SME Service description

Identifier: **EISPP-04-001-MI**

Version 2.0
Date 2003/05/08

Table of Content

Glossary

ASCII	American Standard Code for Information Interchange
ASP	Application Service Provider
CERT	Computer Emergency Response Team
CCI	Chamber of Commerce and Industry
CVE	Common Vulnerabilities and Exposures
EISPP	European Information Security Promotion Program
FAQ	Frequently Asked Questions
HTML	HyperText Markup language
HTTPS	Secure Hypertext Transfer Protocol
IDS	Intrusion Detection System
IIS	Internet Information Services
ISP	Internet Service Provider
IT	Information Technology
MS-SQL	Microsoft Structured Query Language
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
SME	Small and Medium Enterprise
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Simple Message Service
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
WP	Work package
XML	eXtended Markup Language
XSLT	eXtended Stylesheet Language Transformations
WPi	WorkPackage # i
WWW	World Wide Web

Related documents

Applicable Documents

Ref.	*Title*	*Version*	*Date*
EISPP-D3-001-TR	EISPP Common Advisory Format Description	1.2	2003/03/28
EISPP-D3-002-TR	EISPP - Requirements for CERT common vulnerability repository	1.1	2003/03/18

Reference Documents

Ref.	*Title*	*Version*	*Date*
	None		

1. EXECUTIVE SUMMARY

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.

The basic service provided by EISPP is an advisory service, i.e., the distribution of so-called 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. 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.

EISPP further experiments with value-added services to the advisory service with the aim of helping SMEs to 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).

2. INTRODUCTION

The EISPP project aims at developing a European framework, not only to share security knowledge but also to define the content and ways of disseminating security information to SMEs. By providing European SMEs with the necessary IT security services, SMEs will be encouraged to develop their trust and usage of e-commerce, leading to increased and better opportunities for new business. EISPP is a pioneer in the European Commission's vision of forming a European warning and information system on the basis of international networks and co-operation within the European Union.

The first security service SMEs will be provided with is an advisory service, i.e., the distribution of so-called security advisories that provides system administrators with precise and timely information about new vulnerabilities and what can be done against them. Such information is essential for IT security, because new vulnerabilities are discovered on a daily basis. IT systems can only be kept secure, if they are regularly upgraded or patched such that the latest security holes are closed.

The second service SMEs will be provided with is an additional security service that complements the advisory service. Whereas SMEs may not find security advisories helpful per se, they may, for example, find that the same advisories become useful when accompanied with tailored information on how to protect themselves against the described threats by using a virus scanner, intrusion detection system or vulnerability scanner (or indeed a combination of these).

This document is the first deliverable from EISPP WP4. This workpackage is responsible for defining security services expected by SMEs and to develop an "adapted" resource-funding model for this type of activity that is supplying SMEs with such security services. This document describes the services made available to SMEs within the EISPP project.

The document is organised into four main sections summarised as follows:

- proposed organisation around three entities: CERTs, intermediaries (ISP, ASP, CCI), and SMEs (section 3)
- security advisory service description (section 4)
- value added service description (section 4)
- PKI usage in relation to the services (section 5)

The services described in this document will be deployed during a six-months trial period; this document will be updated with additional information gathered during this period, e.g., by means of further interviews with SMEs, additional responses to questionnaires that were sent to SMEs, and experiences made in providing the services.

3. PROPOSED ORGANISATION

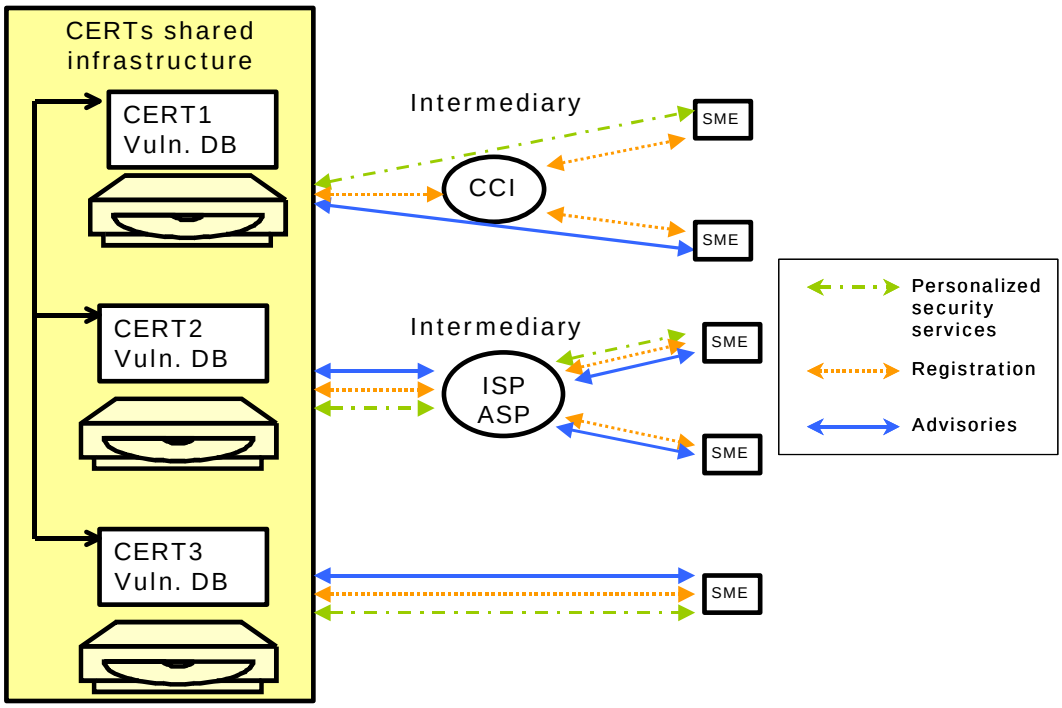
The proposed organisation is based around three entities: CERTs, intermediaries and SMEs.

- Level 1 corresponds to **CERTs** (Computer Emergency Response Teams) involved in the EISPP project and thereafter in an EISPP "network" of co-operating CERTs. CERTs provide security services (advisories and specialised services) intermediaries and SMEs described below.
- Level 2 corresponds to **intermediaries**: they add an intermediate layer between SMEs and CERTs. Because CERTs are usually not in direct contact with SMEs, they rely on intermediaries in order to reach the SMEs. Typically, they can be
  - ⇒ ISPs (Internet Service Providers),
  - ⇒ ASPs (Application service providers),
  - ⇒ CCIs (Chambers of Commerce and Industry).

  There are two types of intermediaries:
  - ⇒ The first one may just deal with SMEs registration, administration, follow up and help desk. The advisories and security services are directly provided to SMEs by CERTs.
  - ⇒ The second one not only deals with SMEs registration and follow up, but also receives security advisories and services provided by CERTs, and re-disseminates them to SMEs. This type of intermediary may add personalised security services (see Section 4.2).

- Level 3 corresponds to **SMEs** (Small and Medium Enterprises). SMEs are the beneficiaries of security services provided either directly by the CERTs, or through intermediaries.

The figure below shows how CERTs, intermediaries and SMEs interact:



4. SERVICES DESCRIPTION

This service description is based on all EISPP participant knowledge, on feedback received from SMEs via interviews and their answers of a EISPP questionnaire. The services listed in the following table are described in detail in Sections 4.1 and 4.2.

Security Advisory and Alert services	Security advisory dissemination service
	Alert dissemination service
	Profiling service
	Security information digital signature
	Advisory access/retrieval service

Value Added Services	Intrusion Detection Systems
	Vulnerability Scanning
	Patch Update Service
	Virus detection
	Firewall configuration
	Remote server maintenance, administration and patching

4.1. Security Advisory and Alert services

Security advisories are documents that contain timely information about newly discovered vulnerabilities: since new vulnerabilities are discovered on a daily basis, IT systems can only be kept secure, if they are regularly upgraded or patched such that the latest security holes are blocked. In order to do so, system administrators need precise and timely information about new vulnerabilities and what can be done against them. Security advisories containing such information are issued by vendors for their own products and CERTs for the products that are of interest to each CERT's constituency.

Indeed, the contents of a security advisory must allow a system administrator to quickly discern whether any of his systems may be affected, and to assess the severity of the vulnerability so as to judge how fast he needs to react. If ways to remove the vulnerability or at least to mitigate the risk are known, the security advisory should further inform the reader about these possibilities.

Even though the basic requirements for security advisories can be spelled out in a few lines as done above, practice shows that writing really helpful security advisories is not easy. The EISPP project therefore pools the expertise of four European CERTs to (1) define a common advisory format and (2) co-operate in the production of security advisories. As a result, EISPP partners will receive security advisories whose format has been distilled from four best practices and whose contents have been influenced by the expertise of four CERTs rather than a single one.

The advisory format developed with EISPP is based on XML, thus separating between "raw" advisory data and advisory presentation. The XML format will be used for exchanging advisory data between the member-CERTs of EISPP; this will allow efficient cooperation on the production of advisories. For presenting advisories to readers such as system administrators, standard transformation mechanisms such as XSLT can be used to transform an advisory in XML format into a presentation format such as HTML, ASCII, etc. Through this transformation, advisories also can be customized to a certain degree, for example by stripping out the more technical content fields of the XML format when addressing administrators with little expert knowledge.

It is important to note that EISPP does not provide one single "standard" advisory for each vulnerability that is treated: each member-CERT will continue to issue its own advisories for its own

range of supported products. The key in EISPP cooperation lies in the risk-rating of vulnerabilities treated by more than one member-CERTs plus sharing expertise when authoring advisories.

Because CERTs are in close contact with the security community, they are informed when high-risk threats arise on the Internet (for example, an exceptional virus activity, a generalised attack based on a vulnerability, etc.). In addition to disseminating information about such threats via security advisories, a CERT may want to quickly alert the SMEs about the important characteristic of the threat to take quick measures and react consequently. In order to do so, the CERT will release a document called "security alert".

Security alerts do not replace security advisories; they must be very exceptional in order to be treated with the proper urgency by SMEs.

Depending on each CERT organisation, the security alerts may or may not follow the EISPP common format (elaborated by the EISPP project i.e. WP3).

The next sections describe various aspects of the advisory service and they will be examined for each participant of the EISPP project. These aspects are:

- Security advisory dissemination
- Alert dissemination service
- Profiling service
- Security information digital signature
- Advisory access/retrieval service

4.1.1. Security advisory dissemination service

It is current practice for a CERT to offer its constituency a profile based dissemination (a profile is a list of systems that a SME will receive security information/services about) of advisories and alerts related to the latest vulnerabilities so as to (1) alert its constituency about potential threats to the security of their systems, and (2) to provide information about how to avoid, minimize, or recover from the damage.

The CERTs involved in EISPP project, will manage their SMEs and intermediaries as part of their own constituency. Each CERT manages a list of SMEs and intermediaries in order to send them security advisories and alerts.

Note: The management of SMEs list (Email addresses) and profiles can be delegated to the intermediary. In this case, the intermediary will send all information to CERTs.

esCERT (Spain) service

All services are released and managed by esCERT-UPC and commercialised by INETSECUR (Spain).

Users of Security Advisory service receive daily-customized advisories via email about all new vulnerabilities discovered in their computer and network systems. All these advisories fulfil the EISPP Common Format. Advisories are sent using the standard protocol SMTP (Simple Mail Transfer Protocol).

SMEs using this service need an email client that is able to display ASCII or HTML content.

CALLINEB (Sweden) service

The Security Advisory dissemination service is the basic, entry-level service CALLINEB provides its customers with. Advisories are distributed via e-mail and fax. The requirements are that SMEs and Intermediaries can use e-mail or have a fax machine.

As a complement to the advisory service, CALLINEB offers an information service that can be used by customers who wish to get more information than CALLINEB provides in the advisories. This can for example be the complete discussion about a discovered vulnerability on a mailing list, something that CALLINEB cannot provide in advisories.

CALLINEB gather large amounts of information on a daily basis from e-mail discussion lists and web pages. This information is stored in archives (HTML-based) for easy access. The information is read and sorted (based on operating system, application, hardware, etc). CALLINEB also put a severity rating on the information contained in the gathered information. Thus, CALLINEB make it possible for its customers to filter out unneeded information. This saves time for the customer since they will not need to read each and every message on BugTraq, Incidents and so on in order to find the information they need.

Cert-IST (France) service

The Security Advisory dissemination service is the basic service provided by Cert-IST to its SMEs/Intermediaries.

The requirements are that the SMEs and Intermediaries can use an e-mail client.

CLUSIT (Italy) service

CLUSIT is an intermediary between CERTs and Users. Its role is simply to collect advisories and forward them to the proper persons. This may include some limited help desk activity, e.g. because advisories are not in the SMEs native language. Advisories won't be fully translated. However, if the requirement arises, CLUSIT will investigate the issue. No PKI usage is required between CLUSIT and the User, since advisory authentication is handled by the CERTs.

I.NET (Italy) service

I.NET operate as an intermediary between the SMEs and CERT disseminating Security Advisory using a multi channel media.

The SMEs can choose to receive Security Advisory by e-mail and, or, consulting a website. The requirements for user depend on the chosen media. To use the mail channel the user has to handle mail clients and PGP. I.NET will give the user a basic help with understanding PGP usage and philosophy.

The SMEs that choose the web channel have to know how to use a web browser and X.509 certificate; if necessary, I.NET will provide all information about the installation and use of personal certificate.

4.1.2. Alert dissemination service

esCERT service

The esCERT alert service provides its clients with specific information about new attack patterns (ways of exploiting existent vulnerabilities).

This information is sent via e-mail, with S/MIME signature, and can be used by customers to update their protection/detection systems configuration.

CALLINEB service

CALLINEB issues alerts based on published information, submitted information and rumours. The alerts have a confidence level stating the reliability on the information in the alert.

The customers receive the alerts primarily via e-mail (PGP-signed and in some cases also encrypted) but there is an archive where the customers can access current and archived alerts. Alerts that are sent encrypted are stored unencrypted on the website.

Alerts are issued only when the impact of the problem is serious.

Cert-IST service

When an intensive usage of an important vulnerability occurs or a worm is spreading widely, Cert-IST may decide to publish an alert.

The goal of an alert is to warn quickly SMEs/Intermediaries about a threat. This alert (sent in an S/MIME signed e-mail) explains the reasons of its publication (e.g. the threats) and the technical basics of the threat.

Usually an advisory giving the full details of the problem is published either before or after the release of the alert.

I.NET service

Users can activate an alerting service via their profile. Users are alerted via e-mail, fax or SMS. The alerts may inform that important information is available on web site or was sent by mail.

4.1.3. Profiling service

The advisory providers (i.e. CERTs) offer a profile-based service: 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.

esCERT service

Advisories customisation is realized by allowing SMEs to subscribe to the platforms they are interested into (out of a range of platforms supported by esCERT); the platforms are classified by vendor. Furthermore, personal data such as the mail accounts to which advisories are to be sent can be managed. The profile is maintained via the web. SMEs using this service need a web browser to edit their profile.; Authentication is carried out either via username and password or a certificate provided by esCERT).

CALLINEB service

The SMEs are able to define profiles to personalise the content on CALLINEB web as well as what advisories they are interested in receiving.

The profile based service filter out unwanted advisories based on a SME's profile. Larger organisations with multiple profiles get advisories sent directly to the person listed in the respective profile.

The customers can change their profiles to match organisational changes in their company via a configuration page in CALLINEB client system. To ensure privacy and secure transmission of sensitive information access to CALLINEB web based client system is protected via HTTPS and X509 client certificates.

Cert-IST service

This service enables the SMEs/Intermediaries to choose the products they are interested into from a list of products released by Cert-IST. Thus they will only receive, by e-mail, advisories for those products, and when browsing Cert-IST Web site, they will only see the advisories related to them.

If an SME requires new filtering criteria, it can submit a request to Cert-IST who will update the service accordingly.

Cert-IST offers two languages for its advisories: French and English. An SME can choose to receive advisories in French, in English or in both languages.

Cert-IST allows its SMEs/Intermediaries to choose between three formats for the advisories: TXT, HTML or XML (or a combination of these).

Different advisory content is offered to SMEs and intermediaries: to start with, two different content models (“expert” content and “basic” content) should cover the requirements of most SMEs organisations: it is anticipated that small organisations without expertise regarding information systems will be interested in a very basic presentation of security advisories (with only description of risk and the solution), whereas organisations with some expertise will prefer to receive comprehensive information.

CLUSIT service

CLUSIT will help the User in collecting the information required for profile registration, and will act as intermediary between the User and the CERTs. This will provide the user with an interface speaking its native language; information can be collected in Italian and translated by CLUSIT. PKI usage will be adapted to the needs of the CERTs. CLUSIT will help in the integration of the CERT PKI in the user infrastructure (e.g. checking that the proper certificate is accepted by the User). This will reduce the technical skills required to SMEs to use the service.

I.NET service

I.NET collects and redistributes security advisories to its users. Advisories are stored in a database and translated to Italian language. Users can profile the access by choosing language, media (web or mail) and alerting.

4.1.4. Security information digital signature

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 take into account this requirement, CERTs digitally sign the security advisories and alerts before sending them to SMEs.

esCERT service

esCERT security advisories are signed using a X.509 digital certificate. This certificate was released specifically for signing the security advisories.

SMEs only need an e-mail client compatible with the S/MIME standard for authenticating the advisory sender, that is, to verify the signature in each security advisory.

Cert-IST service

In order to send the advisories and alerts by signed Email, Cert-IST uses the S/MIME encryption mechanism, which is recognised by most of SMEs' Email clients.

The requirements are that the customer can use an e-mail client compatible with S/MIME standards for advisory authentication. To authenticate Cert-IST signature, Cert-IST certificate is signed by a major Certification Authority (VeriSign).

CALLINEB service

CALLINEB security advisories are signed with CALLINEB PGP-key (support for other signing methods will also be used) and can be encrypted if the recipient requires this. . The requirements are that SMEs and Intermediaries can use e-mail or have a fax machine and that they can use PGP for authentication of the advisories.

CALLINEB provides basic help with understanding PGP if the customer has no prior experience in using the product.

I.NET service

I.NET digitally sign Security Advisory translated into Italian language using PGP. A basic help will be provided to user to use and understand PGP system.

4.1.5. Advisory access/retrieval service

In addition to the profile-based advisory distribution, a vulnerability database is made available to the SMEs.

esCERT service

Users of Security Advisory service can also consult via web a mySQL Database which contains all the security advisories released by esCERT-UPC (using HTTPS). This Database also contains information about thousands of vulnerabilities that appeared during the last years.

SMEs using this service need a web browser to access to this information and the same account username/password or the personal X.509 certificate mentioned previously.

CALLINEB service

CALLINEB stores all published advisories on the customer part of its website. The customers can access via WWW all advisories issued in the archive section. The archive is searchable and profiles can be used.

CALLINEB does not provide the SMEs with the possibility to get previously published advisories sent via e-mail. If there are requirements of such a service CALLINEB will investigate the issue.

The basic service includes no filtering thus giving the customer access to all advisories regardless of what the SME needs.

All SMEs get personalised X509 certificates for each member of the staff that needs access to the web based system. CALLINEB uses 128 bit SSL for access to its website and the X509 certificate for authentication.

Each SME gets access to a common area in the system where they can access advisories and other services CALLINEB provides and they subscribe to.

If a group of SMEs want to have a common area (sector based) CALLINEB can provide them with an area where they can share information within this group.

Cert-IST service

All previously published Cert-IST advisories are available on the Cert-IST private Web site for its SMEs/Intermediaries.

Depending on its profile, an SME is able to browse only the advisories concerning the products it is interested in. Also a search engine is available for the SMEs: it allows to search advisories by keywords or by reference numbers (advisory reference or CVE reference for instance).

To access the Cert-IST Web site, the SMEs need to access to Internet via the HTTP/HTTPS protocol and to have a personal X509 certificate in order to use this service.

I.NET service

I.NET collect security advisories from CERTs and stores them in a database that can be accessed by SMEs using a web front-end.

Authentication to the web server is carried out by X.509 certificate and secured by SSL. Basic help will be provided to the SMEs in order to use and to install the certificate.

4.2. Value added services

The value-added services have the aim of helping SMEs to make full use of the information contained within the advisories. For most of the SMEs, the vulnerability advisory service is not enough by itself; for example, SMEs may need assistance to adapt the available security mechanisms (such as firewalls or antivirus) to the new threat. A possible way to provide value added services is to add to the security advisories information related to a specific security mechanism, or to use the information provided in the advisories to improve security mechanisms settings remotely.

The objective of EISPP WP5 is to evaluate the real viability and utility of such type of services. The services described in the following are carried out by the participants of WP5 (see Section 4.2.7).

4.2.1. Intrusion Detection Systems

Intrusion Detection Systems are useless if not properly updated to deal with new attack patterns. In a Distributed IDS the goal is not just to monitor an Internet connection, but also to deal with internal attacks. Vendor supplied updates need to be tuned to the SMEs' situation, and other control need to be added (e.g. traffic peaks for specific services, or alarms for specific messages). This is a hard task for most SMEs, especially if new needs are to be evaluated after each advisory.

Therefore, a IDS configuration and update service will be deployed to SMEs. Thus, updates will be properly installed and tuned, and additional controls will be put in place when required.

A key factor in the viability of this service as value-added service for advisories, is that standard rules can be detected and applied to different users, so that costs and time can be reduced to the needs of most SMEs.

4.2.2. Vulnerability scanning

This service is based on a computer placed in the network of the customer that will use Nessus (http://www.nessus.org/) to scan the critical systems at the SME's site. This is done to establish a baseline. A preferred configuration is developed and implemented on each system. A new scan will be performed every week and the deviations from the agreed configuration will be reported.

Information about the systems is also stored in a central system making it possible for the SME to get information about new vulnerabilities related to these systems. This gives the SME a better overview of vulnerable systems in their organisation making it easier to maintain a higher level of security.

When new advisories are released and related test methods are available the systems are tested for the vulnerability. The results of the tests are processed and cross-references to existing advisories are added to the report.

With the information given in the scan report and the information present in related advisories the SME has the information needed to take appropriate actions in order to close the vulnerability or, if no known fix is available, information on how to detect possible attempts to exploit the vulnerability or possibly other ways to minimise the risk of exploitation of the vulnerability.

4.2.3. Patch Update Service

Combined with the vulnerability scanning service (see section 4.2.2), this service provides the solution for the problem found.

Whenever a new security related patch is released by the vendor, the patch update service will report this to the SMEs.

The information about new patches can be included into an advisory or if the vulnerability is regarded as less severe, into the Information Service (see section 4.1.1).

For less common systems and applications, the service monitors new security related patches and includes them into the Information Service. If the vulnerability is considered to be severe, the service has the option of releasing an advisory to stress the importance of the vulnerability despite the fact that it is a less common system or application.

The service does not perform any validation service on the patches, it just provides the customers with the information that patches are available. The service can however help the SMEs to set up a test environment at their site in order to verify that the patch will not break anything in their environment.

4.2.4. Virus detection

The virus detection service consists of three components described below.

4.2.4.1. First component: virus/worm alerts

The first component is virus/worm advisory/alert dissemination. According the severity of the virus/worm threat, the service will release an advisory or alert.

This advisories/alerts will provide:

- a virus/worm description,
- information to detect manually the virus/worm on a comprised host,
- elements to check, for a given anti-virus (for only defined anti-virus software), whether the anti-virus is updated in order to protect hosts/networks against the virus/worm.

For critical alerts only, the service will also attach in the e-mails sent to SME/Intermediary the official anti-virus editor's signature (for only defined anti-virus software) to detect the virus/worm. This service prevents the SME/Intermediary to receive signatures in a timely fashion without being affected by the possibly overload of servers of the anti-virus editors that is likely in a critical situation.

4.2.4.2. Second component: technical support regarding anti-virus domain

The second component is a limited technical support (with quota) service available for SMEs and intermediaries.

This service will be provided via phone support and a FAQ available on the website.

It will provide answers regarding

- virus/worm issues (for example: "I have a virus. What do I do ?"). The FAQ will centralize the main requests to publish them to the whole EISPP community.
- configuration of anti-virus software (to be updated regularly, to have an optimised detection engine,...).
- checks whether anti-virus software is updated to protect the hosts/networks against a defined virus/worm.

4.2.4.3. Third component: technical support for worm-related incident response

Finally, the third component will help the SME/Intermediary to check whether his network (SME) or the network of his customers (Intermediary) is protected against the important threat. The main (and the most harmful) worms released on Internet during the last years rely upon the automatic exploitation of a known vulnerability (Microsoft IIS, MS-SQL, etc.). So, for specific situation (wide worm spreading), the service will use specific tools (scanner) to detect whether networks/hosts are vulnerable for a given worm.

4.2.5. Firewall configuration

When a new vulnerability is discovered, or a new worm start spreading, there is usually a time delay between the advisory dissemination and when production systems can be updated to deal with the problem. This because patches may not be immediately available (especially when localized for the different countries), and changes to production systems require some care and testing. In the meantime, the user network can be unprotected. Temporary filters on a firewall can greatly reduce the risks of this situation, and to avoid that local infected hosts may help in spreading the worm.

The firewall configuration service will examine the advisories and their ratings, and decide with the user if a temporary rule is required on the firewall.

A key factor in the viability of this service as value-added service for advisories, is that standard rules can be detected and applied to different users, so that costs and time can be reduced to the needs of most SMEs.

4.2.6. Remote server maintenance, administration and patching

The objective of the service is to carry on the activity of maintenance, administration and patching as soon as it's necessary. The activity of remote maintenance is carried on in two ways: periodical activities and on demand activities.

- Scheduled activities:
  Every week, the service will access the user network to check the functionality of servers under observation. For example, the following will be checked:
  - ⇒ system logs,
  - ⇒ disk status,
  - ⇒ application responsiveness.

- On demand activities:
  The aim of these services is to satisfy those requests that cannot be scheduled. For example, the following activities are performed:
  - ⇒ security advisory application,
  - ⇒ system management,
  - ⇒ user requests,
  - ⇒ coordination with vendor for hardware replacement.

The patch service is carried out under responsibility of the user, i.e., the patch is not validated beforehand. For mission-critical projects, the user is suggested to use a test environment for testing the patch.

The service is carried out using remote access tools and protocols; to avoid unwanted access much care is taken to ensure a secure channel.

4.2.7. Services and EISPP participants

Each participants involved in each service during the project are listed in detail in the table below.

Value added services	Participant involved
Intrusion Detection Systems	**INETSECUR (Spain) and CLUSIT (Italy)**
Vulnerability Scanning	**CALLINEB (Sweden)**
Patch Update Service	**CALLINEB (Sweden)**
Virus detection	**Cert-IST (France)**
Firewall configuration	**CLUSIT (Italy)**
Remote server maintenance, administration and patching	**I.NET (Italy)**

5. PKI USAGE IN RELATION TO THE SERVICES

The PKI related topics in relation to the service described previously are listed below for each participant.

esCERT usage

The access to the web site related to the Security Advisories Service is secured via SSL; authentication is carried out with a digital certificate or a username/password account.

The Certification Authority of The «Universitat Politècnica de Catalunya», which is being administered by esCERT-UPC, has released all certificates. All security advisories are signed with a digital certificate released by the same Certification Authority.

CALLINEB usage

SESIC Cert Team currently uses PGP for advisory signing and SSL with client certificates for secure access to its website.

The certificates used in the SSL communication are self-generated, but CALLINEB has plans to cooperate with Chambersign (http://www.chambersign.se/), which issues certificates supported by the Swedish Chamber of Commerce.

Cert-IST usage

Cert-IST currently uses S/MIME technology for advisory signing and HTTPS/SSL with X.509 client certificates for secure access to its website.

The certificate used to sign Cert-IST advisories through S/MIME has been released by Verisign. This solution allows this certificate to be automatically authenticated by standard SME mail clients (this Cert-IST certificate is signed by a CA imported by default in most of browsers/mail clients).

The X.509 certificates used in the SSL communication may be:

- generated by the Cert-IST PKI
- generated by Chambersign PKI (http://www.chambersign.com), which already works with French Chambers of Commerce (http://www.chambersign.com/partners.htm).

The second solution will be chosen by default because Chambersign certificates are already used by French SMEs to access to secure French administration websites.

CLUSIT usage

Being intermediaries, CLUSIT won't produce advisories. CLUSIT may accept the Certificates that information providers will ask it to use.

I.NET usage

I.NET service fulfils best practice on secure communication between user and supplier.

E-Mail distribution channel uses PGP architecture. The web server channel is secured using SSL and X.509 certificates. Thawte certificates are used for SSL, and I.NET's own certificates for X.509.

6. CONCLUSION

The document describes the security services that will be provided to SMEs. They are organised around three entities CERTs, intermediaries and SMEs. The security services will follow two different options:

(1) Security advisory and alert dissemination. In order to ensure the reliability of the information, sender authentication, information integrity and confidentiality will be provided using cryptographic measures. Each security advisory sent to SMEs or intermediaries will follow the EISPP common advisory format.

(2) Additional value added services based around the advisory distribution. The security advisories will be complemented with information on how to protect against the described threats by using, for example, virus scanners, intrusion detection systems, vulnerability scanners, firewall technology, and remote system update/patching.