may find a wider audience and may be used more easily. This WP includes trials of the services to end user SMEs

Five pilots have been run, based on different technologies –listed below-, and those pilots were run with the same users as the ones identified in WP4. Furthermore, as the Centre of expertise that was selected to run the pilots had access to the results of WP3, the combination of servi ces should have greatly enhanced the effectiveness of distributing security information.

The technologies that were identified for this WP are:

- Antivirus maintenance and configuration
- IDS operational maintenance
- Continuous Scanning and automated dissemination of advisories
- Firewalls
- System update

4. RESULTS AND ACHIEVEMENTS

This chapter describes the results and achievements realized with respect to the project objectives. Each subchapter below details specific results and achievements related to every WP from WP2 to WP5.

4.1. Project result dissemination (WP2)

The dissemination of EISPP progress and results have been done during the project through different national workshops, that are composed of presentations to groups of users (belonging to SMEs in most cases), presence in exhibitions, and writing for the press.

At a national level, several events have been identified as good opportunities to show EISPP results and try to get the interest of SMEs:

- Internet Global Congress in Barcelona (Spain), where in May 2003 UPC conducted a workshop entitled “Quality guides in managed security services”, that focused on the options SMEs have with respect to outsourcing security services. The services offered through EISPP that target mainly system administrators with little knowledge about security matters were seen by the attendees as a good choice. The event was organised by the Chamber of Commerce of Barcelona, amongst others.
- Eurosec in Paris (France), a forum on information systems and its security, where Cert-IST presented two successive talks at 2002 and 2003 editions. The first one was under the title of “A European CERT network” and consisted of an overview of EISPP with a special focus on its objectives, its issues and perspectives. The EISPP point of contact to join the pilot was provided to all the attendees. In March 2003, an update concerning the project was presented. The presentation was made with some focus on points that had maturated since the previous presentation, as the description of the complement services to be provided to SME. The audience could be split into two parts: SME’s users as potential “direct” customers and potential intermediaries and security services providers that could become partners in a future network.
- Websecurity 2003 in Milano (Italy), organised by Edipi, a publishing house specialised in problems related to technology innovation, and with the collaboration of Clusit. Websecurity is a conference targeting "web oriented" companies, e.g. companies dealing with e-commerce. Clusit did the opening talk “Investing in security starting from the basics”, where the EISPP services were presented as a tool to help this kind of companies with the most common practical security problems.

Other presentations were done (see D2.02 Market survey and results of the national workshops for more details), and also an article in an Italian ICT specialised magazine (ICT Security).

Another way to get SMEs involved was the contact with national Chambers of Commerce. In spite of having happened to be a difficult target to reach (more specifically in Sweden and Spain, although in the latter case some kind of workshop is expected to be held, most probably beyond the EISPP project’s end), the Chambers were present at a couple of workshops performed in Italy and France. The bodies are the Chamber of Commerce of Toulouse and the Chamber of Commerce of Firenze through its special agency Firenze Tecnologia.

Lastly, other CERTs external to the EISPP project have been made aware of its progress in several TF-CSIRT meetings, during the FIRST Technical Colloquium held in February 2003 at Uppsala University (Sweden) and during a BoF session in the FIRST annual conference held in June 2003 at Ottawa (Canada). A special meeting was held previous to 9th TF-CSIRT in Warsaw (Poland), where people from different CERTs attended, and where subjects like common format enhancement, cooperation in writing advisories and the CEISNE network were treated. As a result, CERTs external to EISPP expressed interest in the common format for the security advisories, and once the agreements to join CEISNE have been established, the EISPP Consortium members expect other CERTs to join CEISNE into practice.

In addition to this, a web site was created in October 2002 and has been maintained during the course of the project. Apart from an internal part used for the project co-ordination, a public site has been available with information about the project participants, final users, partial results, public deliverables, and any other information that has been considered as interesting for the general audience.

In section 5.2 a table listing the outputs generated by the EISPP project can be found.

4.2. Shared advisory infrastructure (WP3)

From the early beginning of the project, EISPP strongly believes that a cooperation scheme must be defined at the European level to enable European CERTs to share expertise and knowledge on security advisories. To achieve this task WP3 was layered in successive objectives (as described above in chapter 3.2):

- Standardizing the advisory format
- Cross-access to the participant advisory databases
- Extension of the cooperation model through the CEISNE model

Each objective is reviewed below in a dedicated chapter.

4.2.1. Standardizing the advisory format

A common format for exchanging security advisories has been defined by EISPP, based on compiled best practice information of EISPP CERTs and other available best practice information. This common format is described in the deliverable D3.01.

The EISPP advisory format was adopted by all EISPP CERTs and has been in productive use since March 2003, which shows that the format works not only in theory but also in practice. Apart from the possibilities of co-operation the common format makes possible, the EISPP CERTs also noted improvements in their advisory service due to advantages of the EISPP format over their old, proprietary formats. Problems experienced with the EISPP format and feedback collected from other CERTs have been used to define a new, improved version of the format.

The EISPP advisory format has stirred definite interest within the European CERT community. The CERTs that participated at a workshop regarding EISPP held in conjunction with the 9th TF-CSIRT meeting in Warsaw, as well as other CERTs that expressed an interest into EISPP, were asked for feedback regarding the advisory format. The feedback was collected via questionnaire; nine CERTs from five European countries returned the questionnaire:

- All of them rated the EISPP advisory format either very useful (three votes) or useful (six votes);
- Three CERTs plan to adopt the EISPP advisory format as is, four plan to adopt a somewhat modified or simplified version (e.g., the common format supports advisories in multiple languages, which is not a requirement for every CERT);
- Two CERTs plan to adopt the common format in the short term, two in the long term; for the other CERTs it was too early to tell when changes within their advisory infrastructure can be implemented.

Within the German CERT community, the EISPP advisory format is seen as a viable basis for closer co-operation between the German CERTs: several German CERTs will adopt the EISPP format in the short term. Once the EISPP format has established itself as de-facto standard used by the major players within the German CERT scene, there should be a good chance that the majority of German CERTs follows suit.

Also within Europe, there are excellent chances that EISPP will establish itself as standard advisory format within the next years: during the 11th TF-CSIRT meeting in Madrid (held in January

2004) it was decided that the EISPP format has to been taken as a basis for a new working group (to be established within TF-CSIRT) to create an IETF standard for advisory formats.

Finally, a major vendor has expressed interest into using the EISPP format as basis for an initiative to push for a standard advisory format adhered to also by the most important software and hardware vendors.

4.2.2. Cross-access to the participant advisory databases

As a basis for collaboration on advisories, mechanisms have been designed to make the advisory written by any EISPP CERT available to all other EISPP CERTs. Of course, all the advisories are exchanged using the EISPP advisory format.

An infrastructure to exchange advisories has been defined, at the requirement level, in D3.02. The infrastructure consists of a distributed repository, where each CERT maintains a local advisory database. The advisories circulate between EISPP CERTs primarily using a "push" approach where an automatically generated email is sent to all the EISPP CERTs when an advisory is created or updated. Additionally, a "pull" model that allows an EISPP CERT to retrieve advisories from another CERT "on demand" has been also realized. One of the main reasons for adopting this decentralized model was to avoid the "single point of failure" associated with any centralized site containing all the advisories from all the CERTs.

This infrastructure has been implemented by EISPP, and, as demonstrated in D3.03, started to operate on April 14, 2003. It has been used on a daily basis during the rest of the project life to exchange the advisories released by EISPP CERTs.

The infrastructure did serve the project, and collaboration experimentations could not have occurred without it. However, from the half a year experimentation EISPP had, the limitations of a completely decentralized structure became clear:

- a decentralized infrastructure does not scale up very well: new participants are required to implement a local database for advisories in the EISPP format such that new advisories that are pushed to their site can be processed;
- using the "pull" method for requesting advisory data is rarely useful with the "push" method in place (during the collaboration experiments carried out within the EISPP project, the "pull" method was hardly ever used). Using the "pull" method exclusively, on the other hand, is not practical, as all participants' sites have to be queried one by one;
- successful collaboration requires adequate tool support, e.g., for correlating advisories from several CERTs about a given vulnerability. Such tools must be provided centrally for all participants.

These findings were key elements that helped the project shape the CEISNE model.

Integrity and confidentiality issues with respect to the exchange of security advisories have been only partially addressed by the project.

Currently, all advisories within EISPP are exchanged using S/MIME signed emails. This insures the integrity of data during the transport. An alternative solution should be to protect the advisory data by adding a signature mechanism embedded in the advisory format, thus moving integrity information from the transport layer into the advisory data. Because the EISPP advisory format is XML based, such a solution should be realized using an adequate XML standard. Because the relevant standards are not sufficiently mature, yet, the current version of the format definition does not treat integrity.

4.2.3. Extension of the cooperation model through the CEISNE model

The infrastructure implemented by EISPP (described in the previous section) enabled the EISPP CERTs to start an experimentation phase regarding co-operation on advisories. That experimentation started on April 14, 2003 and was formally closed on November 30, 2003 (we use the term "formally" because EISPP CERT do continue to exchange information through the infrastructure).

During the experimentation phase, several co-operation models where defined and experimented with. The experimentation focused on quality control and quality improvement for advisories, information exchange about vulnerabilities, re-use of advisory data, and co-operation in monitoring new vulnerabilities At the same time, feedback from European CERTs about their ideas and expectations regarding CERT co-operation was also collected.

Based on the experience gained from experimenting with cooperation on security advisories, the EISPP project has designed a blueprint for a Co-operative European Information Security Network of Expertise (CEISNE). This network should become the infrastructure for cooperation between European CERTs in the field of security advisories. CEISNE is not envisioned as an organisation on top of existing CERTs, but rather a set of procedures and services that helps existing CERTs work together.

The experimentation results and the model designed by EISPP for CEISNE are described in D3.04.

4.3. Advisory distribution to SMEs (WP4)

The WP4 aims at distributing the security advisories produced by WP3 to the SME community. To achieve this, WP4 was layered in successive tasks described below:

- definition of SME advisory dissemination services,
- experimentation of the services,
- definition of the funding model.

Each objective is reviewed below in a dedicated chapter.

4.3.1. SME advisory dissemination services definition

WP4 first defined the advisory dissemination services that are required to deliver appropriate security material to the SME. These services are described in the **D4.01**. We give below a short abstract of each service.

1. **Dissemination of security advisories and alerts**

Security advisories contain precise and timely information about the latest vulnerabilities and counter measures. Security advisories are distributed either directly from CERT to SME or via intermediaries (ISP, ASP, CoC, security organisations). When an intensive usage of an important vulnerability occurs, an alert is released. The goal of an alert is to warn quickly SMEs/Intermediaries about a threat. The security advisories and alerts are pushed by e-mail. One major issue is to guarantee SMEs that advisories and alerts have not been modified (advisory integrity) and that the sender is authenticated. In order to fulfil this requirement, the advisory providers digitally sign the information before sending it to SMEs. S/MIME has been used for this purpose, mainly because this mechanism is supported by most of the SMEs' email tools.

2. **Profiled-based dissemination**

At this level of service, the SMEs/Intermediaries only receive the security advisories, by e-mail, about hardware and software they use in their organisation in IT networks and systems. They choose the products they are interested in from a list of products released by the advisory providers. Each CERT manages profiles of SMEs and intermediaries that contain information about the systems used by an SME and the SME's level of expertise. Thus, an advisory service that is tailored to the needs of each SME can be offered.

Another requirement is to provide information in a form that is understandable and noticeable by a wide range of SMEs profiles (with or without IT competence). An effort is made in presenting, selecting and distributing the information to the user: this means at least translating the advisories into local language, but also offering various formats (HTML, TXT or XML) and contents according to the IT skills (like avoiding technical details or language) and frequencies (on the flow, weekly, monthly, …).

3. Access to vulnerability database

A vulnerability database (containing the collection of all the published advisories) has to be made available to the SMEs so that they can access and retrieve security information. This access is done via a web server ("Pull" approach) and secured using digital certificates (HTTPS server with client certificates).

4.3.2. Experimentation and assessment of the services

The experimentation was organised as a trial period. During this period, a set of more than 300 SMEs have got access to the services. This trial has given to EISPP participants a better approach of the SMEs' world where the IT security needs are generally different from the EISPP CERTs members' ones. The trial has enabled EISPP to assess the security level of the SMEs, the quality of the advisories provided, and to communicate in the best way with SMEs.

4.3.2.1. Trial period

All EISPP participants involved in WP4 have tested during more than 6 months the security advisory dissemination services.

EISPP participants have defined their own level of service as a combination of the services described above (see section 4.3.1). For example, light services with only advisories and alerts dissemination with simple profiled-based dissemination and/or full services with advisories and alerts, enhanced profiling, and vulnerability database access.

During the project, they have set up their own infrastructure and did their own advertising of the programme and the trial.

The complete description of each participant services, infrastructure and advertising program is described in the **D4.03**.

Five trials have been set up by Callineb, Cert-IST, UPC, I.NET and CLUSIT. They have involved a large number of SMEs and Intermediaries (See the **D4.02** for the list of SMEs) managed by each participant.

- The SMEs represented a broad sample of communities of SMEs: different sizes (very small, small, medium and large SMEs), various sectors (primary, secondary and tertiary) and businesses.
- The Intermediaries were mainly CoC, ISPs, ASPs, and security consultants. EISPP worked with intermediaries that have small SMEs customers and therefore have good insight regarding SMEs' constraints and their point of view regarding computer security.

The trial period allowed to have a better understanding of SMEs' world, SMEs' IT security needs and assessment of the advisory dissemination service. Furthermore, the trial has resulted in giving the necessary information on how to improve the service in the future. All the trial results are described in the **D4.03** and are summed up in the next section.

4.3.2.2. Results

EISPP has received many feedbacks from SMEs involved in the "advisory dissemination service" trial. Generally, these feedbacks are SME profile dependent. The SMEs' needs regarding the service are different depending on:

- the SME resources and size,
- the IT knowledge available in the SME,
- the internal competency to handle security information like advisories and alerts.

Therefore, the benefits and problems encountered during the trial have been split into two parts depending on the size and the IT knowledge of the SMEs.

Dedicated WP4 questionnaires prior and after the trial have been filled out both by service users and by EISPP participants.

1. Small SMEs with no or little IT knowledge

The advisory dissemination service has been evaluated as "**not useful**" for the very small and small SMEs and most of them do not want to invest in the service. They prefer to have and to pay for security transparent services (like full protection instead of information).The small SMEs have no time and quite often not a lot of knowledge to update their platforms after a vulnerability occurs. For them, IT security and protection of the platforms mean only antivirus software and they mostly rely on it.

Most of the SMEs have not seen the difference between the alerts and the advisories. The advisory content has been considered as very technical and must be more succinct (less technical details on the vulnerability, shortest content of the advisory description,…) and simpler. The "look" of the HTML format is well appreciated and the translation into the local language is mandatory. These SMEs did not show interest in receiving advisories digitally signed and the use of PKI technology is viewed as an annoyance for them.

One way to improve the service is to send to these SMEs only the security advisories on the major vulnerabilities (and especially those where public awareness is very high - e.g. vulnerabilities on Microsoft Windows such as the one exploited by the "Blaster" worm). Additionally, instead of the vulnerability database access (which is too technical), a dedicated public web site will better serve the SME audience.

2. Medium and large SMEs with IT knowledge

For medium and large SMEs, the service has been considered as **useful** and **successful**. These SMEs feel more sensitised about IT security. The service provided is understood, and they feel concerned about the information. The advisories have been appreciated because they are an independent source of information (they do not come from vendors).

The service improved their level of security awareness in their organisation, and provided them with a better understanding of new vulnerabilities.

The EISPP advisory format and content

For the majority of the medium and large SMEs, the information inside the security advisory or alert was easy to understand and applicable to their organisation. Regarding the technical details given, the majority feel that there are enough details and that the advisory is long enough. Most of them have understood the EISPP vulnerability classification and how to assess the risk level.

The HTML format is more appreciated than the other formats. The SMEs which want to re-disseminate the advisories to their structure or to other SMEs (like intermediaries) showed a great interest in the XML format. The local language version is mandatory for SMEs as well as the English translation for those which have entities or offices abroad.

Dissemination

The dissemination "on the flow" or in "real time" is a good frequency and an important factor. All SMEs considered that the advisories were received at the proper time regarding the apparition of the security vulnerabilities.

However, new type of information has to be proposed to SMEs, when they do not have time to handle the security information "on the flow" or "on real time". SMEs communicate that weekly digest (containing the limited list of the classified vulnerabilities released during a week, according to their profile) or monthly newsletter (with security awareness information and the list of critical vulnerabilities) are useful information.

The profiling

For SMEs, an important success factor is to receive only security advisories about hardware and software they use in their IT networks and systems (profile-based dissemination) and not to be flooded by all the vulnerabilities. Most of them thought that the lists of products followed by the EISPP participants were exhaustive.

Improvements have to be made in presenting, selecting and distributing the information to the user. The way the information is presented to an SME is very important: the information content must be adapted to the SME's profile, that is, usable and simple information must be sent to the SME. Despite the EISPP common format does not address this issue (because the possibility of adaptation is limited), the "profiling" could be improved in order to respond to larger SMEs' needs. For example, doing an enhanced filtering, which means sending only the advisories with a particular level of risk of the vulnerability (generally "very high" to "high" risk rating advisories), and focusing on an advisory content only with the relevant information for the SME.

Last, medium and large SMEs indicated that they would be greatly interested in the management of their profile via a user interface (private web site). The CERT's web site aims at providing all the information for the SME registration, profile initialisation and management. For example, filling out an adapted form with the list of products chosen by the user. For a wide range of SMEs behind an intermediary, the profiling service should be delegated to the intermediary.

The digital signature

Digital signatures have been understood by the users. They felt it as a mandatory feature, because it raised their level of confidence regarding the information received. S/MIME has been used for that purpose, because it is recognised by most of SMEs' e-mail clients and is transparent to them.

Vulnerability database through a web interface

The access to the vulnerability database through a web interface is the good way to sensitise SMEs, to attract them and to develop other alternatives to provide the information. For SMEs, it is a value added service. The vulnerability database has been consulted and accessed during the trial in order to get more details of a vulnerability and to check a vulnerability had been updated.

In order to securely access to the vulnerability database through a web interface, digital certificates have been provided to SMEs. SMEs successfully applied PKI. EISPP CERTs use their own PKI but these infrastructures were not set up to provide and manage a large amount of certificates for a lot of SMEs. During the trial, EISPP tried to use the certificates provided by a PKI in an "open" environment (Chambersign) but did not succeed. If a large amount of SMEs is targeted, EISPP is confident of the necessity of a PKI in an open environment. One of the roles of the intermediary is to provide and manage these certificates (like Chambersign certificates in the case of the CoCs).

4.3.3. The funding model

The objective of the funding model was to "develop a service funding model for supplying the service". The project has found that it does not exist one easy solution to fund the service; rather several models that should be used simultaneously in order to make the SMEs finance the service. These general models should work in every country in spite of the differences between national markets. In **D4.04** "SME Security Preventive Information Dissemination service funding models" the models are presented and assessed in terms of feasibility and chance of succeeding.

The conclusion of the funding model is that there is some interest and absolutely a large need for IT-security related advisory services focused on "normal" users, such the ones found in SMEs. Some services that fulfil different parts of these services already exist, but no one is customised towards the SMEs' needs. There should also be a vendor neutral alternative available in the market since most advisory services are not.

Creating a funding model for an advisory service based solely on SMEs as target group with the goal of achieving customer finance is at least difficult and perhaps not possible. This is mainly due to the way SMEs look at IT-security. A small company has a lot of other business risks to take into account, as well as little knowledge or interest in IT-security. The few that have an interest can get some information through various sources.

To be successful, the preferred strategy is to provide a “mix of service offers”:

- A **service free of charge** should be available for the public as an independent source of true information regarding vulnerabilities. It would also be a promotion tool for the paying advisory service. There is of course a trade off between how useful the free service should be in order not to cannibalise on the sales of the paying services.

- A **light service** is a basic advisory service streamlined and adapted to SME’s requirements which makes it possible to manage a large number of users with limited resources. The pricing is low. These services should be marketed through intermediaries such as ISPs, ASPs or security consultants. The requirements for an intermediary are an existing SMEs database, sales force, customer services, and an established subscription business model. The best way to distribute the paying services for SMEs is through this type of intermediary, which already has the infrastructure in place in order to sell and distribute the service.

- A **medium service** is the best service for the EISPP members to sell directly to the SME market. The low cost / high volume alternative is not very attractive for EISSP members because their business profiles tell that they are better suited to a business model serving fewer clients at a higher price. The conclusion is that they should sell a budget version of the **full service**[3] to the few SMEs that already have the motives for investing in an advisory service.

All characteristics of the light, medium and full advisory services are described in D4.04 (section 5.3).

4.4. Deployment and integration of ICT security products (WP5)

This Workpackage is oriented to explore new features that can be distributed along with the vulnerability advisories service as a value added service. It has given us the feedback from certain SMEs that have been collaborating with the different EISPP partners.

First, a section about the services description explains what services have been included in wp5 and which are their goals.

Finally, results and conclusions taken from each pilot experience are presented.

4.4.1. Pilot services description

There are some services really close to server administration and patching in which the advisory service should have special impact, and we have proposed to the SMEs five different kinds of services to make these tasks easier. The services have been proposed as different Pilots, which are:

- **Antivirus Service**: this service provides the SMEs with the possibility of having their antivirus software up to date and well installed, having special updates and information when a new worm is released. A technical help to prevent the users from becoming a victim of a virus is provided, and also the assistance in case a technical action is needed because of an infection. The pilot “virus detection” was divided in three main services :
  - Alert/advisory service: virus/worm/trojan advisory release and dissemination
  - Basic Support service: Technical support
  - Crisis support: Technical support during a crisis situation (like strong worm activity).

[3] **Full service**: highly professional service also suitable for larger companies. This should be offered to the high-end of the SME market

- **IDS Service**: this service provides a complement to some vulnerabilities that can be exploited through an attack in real networks. This pilot gives the information needed by the end users to configure their networks for being able to detect these attacks. Part of the service is the installation of an IDS system remotely updated and managed.
- **Firewall Service**: this pilot is designed to use the advisory information to verify the firewall configuration, and to operate a firewall reconfiguration if required, e.g. a temporary solution before a patch to correct a vulnerability is available. It may also help block the traffic of worm scans during infection peaks, avoid system overload, and detect scans starting from internal compromised systems.
- **System Update Service**: this service updates the systems on behalf of the users. Managed systems include Windows 2000 server, Linux, and OpenBSD. Each time a relevant advisory is received, the need for a reconfiguration or a patch is evaluated. The system can be updated immediately, periodically or on demand. A web service for advisory download was also provided, as part of WP4 activity.
- **Vulnerability Scanning Service**: This service gives the SMEs the real state of the robustness of their systems. Scans are performed periodically to assure the right use of security good practices. First, the systems are studied, and then a good scanning program is designed taking into account the security requirements of the SME.

4.4.2. Results of the pilots

The pilots into which wp5 has been divided are the most interesting services that SMEs can outsource in order to improve their computer security.

Results of the trials are described below.

4.4.2.1. Antivirus pilot

The virus threat is one of the main dangers for SMEs' data. The feedback of the "**virus detection**" pilot showed that all the SMEs need to be protected by an updated antivirus solution. However, according to the SME's size and profile, virus protection already exist with more or less strictness. Big or medium SMEs run antivirus in their networks and regularly update them (automatically or through manual action). On the other side, the small and very small SMEs may have antivirus which are updated or not (due to a lack of IT knowledge or/and a lack of financial means).

The trial has resulted in giving the necessary information on how to improve the service in the future. All the trial results are described in **D5.03**.

This pilot showed interesting results about the SMEs' needs regarding the virus activity. All the SMEs have not the same needs, but each of them communicated that they are interested in an antivirus service.

- For medium and large SMEs, the "Virus advisory dissemination" service has been considered as *useful and successful*. This service enables them to check their antivirus updates with information provided by a neutral source (CERT). However, this type of service requires, at the SME level, internal communication and procedures in order to be used in an efficient way. Otherwise, the information may be lost or not processed by the SME.
- The "Basic support" (see 4.4.1) service has been evaluated as *moderately useful*. It interested principally the medium SME.
- However, the "Crisis support" (see 4.4.1) service has been considered *very useful* by a majority of SMEs, because it helps them have more information during a massive worm spreading (e.g. "Blaster"). A dedicated channel (mailing lst) to group the information is mandatory to perform this support.
- Small SMEs, which generally have no IT knowledge, have communicated that they prefer a transparent service like remote antivirus administration embedded into

other ISP/ASP services (like Internet connection service, …), instead of an information and support service.

Furthermore, the service presentation is also a key element which contributes to the success of the service at the SME level. It must convince SMEs of the usefulness of such a service and help them include it in their activity in an efficient way.

In order to adapt the "Virus detection" service to all SMEs' needs, and more particularly to Medium and Small SMEs, EISPP further experimented a remote antivirus administration solution like antivirus appliance (NAI webshield). The results of the experiment showed that this solution:

- is not mature enough to manage a group of SMEs antivirus appliances from a remote central point (Intermediary for example);
- must not be used as a stand alone solution (it requires to be coupled with a firewall);
- can become very expensive for a SME's budget (3 K€ to 15 K€).

Following the above assessments, EISPP studied another solution based on antivirus clients directly installed on PC/Servers and managed from a remote central point. An EISPP partner (French ASP) has been involved and provided this kind of solution to its SME customers (with the F-Secure products). This solution is already used and very successful for Small SMEs (low budget like 3 € /host/month). However, for such a service, if an infection occurs, the responsibility of each party must be strongly defined in the service agreement.

A service dedicated to the virus protection is useful for SMEs. In order to be successful, it must be divided in **sub-services** to cover all the SMEs' needs and budgets, and it cannot be only provided by a CSIRT but must involve **Intermediaries** (ASP/ISP) to address a large group of SMEs (several hundreds).

Sub-services and actors involvement (workload):

- Alert/advisory service: security information sent to SME
  - ⇒ Actor Involvement:
    - CSIRT: + + +
    - Intermediary: +
- Support service: technical support via phone, e-mail, FAQ; technical support during a crisis situation via phone, e-mail and a dedicated communication channel (mailing list)
  - ⇒ Actor Involvement:
    - CSIRT: + +
    - Intermediary: + +
- Transparent service: remote SME's antivirus administration with a low cost and packaged with other ISP/ASP solutions
  - ⇒ Actor Involvement:
    - CSIRT: +
    - Intermediary: + + +

4.4.2.2. IDS pilot

IDS (Intrusion Detection System) service is a useful security service only if the device is well *configured and managed* –an IDS, in this pilot, is considered as a hardware (PC) with a Linux operating system and a network sensor gathering traffic–. The tunning process of each IDS and the creation of some scripts have led us to minimize the management process. The other part of the service is the alert generation, which consists of generating rules to update the IDS knowledge base, and keep the SMEs informed; *alert generation* is critical because a right alert guarantees good IDS response to attacks.

Tipically the SMEs have not enough resources to interpret the results and to identify the bad traffic –called alarms– properly, so they prefer to outsource, only if the service has a good price and conditions. It is not easy to deploy an IDS System, to monitor a network 24 hours a day, and to report all the 'rare' events that happen, because of their heterogeneousness.

A high quality and competitive service has been provided, and end users are really happy with the results. They have learnt about IDS technology and they have improved the knowledge of their networks. IDS technology has turned to be a new and interesting technology for users, since it lets them see the whole picture of their network traffic. Nevertheless, IDS management is a very time consuming and specialized service, so most of the SMEs would not use this kind of technology without outsourcing it. Users have appreciated not only to be released from maintaining an IDS, but from looking at the possible false-positives alarms. A false-positive is an alarm that does not match with a real attack; it is usual to have hundreds in an IDS, and the expertise of the CERT team has given a more accurate vision about the attacks detected in the IDSs.

SMEs are very interested in having someone managing their IDSs, but it is necessary to keep them informed about what the IDS is exactly doing, so that they can get involved in the process somehow and learn how it works. **Alert advisories** have done this task by letting them know what signatures are included into the IDS at any time, and review them if necessary.

4.4.2.3. System Update pilot

SMEs are very interested in this service. Day-to-day system management requires updated information of system vulnerabilities, along with a risk rating and possible solutions. Advisories provide this kind of information; however, there are other sources of information.

This service is very time-consuming and does not scale well. No two systems are identical in practice when they are set up by different companies, so automatic patching and reconfiguration is seldom possible; the impact of patches must be evaluated with respect to the applications and configurations, so even a highly specialized ISP/ASP as I.Net basically deals with the systems one-by-one, as blocking the services because of an automated update is not a valid option.

The service has a great value for SMEs with standard services of medium complexity; SMEs with complex services already have the personnel to deal with them, so a service just for system maintenance has little value, while outsourcing the whole management is not practical. SMEs with basic services can better base their activities on hosting services, where system maintenance is already part of the service.

A SME needs to evaluate the risk of outsourcing the system management before accepting the service. After that, the SME is usually not interested in details on the day-to-day system management activity. In particular, SMEs are scarcely interested in activities that do not require direct actions by them, or in advisories on problems that are already handled by the Intermediary. A consequence is that this service is an alternative to the advisory service, and not a value-added.

SMEs want to avoid any service disruption. In some cases, e.g. when it is not clear if a patch may have any consequence on the services and the vulnerability is not rated at a high-risk level, patching is avoided.

During the workshop some participant confirmed that the use of an official source of advisory information can be a plus when selecting an outsourcer; however, if there is a service disruption, then it is the intermediary problem not to be compliant with its contract with the SME. So, despite the fact that offering an “official” advisory service can be useful when presenting a service to a potential customer, it is less useful in case an actual problem arises.

4.4.2.4. Firewall management pilot

This service, in the same way that system update, is very time-consuming and does not scale very well. As every two systems are different in practice when they are set up by different companies, automatic reconfiguration is seldom possible; the impact of reconfigurations must be evaluated with respect to the services and activities of the SME and the network configuration, e.g. connections with the Internet and service positioning at the DMZ. Day-to-day firewall management is based on two tasks: reconfiguration to take into account new needs on traffic (e.g. a new service is offered to the Internet users), and logs monitoring to detect unusual or dangerous traffic that is blocked by the firewall. This second task is difficult since firewalls usually block unauthorised connections from the first packet, and in can be hard to understand what the connection attempted to achieve, or if it was an attack at all. Advisories help in the analysis of the log by giving information of new attacks or current traffic trends, e.g. new worms. Without fresh information of these topics, firewall logs can be almost useless.

Many sources of information should be monitored to collect all the relevant parts of them. Moreover, trustworthiness of these sources needs to be evaluated, especially if decisions are to be taken based on this information. A single source of information can be very useful if it is trustworthy: having the relevant information pushed by an organisation dealing with collection and selection greatly reduces the effort required.

As for other services, after the SME has evaluated the risk of outsourcing the firewall management, it is usually not interested in details on the day-to-day firewall management activity. In particular, users are not very interested in activities that do not require their direct participation, or in advisories of problems that are already handled by the firewall configuration.

Users want to avoid any service disruption, even during emergencies, and tend to avoid actual reconfiguration of the firewall. However, most of the problems related to vulnerabilities exploitable through the firewall are either on ports that should be already blocked by a properly configured stateful firewall, or on public services (e.g. web or mail) where most firewalls cannot do much to prevent the attack. As a consequence, a properly configured firewall needs some action mostly to prevent outgoing attacks from internal compromised systems, since traffic from internal networks to the Internet is often less restricted by the user's security policy.

4.4.2.5. Vulnerability Scanning pilot

The main experience from the trial was that the success of the service depends very much on how the information is presented to the customer. By presenting the information in an easy-to-understand way, with step-by-step instructions on how to correct the vulnerabilities, the service can be very useful, even for customers with no or little experience in information security. The backside is that it takes more time, thus making the service more expensive and perhaps out of reach for some companies. By using a pre-defined report template some of the work can be streamlined and perhaps a system with a knowledge-base can reduce the cost for each report even further. Many of the vulnerabilities that are discovered exist in many systems and many clients, and once one report is written, the information can be shared between documents.

It is also important to understand that the large volume of information generated by a vulnerability scanning tool can be overwhelming for a novice customer. It also increases the risk of misinterpreting the results. False-positives are also common in the results, but by having experienced staff these can be sorted out and removed from the report.

If the report is not clear and easy to understand, the customer must put in it more time and effort to make good use of it, thus making the service more of a burden than a help.

The value of the service is directly proportional against the number of systems in a network. A small network with only one or two systems can be maintained without the help of an expensive vulnerability scanning service, but a network with ten or more systems greatly benefits from a vulnerability scanning service, since it is faster than performing a manual check of each system. This is even more true once the baseline is established and combined with an advisory service of high quality (such as the services in WP4).

The customers with smaller networks may also benefit from a vulnerability scanning service once the more labor intensive work of establishing a baseline is done. The effort to correct deviances from the baseline found in the compliance scans are usually small and can often be implemented by following a step-by-step guide.

4.4.2.6. Overall conclusion

Grouping all the services described above, a security pack can be made to guarantee the SMEs that their security issues are properly treated. All the services are required to have an acceptably secure network. All the pilots have been oriented to improve the vulnerability advisories service, and all of them have been considered as value added services by SMEs. Each pilot has improved in one or more ways the viability of the vulnerabilities advisories service.

In general, all the pilots have contributed to make the security management of the SMEs' systems easier, and have helped the different organisations with their security. Insecurity is a fact inherent to being connected to an open network, and having a professional team helping in it is more useful than SMEs in general expected. It is cheaper for small enterprises to outsource that kind of services than having specialized people.

SMEs have been really interested in WP5 services and they have been in fact more secure while taking part of one of the pilots. It is hard to reflect the impact of security services in financial results. SMEs have not become aware yet in security services payment; actually only those who have been victims of security threats are ready to pay for these services. SMEs' primary necessities are the final arbiter of any investment decision. It is easier to promote this kind of services as value added services to the advisory service and, at least, as a complement to ISP services.

In general, the security service demand depends on the SME motivation, profile, needs and budget. All the services are not required by all types of SMEs (e.g. big SMEs already have security services and they would only want one or two additional services).

For example, good added-value services may be one or several packaged sub-services:

- antivirus, firewall, system updates, for basic SMEs (with no IT knowledge);
- vulnerability scanning, IDS, for SMEs with IT knowledge;
- or on-demand sub-services among WP5 services for any SME.

In conclusion, the provided added-value services must be flexible to adapt to all the SMEs' determinants.

5. DELIVERABLES AND OTHER OUTPUTS

This section describes all the documents thought as an output of the project (then to be delivered to the EC), and other outputs that EISPP has generated.

5.1. Deliverables

All the deliverables met during the EISPP project are listed below, along with the dates they were sent to the EC:

Deliverable	Title	Delivery date	Nature (i)	Dissemination level (ii)
D1.01	Project Quality Plan	2002/08/02	R	CO
D1.02	Project Inspection Audit Report (1)	2002/10/31	R	CO
D1.03	Mid Term Report	2003/04/16	R	CO
D1.04	Project Inspection Audit Report (2)	2003/12/17	R	CO
D1.05	Project Final Assessment Report	2004/02	R	CO
D2.01	CERT workshop conclusions	2003/07/31	R	PU
D2.02	Market survey and results of the national workshops	2003/07/21	R	PP
D2.03	SME and Chamber of Commerce workshop	2003/11/04	O	
D3.01	Advisory format description (document)	2002/10/23	R	PU
D3.02	Requirements for CERT common vulnerability repository (document)	2002/10/23	R	CO
D3.03	Cross access demonstrator to participant vulnerability databases	2003/05/20	D	PP
D3.04	Agreement to join CEISNE	2003/12/22	R	PU
D4.01	SME service description(s) document	2003/02/20	R	PU
D4.02	Advisory distribution to users	2003/05/20	O	RE
D4.03	Trial period result document	2003/11/18	R	PU
D4.04	SME Security Preventive Information Dissemination service funding model(s)	2003/12/11	R	PP-PU
D5.01	General methodology report for pilot running.	2003/04/10	R	PP
D5.02	ICT deployment and running of products (4 pilots to be conducted)	2003/05/20	O	
D5.03	4 individual reports describing the benefits experienced by pilot users and the recommended best practices	2003/12/17	R	PU
D5.04	Overall report giving an overview of the issues encountered during the work	2004/01/30	R	PP-PU

D6.01	Evaluation methodology and criteria document	2002/12/03	R	PP
D6.02	Project Report	2004/01/30	R	PP

(i) R = Report
P = Prototype
D = Demonstrator
O = Other

(ii) PU = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)

Below there is a short description of each deliverable listed.

5.1.1. WP1 deliverables

D1.01 Project Quality Plan

Deliverable	Deliverable name	Version	Date	Delivered to EC
D1.01	EISPP-D1-001-MP-1-0-PP.doc	1.0	2002/08/02	**X**
D1.01	EISPP-D1-001-MP-1-1-PP.doc	1.1	2002/11/28	**X**

This document lays down the principles to manage and control the project quality.

It provides management rules and procedures that must be applied by all participants. It gives the rules of document management as the document nomenclature and the documents validation processes. It also presents the roles and responsibilities of project participants and explains the meeting and reporting rules.

D1.02 Project Inspection Audit Report (1)

Deliverable	Deliverable name	Version	Date	Delivered to EC
D1.02	EISPP-D1-002-AR (ISO 9001 Audit Report 1).doc	1.0	2002/10/24	**X**

Two quality audits were done during the project in order to assess the overall quality of the work and the respect of the project quality plan.

The first audit was conducted by the Quality team of one project participant. The D1.02 document provides the results coming from this first audit that took place in October 2002. It shows different items to be looked after and the project had put an action plan in order to take the highlighted points into consideration.

The audit results pertinence was ambivalent because the auditor only worked without making any request to the project coordinator and, so, experimented difficulties to access the appropriate versions of documents.

Anyway, we can highlight the following key points that needed to be looked after:

- the Consortium agreement finalization
- the production of reports (PAPR, WPR, MR) in due period, starting by filling up the unitary reports (PAPR) so as to improve elaboration duration and report content exhaustiveness

Afterwards, we can make the following analysis on these points:

- The Consortium Agreement took globally some time to be agreed among partners but it converged simultaneously with the birth of the new consortium coming from the restructuring of early 2003 (see section 0 Coordination)
- The production of reports in the project was an active effort that was regularly reminded in the project coordination actions. Some good progress was done on this point in the course of the project as project participants became more familiar with the reporting processes

D1.03 Mid Term Report

Deliverable	Deliverable name	Version	Date	Delivered to EC
D1.03	EISPP-D1-003 Mid Term Report Jun02-Feb03.doc	1.0	2003/03/08	**X**

This report, covering the period from June 2002 to February 2003, makes a global status on the project progress since the beginning. In this period, the main point was a big change in the consortium constitution, with the withdrawal of one participant and the introduction of two new participants. A new project plan was elaborated to take these changes into consideration.

D1.04 Project Inspection Audit Report (2)

Deliverable	Deliverable name	Version	Date	Delivered to EC
D1.04	EISPP-D1-004-AR(Audit Report 2) Ed01.doc	1.0	2003/10/29	**X**

Two quality audits were done during the project in order to assess the overall quality of the work and the respect of the project quality plan.

The second audit was conducted by the Quality team of the Project Coordinator. The D1.04 document provides the results coming from this second audit that took place in October 2003. It points out some improvements to carry out. As the audit was rather near the end of project, it makes a distinction between immediate actions that need to be done and some learning points that should help improve the running of any other IST project.

The key findings are related to:

- Risks Management
- Progress visibility
- EISPP internal web site use

As for the first audit, the project elaborated an action plan in order to take the highlighted points into consideration during the project progress. The Progress Coordination Committee treated immediate actions in first priority but also took into consideration in its action plan some very interesting learning points as, for example, about the improvement of private web site's clarity.

D1.05 Project Final Assessment Report

Deliverable	Deliverable name	Version	Date	Delivered to EC
D1.05	EISPP-D1-005-PR-1-0 (Final Assessment).doc	1.0	2004/02	**X**

This report, covering the period from June 2002 to January 2004, makes a global assessment of the project progress since the beginning; it is the final management report of the project.

5.1.2. WP2 deliverables

D2.01 CERT workshop conclusions

Deliverable	Deliverable name	Version	Date	Delivered to EC
D2.01	EISPP-D2-001-TR-1-0-PU.doc	1.0	2003/07/29	**X**

This document was generated after holding a workshop with other CERTs external to EISPP. The feedback got from these other CERTs was considered very important for us, because one of the goals of EISPP is to set up a network of expertise between European CERTs about vulnerability information.

The main conclusions extracted from that meeting were:

- There is in fact a large demand for more exchanges on security advisories between entities such as CERTs;
- The larger the number of participants in such a network of expertise is, the higher the demand for a more efficient collaboration will be, so it is worth by the EISPP members defining and experimenting these collaboration processes;
- The common format is very useful (and some suggestions to improve it were given); anyway, the core is what goes inside it, this is, all the information related to a certain vulnerability.

D2.02 Market survey and results of the national workshops

Deliverable	Deliverable name	Version	Date	Delivered

				to EC
D2.02	EISPP-D2-002-TR-1-0-PP.doc	1.0	2003/07/10	**X**
D2.02	EISPP-D2-002-TR-2-0-PP.doc	2.0	2003/12/15	**X**

A first version of this deliverable was released at the end of July 2003. The document analyses the market structure regarding Vulnerability Assessment and Intrusion Detection to try to find the best position for the EISPP members, who must focus on the strength and opportunity of CEISNE, to basically make cheaper advisories with a high level of quality, and may intensify cooperation with service multipliers or intermediaries, both to help finance the service and to raise security awareness within SMEs.

Several national workshops were held intended to reach the maximum number of SMEs and keep them aware of the EISPP content, achievements, and the way to participate in it. The workshops were performed in Italy, France and Spain, mainly through presentations, exhibitions and some article.

This document was updated by the middle of December 2003 with the results and conclusions taken from workshops held in France and Italy with Chambers of Commerce, and the contact progress with this kind of bodies in Spain and Sweden. The main conclusions, applicable to the countries were the workshops were performed but that may be able to be extrapolated to other countries, are:

- SMEs have a lack of security awareness;
- SMEs with no IT staff are not as interested in receiving security advisories as in being offered more transparent security services;
- General users find security advisories very useful and think that they raise security awareness;
- They also appreciate that the advisories come from a trusted source (a CERT part of the CEISNE can be).

D2.03 SME and CoC workshop

Deliverable	Deliverable name	Version	Date	Delivered to EC
D2.03	EISPP-D2-003-O-1-0-PP.doc	1.0	2003/10/31	**X**

This is a milestone document that only contains the data of the workshops to be held with Chambers of Commerce; it was delivered before the realisation of these workshops.

5.1.3. WP3 deliverables

D3.01 Advisory format description (document)

Deliverable	Deliverable name	Version	Date	Delivered to EC
D3.01	EISPP-D3-001-TR-1-0-PU.doc	1.0	2002/10/21	**X**
D3.01	EISPP-D3-001-TR-1-1-PU.doc	1.1	2003/02/05	**X**

D3.01	EISPP-D3-001-TR-1-2-PU.doc	1.2	2003/03/28	**X**

This document describes the common format defined by EISPP for security advisories. The format is the technological basis for exchanges of and co-operation on security advisories.

The document gives a description of required and optional fields within an advisory and defines a formal XML-based grammar for the document format. A comprehensive informal presentation of the advisory format supplies advisory authors with the necessary guidelines for authoring security advisories in the EISPP format. In particular, it defines an assessment methodology to rate the risk level for a given vulnerability.

The EISPP advisory format supports the authoring of an advisory in several languages (local languages plus English), a feature that is essential for co-operation in a European context and also for tailoring the advisories to the SMEs.

D3.02 Requirements for CERT common vulnerability repository (document)

Deliverable	Deliverable name	Version	Date	Delivered to EC
D3.02	EISPP-D3-002-TR-1-0-CO.doc	1.0	2002/10/23	**X**
D3.02	EISPP-D3-002-TR-1-1-CO.doc	1.1	2003/03/18	**X**

This document describes the infrastructure created by EISPP as the basis for cooperation on security advisories within the EISPP project.

The infrastructure is designed as a distributed repository: each EISPP CERT keeps a local advisories database and distributes these advisories to the others CERTs using either the "pull" or "push" approach. The global infrastructure creates a common vulnerability repository which stores all the knowledge collected by the EISPP participants about vulnerabilities.

The document presents the overall model and defines the requirements that have to be fulfilled by EISPP participating CERTs: functionalities to implement, security constraints, technologies and standards to conform with.

D3.03 Cross access demonstrator to participant vulnerability databases

Deliverable	Deliverable name	Version	Date	Delivered to EC
D3.03	EISPP-D3-003-TR-1-0-PP.doc	1.0	2003/04/22	**X**

This document describes the infrastructure that has been set up by each EISPP participant to implement the common vulnerability repository (D3.02). The first aim of this deliverable is to show that the "cross-access demonstrator" project milestone has been reached and that this infrastructure is now running.

D3.04 Agreement to join CEISNE

Deliverable	Deliverable name	Version	Date	Delivered

				to EC
D3.04	EISPP-D3-004-TR-1-0-PU.doc	1.0	2003/12/17	**X**

This deliverable presents the road map defined by EISPP for establishing CEISNE within the European CERT community.

The roadmap was shaped on the results of the half a year experimentation phase and a large part of the document is dedicated to describe these results regarding both the supporting infrastructure and possible models for CERT co-operation. A brief introduction modelling the advisory creation process is also provided.

The document contains the project's recommendations regarding the establishment of CEISNE. Future actions of the EISPP members after the end of the EISPP project to work towards the establishment of CEISNE within the European CERT community will be based on this document.

5.1.4. WP4 deliverables

D4.01 SME service description(s) document

Deliverable	Deliverable name	Version	Date	Delivered to EC
D4.01	EISPP-D4-001-MI-1-0-PU.doc	1.0	2003/02/14	**X**
D4.01	EISPP-D4-001-MI-2-0-PU.doc	2.0	2003/05/08	**X**

This document's objective is to describe the security services provided by EISPP to SMEs. The description of the services covers their key elements, the basic technologies that are used, formats and protocols, PKI-technologies used, and requirements for SMEs to use the service.

Because D4.01 is the only project document which describes all the security services to SMEs, it covers either WP4 services (advisory services) and WP5 services (value-added services).

Advisory services: The basic service provided by EISPP is an advisory service, i.e., the distribution of security advisories that contain precise and timely information about the latest vulnerabilities and counter measures. Security advisories are distributed either directly from CERT to SME or via intermediaries (ISP, ASP, CoC, security organisations). SMEs will only receive security advisories about hardware and software they use in their organisation in IT networks and systems (profile-based dissemination). Furthermore, SMEs can access a collection of published advisories via a web server.

Value-added services: EISPP further experiments with value-added services to the advisory service with the aim of helping SMEs make full use of the information contained within the advisories. At the moment, value-added services include the following technologies: IDS (pattern and system update), Virus detection, Vulnerability Scanning, Firewalling Technology, and Remote System Update (security patches).

D4.02 Advisory distribution to users

Deliverable	Deliverable name	Version	Date	Delivered to EC
D4.02	EISPP-D4-002-MI-1-0-RE.doc	1.0	2003/05/12	**X**

D4.02	EISPP-D4-002-MI-2-1-RE.doc	2.1	2003/12/11	**X**

This document provides the starting date of the security advisory distribution to end users (SMEs and intermediaries).

It contains a table with the EISPP participant which contacts the SME or the intermediary, the name of the SMEs and intermediaries involved in the trial period, and the dates of the user agreement signature between the EISPP participants and their end users.

D4.03 Trial period result document

Deliverable	**Deliverable name**	**Version**	**Date**	**Delivered to EC**
D4.03	EISPP-D4-003-TR-1-0-PU.doc + annexes : D4.03_set_of_trial_reports_v1-0.zip and questionnaires_Q4a_and _Q4b.zip	1.0	2003/11/03	**X**
D4.03	EISPP-D4-003-TR-2-0-PU.doc + annexes : D4.03_set_of_trial_reports_v2-0.zip and questionnaires_Q4a_and _Q4b.zip	2.0	2003/12/24	**X**

The document provides the results and assessment of the 6 months trial period which took place during the EISPP project. The WP4 trial period allowed the EISPP project to test all the SME Security Preventive hformation Dissemination Services (described in the D4.01) with the SMEs and intermediaries involved in the trial (described in D4.02).

A summary of Trial report conclusions is described in the section 4.3.2 of the present document.

D4.04 SME Security Preventive Information Dissemination service funding model(s)

Deliverable	**Deliverable name**	**Version**	**Date**	**Delivered to EC**
D4.04	EISPP-D4-004-TR-1-1-PU.doc	1.1	2003/12/01	**X**

There are several ways of financing an advisory dissemination service. This document tries to analyse and evaluate them, according to the possibilities that the IT market offers and the nature of the EISPP Consortium members.

The Market Survey and results of National Workshops (D2.01) gives an overview over models that are being run by competitors regarding to similar services.

Different models are proposed here, with a description, an evaluation of pros and cons, and an *a priori* categorisation into losing, dependent, and winning models.

Also the final users of the service have given feedback through the questionnaires designed within the project, that helped improve the evaluation and increase the feasibility of such business models. Basically, most SMEs do not feel like paying a budget in exchange of an advisory service. As discussed inside the document, the business model with an intermediary which can redistribute the advisories and include the cost into some package of services happens to be the more feasible one.

A summary of Funding model conclusions is described in the section 4.3.3 of the present document.

5.1.5. WP5 deliverables

Most of the documentation generated during the trial period have been used as internal documentation to coordinate the whole pilots and conclude what is explained in D5.04.

D5.01 General methodology report for pilot running

Deliverable	Deliverable name	Version	Date	Delivered to EC
D5.01	EISPP-D5-001-1-TR-1-0-PP (CLUSIT pilot description).doc	1.0	2003/04/08	**X**
D5.01	EISPP-D5-001-2-TR-1-0-PP (I.Net pilot description).doc	1.0	2003/04/22	**X**
D5.01	EISPP-D5-001-3-TR-1-0-PP (InetSecur pilot description).doc	1.0	2003/03/31	**X**
D5.01	EISPP-D5-001-4-TR-1-0-PP (Cert-IST pilot description).doc	1.0	2003/03/04	**X**
D5.01	EISPP-D5-001-5-TR-1-0-PP (Callineb pilot description).doc	1.0	2003/02/28	**X**

These reports describe the work that was planned to be done, the objectives of each pilot and dates related to WP5. The SMEs that were going to collaborate are also described. This was an initial deliverable for internal organisational purposes. All this information is reflected in D5.03.

D5.02 ICT deployment and running of products (4 pilots to be conducted)

Deliverable	Deliverable name	Version	Date	Delivered to EC
D5.02	EISPP-D5-002-MI-1-0-RE1.doc	1.0	2003/05/12	**X**

This document explains the deployment of each pilot and partial results of WP5. Each pilot has developed a document explaining the deployment and the agreement signing process with the SMEs. This deliverable was also for internal organisation. All this information is reflected and developed with conclusions in D5.03.

D5.03 4 individual reports describing the benefits experienced by pilot users and the recommended best practices and 1 summary report that gives a general view

Deliverable	Deliverable name	Version	Date	Delivered to EC
D5.03	EISPP-D5-003-0-TR-1-0-PP (Pilots Summary).doc	1.0	2004/01/12	**X**
D5.03	EISPP-D5-003-1-TR-1-1-PP (Antivirus pilot).doc	1.1	2003/10/31	**X**
D5.03	EISPP-D5-003-2-TR-1-1-PP (Firewall pilot).doc	1.1	2003/10/31	**X**
D5.03	EISPP-D5-003-3-TR-1-1-PP (IDS pilot).doc	1.1	2003/12/28	**X**
D5.03	EISPP-D5-003-4-TR-1-1-PP (System update pilot).doc	1.1	2003/12/03	**X**
D5.03	EISPP-D5-003-5-TR-PP (vuln scan pilot version).doc	2.0	2003/12/30	**X**
D5.03	EISPP-D5-003-0-TR-2-1-PP (Pilots Summary).doc	2.1	2004/01/12	**X**

The document provides the results and assessment of the trial period which took place during EISPP project regarding the value added security services. Each pilot has given a part of security related work to integrate, with all of them, a comprehensive security plan useful for any SME that would like to outsource its security issues.

D5.04 Overall report giving an overview of the issues encountered during the work

Deliverable	Deliverable name	Version	Date	Delivered to EC
D5.04	EISPP-D5-004-TR-1-0-PP.doc	1.0	2004/01/28	**X**

This report explains the conclusions of all WP5, taking into account that SMEs dealt with some workload during the pilot experiences and most of them had no extra resources to assist the extra-work they had with each pilot. These problems and daily operation are the main subject of this document. The results have been extraordinary because users have been informed of the matters of their networks and the emerging threats on the fly.

5.1.6. WP6 deliverables

D6.01 Evaluation methodology

Deliverable	Deliverable name	Version	Date	Delivered to EC
D6.01	EISPP-D6-001-TR-1-0-CO.doc	1.0	2002/11/27	**X**
D6.01	EISPP-D6-001-TR-1-2-CO.doc	1.2	2003/04/10	**X**

This document describes the criteria that will be used to overall evaluate the EISPP project; the evaluation will be done in D6.02 Project report.

A set of questionnaires were designed for each WP, to assess how they performed. In this document we can find the points that are the basis of these questionnaires, a set of evaluation and success criteria for each WP from wp1 to wp5, excluding wp6 that is the evaluation part of the project itself. This criteria helps us evaluate what has been successful in a WP, and what may have not.

D6.02 Project report

Deliverable	Deliverable name	Version	Date	Delivered to EC
D6.02	EISPP-D6-002-TR-1-0-PP.doc	1.0	2004/01/28	**X**

This is the present document.

In order to receive an objective view on the project, a pre-release of the this project report has been reviewed by an external expert, David Crochemore (CERTA, France), a FIRST Steering Committee Member. The feedback provided by David Crochemore on the project's achievements and their presentation in general was very good. Comments on the presentation such as the request to provide more information on certain aspects of the project have been integrated into the final version.

5.2. Other outputs

The following table shows the outputs generated by the EISPP members apart from the deliverable documents, which are mainly presentations and workshops. The date, the type of audience, and a brief description are included.

Date	*Description*	*Organiser*	*Audience*	*Dissemination level*
March 2002	Presentation at Eurosec 2002 overviewing EISPP, its objectives and perspectives, and inviting attendees to join the pilot	Cert-IST	Potential intermediaries (ISPs, telcos, administrations), SMEs	France
May 2002	Presentation at 6th TF-CSIRT meeting describing the background of the project, its objectives, structure, target groups and expected results	All	CERTs	Europe
July 2002	Presentation of the project to get users to be involved in wp4 and wp5	Cert-IST	SMEs	France
September 2002	Brief update at 7th TF-CSIRT meeting regarding the start of the project, and the web site that would be available the following month	All	CERTs	Europe
October 2002 and later	A public website was created and has been maintained, with EISPP related information, progress, and some results in form of public deliverables	UPC	Open	Worldwide

Date	*Description*	*Organiser*	*Audience*	*Dissemination level*
October 2002	Panel at SMAU 2002, an exhibition on IT and related technologies, describing the project and related services, focusing on SMEs benefits	Clusit	Open (most employed by SMEs)	Italy
December 2002	Presentation to structural units at UPC of preventive security measures, and description of EISPP as a part of them	UPC	System administrators	Spain
January 2003	Update of the project at 8th TF-CSIRT meeting, describing wp3 in detail, and making the participants aware of the first deliverable of the project (common advisory format). The workshop to be held with CERTs in May was advertised	All	CERTs	Europe
February 2003	Presentation to technical staff about securing an open network as Internet, and the usefulness of an advisory service. The attendees were invited to join the pilot	InetSecur	People mostly working for SMEs	Spain
February 2003	Panel at Infosecurity Italia 2003, describing the project and related services, focusing on SMEs benefits	Clusit	IT-security related	Italy
February 2003	Presentation at a FIRST Technical Colloquium to CERTs about the key elements of EISPP, with special dedication to wp3 -CERT cooperation	All	CERTs	Worldwide
February 2003	Twp pages article in ICT Security (specialised magazine) describing the project structure and goals, focusing on SMEs benefits	Clusit	Subscribers (IT-security related people)	Italy
March 2003	Update on EISPP at Eurosec 2003, describing complement services for the SMEs, public common format available, real exchange of advisories, and inviting attendees to join the pilot	Cert-IST	Potential intermediaries (ISPs, telcos, administrations), SMEs	France
April 2003	Presentation at a German CERT meeting about the common advisory format	Siemens	CERTs	Germany
May 2003	Article for the FIRST TIMES newsletter, with references to the common format and to the EISPP website, and promoting the EISPP workshop held one day before 9th TF-CSIRT meeting in Warsaw	All	CERTs	Worldwide
May 2003	Presentation at Internet Global Congress 2003 focusing on the outsourcing option for the SMEs to manage their security, and the capacity of EISPP to raise security awareness (seen as necessary by the attending SMEs representatives)	UPC	SMEs, Chamber of Commerce	Spain
May 2003	Workshop with European CERTs held one day before the 9th TF-CSIRT meeting, where important findings were done regarding the common	All	CERTs	Europe

Date	*Description*	*Organiser*	*Audience*	*Dissemination level*
	advisory format, the collaboration on advisories, and the CEISNE network of expertise			
May 2003	Update of the project at 9th TF-CSIRT meeting, talking about the common advisory format, the experiments with cooperation models, and the feedback and requirements expressed by other parties such as SMEs and CSIRTs. A first overview of the workshop with CERTs held just before the meeting was also given	All	CERTs	Europe
May 2003	Presentation of EISPP at an IT-security congress organised by the German Federal Institute for IT-Security	Siemens	CERTs, policy makers	Germany
June 2003	Presentation at Websecurity 2003, presenting EISPP services as helpful in dealing with the most common security problems	Clusit	Companies dealing with e-commerce	Italy
June 2003	Technical meeting held as a BoF session at the 15th FIRST, which mainly focused on the common advisory format, and that produced a feedback that was later taken into account for the next version of the format	All	CERTs	Worldwide
September 2003	Presentation at a meeting of the German CERT community. A working group participating in the design of the next version of the EISPP format is established.	Siemens	CERTs	Germany
September 2003	Presentation to Pimecsefes (organisation of SMEs) focusing on security planning and implementation, and describing the advisory service	InetSecur	SMEs	Spain
September 2003	Update of the project carrying out and results at 10th TF-CSIRT meeting	All	CERTs	Europe
October 2003	Presentation of EISPP at a German IT-security congress organized by the Federal Academy for Security Policy and the University of Düsseldorf	Siemens	CERTs, policy makers	Germany
November 2003	Workshop organised by Firenze Tecnologia, a special agency of the CoC of Firenze, with the participation of Clusit amongst others, and mainly focusing on business continuity	Clusit	SMEs	Italy
December 2003	Workshop with the CoC of Toulouse, dealing with SMEs awareness on IT security, and focusing on concrete feedback from security services experiences	Cert-IST	CoC, IT SMEs, Security Consulting organisations	France
December 2003	Advisory workshop conducted at the German Federal Institute for IT-security	Siemens	CERTs	Germany

Date	*Description*	*Organiser*	*Audience*	*Dissemination level*
December 2003	“Public awareness day” during Cert-IST Forum, where amongst others the EISPP project was treated inside the general topic “Security monitoring – mission and experience feedback”	Cert-IST	Potential intermediaries (ISPs, telcos, administrations), IT managers	France
January 2004	Project update at 11th TF-CSIRT meeting, focusing on the common advisory format and the roadmap for establishing CEISNE	All	CERTs	Europe

6. OUTLOOK

There are clear indications that the work of EISPP has made an impact both on the European CERT landscape and on the provision of European SMEs with essential security information and services: the results of EISPP will continue to influence IT security within Europe.

6.1. CERT Co-operation based on EISPP

Within the European CERT landscape, the EISPP advisory format defined in D3.01 has excellent chances to establish itself as standard for exchanging advisory data. Not only will the EISPP CERTs continue to use the format, which makes it the only format to be used by more than one CERT in more than one country. Also, by now it seems certain that the EISPP format will be used within the German CERT community as basis for closer co-operation between German CERTs. Further, the EISPP format has been chosen as the basis for an initiative within TF-CSIRT to establish an IETF standard for advisory formats, which increases the chances that the EISPP format will be adopted by a significant number of European CERTs within the next years.

The EISPP advisory format provides a basis for CERT co-operation which, building on the experiences made within the project, can be extended from the EISPP CERTs to other CERTs with the aim of forming CEISNE, the **C**o-operative **E**uropean **I**nformation **S**ecurity **N**etwork of **E**xpertise. The direct continuation of EISPP as CEISNE by opening EISPP to additional members, however, is not possible: A central result of the experimentation phase conducted within EISPP was, that a centrally managed infrastructure for sharing and evaluating advisory information is essential, but during the EISPP project, a decentralized approach was used. As a consequence, D3.04 "CEISNE model and processes" describes a roadmap for establishing CEISNE under the auspices of an already established organization such as TF-CSIRT. Input from European CERTs gathered during the EISPP CERT workshop (see D2.01) show that there is interest within the European CERT community to establish means for better information exchange between CERTs. The roadmap for establishing CEISNE envisions better, structured information exchange between CERTs as a first step. As a next step, the increased use of the EISPP advisory format within Europe would enable closer co-operation between European CERTs on advisories, thus preparing the ground for significant workload sharing at least between smaller groups of CERTs. The EISPP partners are confident that a majority for adopting a roadmap towards CEISNE within TF-CSIRT can be found and will continue to work towards the establishment of CEISNE.

Within the German CERT community, as already mentioned above, first steps towards closer co-operation within the German CERT community – based on results of the EISPP project – have been undertaken. As a first project, the development of a system that allows the joint maintenance of data necessary for categorizing systems affected by vulnerabilities has been taken up. Such a system would complement the EISPP advisory format, and additionally could evolve into a standard useful for any kind of reporting about vulnerable systems, comparable to the CVE naming scheme. This German CERT co-operation is likely to provide additional impetus for the extension of European CERT co-operation and thus makes the adoption of a roadmap for establishing CEISNE within the European CERT community more likely.

To put it in a nutshell: results achieved by the EISPP project are likely to significantly shape the European CERT community within the following years.

6.2. Strategic role of the Intermediaries to reach SMEs

The more successful way to distribute the services is through an intermediary. The intermediaries like ISPs, ASPs, CoCs and outsourcing consultancy and security firms who manage IT-systems have a very important role in the organisation of the advisories dissemination service in order to easily reach a large number of final users (lots of SMEs are needed to make the service profitable, financially and economically feasible). They either represent the SME in their countries (CoC) or already have the infrastructure in place in order to sell and distribute the service like ISPs and

ASPs (customer database of SMEs, sales force, customer service, established subscription model service).

Intermediaries like ISPs/ASPs and outsourcing consultancy and security firms which already manage and market IT services with SMEs are the best suited to promote and provide security information to SMEs. They have to show to their clients that they worry about security issues, that they follow the threat and are aware of security vulnerabilities. In another case, these intermediaries may propose to their customers the advisory service as an addition to their package of services, or may not sell the service directly to the customer but rather forward the cost. A higher possibility of success happens when the intermediaries are aware of the IT security problems (this may be the reason why contacts with CoCs failed in some countries).

Last, a particular attention should be given to the case of the CoCs, who represent the SME in their countries and want to promote security awareness to them. Because they face financing issues, a partnership with outsourcing consultancy and security firms should be put in place.

6.3. Security services suited to the SME Profile

The European SMEs have very different profiles (size, activity domain, financial means, knowledge of IT and security motivation) which lead to different needs at the security IT level. So, the interest level regarding the "advisory dissemination" service is different from a SME to another.

- **The medium and large SMEs with security IT competences, motivation and equipments** (anti-virus, firewall, …) **and with dedicated ICT employees** (outsourced or not) are the best suited for the Advisory service. The result of the trial period and of the CoC workshop stated that these companies are interested in the typical advisory format, as provided during the project, with even more detailed information. For them it is mandatory to obtain an information service of high quality that contemplates the possibility of obtaining all the news about security related to their systems. This security information service could be provided either directly by CERTs or through Intermediaries (ASPs, ISPs or CoCs).

- **Small or Medium SMEs with minimum IT-knowledge and a little Security motivation** find the service useful. Because they have limited knowledge (in IT or in IT-security), they are not in a position to benefit from a full advisory service and prepared to pay for it. They are more interested and ready to invest in a transparent support service (like remote anti-virus management, automatic patch update, firewall set-up maintenance and scanning) than in an information service. The companies sized to provide this transparent support service are the intermediaries: mainly ISPs and ASPs, and possibly CoCs.

  In order to be valuable and attractive to them, the advisory service has to be strongly adapted to this group. These companies, less focused on IT and IT security, are still interested in the service, but with very limited, relevant and operative information. A requirement is to provide information in a form that is understandable by people without IT competence. Improvements have to be made in presenting, selecting and distributing the information to the user. This means at least translating the advisories into local language, even if the EISPP participants managed to use the English version, but also to avoid technical details or language.

  Most of these SMEs are aware of security vulnerabilities where public awareness is high (mostly viruses and worms: Nimda, Blaster, …). It is the reason why in order to protect their infrastructure they mainly rely on anti-virus software (with or without having updated the anti-virus signature), being first interested in viruses and worms instead of software or hardware vulnerabilities. They might not see vulnerabilities as a threat, neither the connection between vulnerabilities and worms propagation.

- **Very small and Small SMEs with no IT-knowledge, no ICT employees** (even outsourced), are neither interested in nor helped by the advisory service. This type of SMEs has a big lack of security awareness. To improve security, this group must be reached through embedded services provided via intermediaries. The intermediaries like ASPs and ISPs are sized to provide this kind of service.

One way to increase their security awareness is to provide them adapted security information only where public awareness is very high. Intermediaries like CoCs are sized to promote security awareness to these SMEs. The “raw” advisory service is not viable for this type of SMEs.

In general, most of the small and medium SMEs which have no security motivation have not tackled the IT security problem with the Return On Investment (ROI) point of view. For these SMEs, the IT security is a cost and not a profit, and the majority of them are more interested in “services” rather than in “advisories”.

Furthermore, to use a (new) service like the "advisory dissemination" service, SMEs in general must adapt their internal procedures to include this new service (most of the SMEs want somebody to do “what has to be done” when an advisory is received). During the trial period, many SMEs had not enough time to perform this action. If there is an IT team in the SME, then this SME is interested in receiving advisories. Extra work should not be added for system administrators (otherwise the service is likely to fail). However, the most relevant requirement, apparently for all companies, is that handling the advisories and applying the patches should require very little time and resources.

7. CONCLUSIONS

The main objective of EISPP was to set up a European framework aimed at providing European SMEs with essential IT Security services. To this end, the following secondary objectives were pursued:

1. to set up a network of expertise among the European CERTs which will allow them to share and enhance their own prevention material and to "open" it to the other CERTs and organisations involved in prevention.
2. to provide SMEs with adapted, useable and efficient services.
3. the dissemination of project results to the European SMEs and to the other key players.

Within the limitations applying to a take-up action between partners present within five European countries, EISPP has achieved these objectives or at least prepared the ground for further work by providing essential information about blocking points and enabling techniques.

1. Network of Expertise

Regarding the establishment of a network of expertise among European CERTs, the outlook given in Section 6.1 shows that with the EISPP advisory exchange format (see D3.01), which is likely to be adopted as a standard within the European CERT community within the foreseeable future, EISPP has created an essential corner stone for co-operation between CERTs. Co-operation based on the EISPP exchange format exists both in the form of continued co-operation of the EISPP CERTs and first steps of co-operation within the German CERT community. Taken together with the general interest in closer co-operation within the European CERT community, these results form a basis for the creation of a European network of expertise along the lines described in D3.04.

2. Provision of SMEs with security services

The contacts made with SMEs during the EISPP project showed that the major blocking point for providing security services to SMEs is the lack of security awareness in the SME world: IT security is mostly perceived as a cost factor without noticeable return on investment. Reactions of SMEs involved in the EISPP project showed that EISPP helped them better understand risks and solutions in the security management of IS, thus raising their readiness to deal with issues of IS security.

During half a year, EISPP gathered experiences with providing SMEs with a bundle of security services. These experiences, together with feedback collected from participating SMEs, allowed EISPP to evaluate each service with respect to its feasibility and usefulness for SMEs. By eliciting the respective security needs of different groups of SMEs, service improvements for tailoring security services better to SMEs' needs could be found (see D4.03, D5.03, and D5.04).

EISPP also examined the financial viability of marketing security services with a market survey (see D2.02) and a study of possible funding models (D4.04). Essentially, the distribution of security services to SMEs works best through intermediaries such as chambers of commerce and ISPs that already are in close contact with a large number of SMEs.

To put it in a nutshell, EISPP has collected information regarding both technical and economical issues essential for providing security services to SMEs. Other organizations interested into working with SMEs, for example in European countries that have not been involved in the EISPP project, can now benefit from the groundwork carried out by the EISPP. Regarding the EISPP partners themselves: follow-up activities for providing security services to SMEs have already been planned.

3. Dissemination of project results

Information about the EISPP project to SMEs has been disseminated both via dedicated workshops (using intermediaries such as Chambers of Commerce to reach SMEs) and by piggybacking EISPP presentations on several SME-oriented events (see D2.02 and D2.03). Dissemination targeted at the European CERT community via presentations at CERT meetings and a dedicated CERT workshop about EISPP (see D2.01) has succeeded in making EISPP well-known and in generating a high level of interest into the CERT-related project results.

As there is both continuing interest to further co-operation between CERTs and to expand and improve the provision of SMEs with security service, in both cases taking the results achieved by EISPP as a starting point, EISPP will continue to influence the European IT security landscape also after the end of the project.