# CERT workshop conclusions

*Identifier:* **EISPP-D2-001-TR**

Version 1.0

Date 2003/07/29

# Table of Content

# Glossary

| | |
|---|---|
| EISPP | European Information Security Promotion Programme |
| CSIRT | Computer Security Incident Response Team (1) |
| CERT | Computer Emergency Response Team (2) |
| CEISNE | Co-operative European Information Security Network of Expertise |
| WP | Work-Package |
| TF-CSIRT | Task Force of CSIRTs |
| FIRST | Forum of Incident Response and Security Teams |
| TERENA | Trans-European Research and Education Networking Association |
| BoF | Birds of a Feather |

(1), (2) In the present document, CSIRT and CERT are considered synonymous terms.

# Related documents

## Applicable Documents

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

## Reference Documents

| *Ref.* | *Title* | *Version* | *Date* |
|---|---|---|---|
| RD01 | EISPP common advisory format description<br>Available on www.eispp.org | 1.2 | 2003/03/28 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 1. INTRODUCTION

One of the main goals of EISPP is to lay the foundations for a cooperative network between European CERTs. This network, the CEISNE (Co-operative European Information Security Network of Expertise), should allow European CERTs to co-operate in the process of writing security advisories.

Several co-operation models for such a network of expertise are thinkable; within the EISPP project, the project partners are actively experimenting with different models. However, to make sure that all aspects of CERT co-operation are considered and that all relevant requirements of European CERTs are taken into account, EISPP has to actively seek the input of European CERTs.

To involve non-EISPP CERTs in the project, beyond keeping them in touch with it through several presentations at the CERT meetings, a CERT workshop was held in which interested CERTs could learn details about the work of EISPP and give feedback to EISPP.

In this document we first describe how non-EISPP CERTs were kept up-to-date with the developments within EISPP and through which meetings, beside the CERT workshop, feedback on the work of EISPP was gathered. We then sum up the happenings at the CERT workshop and present a summary of the workshop's results. These results will influence the further shape of EISPP considerably.

# 2. EISPP AWARENESS PROGRAM

The main goals of the third workpackage (WP3) of EISPP are

(1) to develop an advisory exchange format that has the potential to become a (European) standard, i.e., to be used by a significant number of European CERTs,
(2) to lay the foundations of a European network of excellence in which CERTs co-operate on advisories.

Both goals can only be realized if European CERTs are aware of the EISPP programme and have the possibility to have their say on both the advisory format and the shape of the network of excellence that is to be established. Therefore, members of the EISPP consortium have been continuously working to put EISPP on the map of the European CERT landscape, starting well before the official start of the EISPP programme.

The main vehicle to reach European CERTs were CERT meetings at national, European, and international level. Additionally, bilateral contacts between members of the EISPP consortium and various CERTs have been established. These activities both prepared the EISPP workshop held in Warsaw (see Section 3) – e.g., for advertising the workshop – and complemented it.

In the following, we examine activities in which other CERTs were made aware of EISPP and kept up-to-date with the progress within EISPP, as well as "technical" meetings and contacts for gathering feedback from CERTs not present at the EISPP workshop.

## 2.1. Keeping other CERTs aware of EISPP progress

The most important platform for informing European CERTs about EISPP and its progress were the so-called TF-CSIRT meetings. TF-CSIRT is a Task Force established under the auspices of the TERENA -Trans-European Research and Education Networking Association- Technical Programme, to promote the collaboration between European CSIRTs (aka CERTs) through sharing experiences and knowledge. Meetings are held between two and three times per year in locations all over Europe.

Before the official start of the EISPP project, Michel Miqueu from Cert-IST gave a presentation about EISPP during 6th TF-CSIRT meeting (May 2002, Copenhagen, Denmark). In this presentation, Michel Miqueu explained the main goals of EISPP, namely to establish a European CERT network and – based on co-operation within such a network – a SME services project providing comprehensive IT security services to SMEs and other target groups such as Chambers of Commerce or ISPs.

Michel Miqueu gave a brief update on the EISPP project at 7th TF-CSIRT meeting (September 2002, Syros, Greece), regarding the start of the project three months before (June 2002) and the web site that would be available the following month. He also informed the attendees that a workshop was being planned to be held in Warsaw adjacent to the 9th TF-CSIRT meeting.

A further update was presented by Michel Miqueu at 8th TF-CSIRT meeting (January 2003, Zagreb, Croatia). WP3 was described in detail; most importantly, the participants were made aware of the first deliverable of WP3 available to the public: the description of a common advisory exchange format. The EISPP workshop – to be held in Warsaw, in

May 2003 – was advertised. The participants were informed about the goal of the workshop, namely to discuss the achievements of EISPP, thus gathering the necessary feedback from European CSIRTs to the project.

Finally, during 9th TF-CSIRT meeting (May 2003, Warsaw, Poland) the latest update of the EISPP project so far was presented. Bernd Grobauer from Siemens CERT talked about the common advisory format, the experiments with the co-operation models (running since April 2003), and the collection of feedback and requirements from other parties such as SMEs and CSIRTs. Further, a first overview over the EISPP workshop held two days before was given.

On an international level, the FIRST Technical Colloquium held in February 2003 at Uppsala University (Sweden) was used to inform CERTs about EISPP (FIRST stands for Forum of Incident Response and Security Teams, and organizes one annual conference and two annual technical colloquia; FIRST is an international coalition composed of a growing number of CSIRTs from government, commercial, and academic organisations). Bernd Grobauer presented the EISPP programme through a talk entitled “EISPP – A First Attempt on Prevention Co-operation”. The talk gave an overview of the three key work packages of the programme, and focused then on WP3.

Also, national CERT meetings have been used to present CERTs with the work of EISPP, gather feedback, and advertise the CERT workshop.

- In April 2003, Udo Schweigert from Siemens CERT gave a presentation about the common advisory format during a German CERT meeting.
- In May 2003, Bernd Grobauer gave a talk about EISPP at an IT-security congress organized by the German Federal Institute for IT-Security.

## 2.2. Technical meetings and contacts

Apart from the EISPP workshop (see Section 3), a technical meeting was held as a "birds-of-a-feather session" (BoF) at the15th Annual Computer Security Incident Handling Conference organized by FIRST in Ottawa, Canada. The BoF was chaired by Bernd Grobauer and brought together nine participants from eight different institutions, four from the US, four from Europe.

The BoF focused mainly on the common advisory format. The vulnerability classification scheme as well as possible systems for categorizing affected systems were discussed in depth. The feedback given to EISPP during the BoF will be taken into account for the next version of the common advisory format.

Bilateral contacts regarding the advisory format have been established with several organizations, e.g., CERT/CC and PreSecure.

# 3. THE EISPP CERT WORKSHOP

The EISPP CERT workshop was held in Warsaw on May the 28th 2003, one day before the 9th TF-CSIRT meeting. The rationale to hold the workshop in conjunction with the TF-CSIRT meeting was that many European CERTs regularly send representatives to TF-CSIRT meetings, and therefore could participate in the workshop without much additional overhead. By and large, this reasoning proved to be sound; some persons, however, who expressed an interest into participating, could not do so, because a different workshop took place on the same day as well as the day before.

There were fourteen people present at the workshop, belonging to ten different European organisations related to computer security. The workshop focused on collaboration between CERTs in a network of excellence with the main focus on authoring security advisories. During the workshop, the common advisory format was examined and discussions were carried out on how to collaborate and how to ensure fair exchange of information. The feedback made by the attendees was very useful and will influence both the future development of the EISPP project and, beyond it, the shape of the network that is to grow out of EISPP.

Please refer to Annex A for the full detail of the workshop. Here we present the major findings of the workshop. These findings are derived from the comments and discussions that occurred during the workshop. They are presented in the same order as for the workshop agenda : first the findings about the **advisory common format**, then those about the **cooperation** process and finally those about the **CEISNE** model. Each finding is summed-up in a key sentence and then explained in a paragraph.

## 3.1. Findings about the common format

**F01: The audience considers the EISPP common format as valuable and useful.**

The advisory common format, that has been designed by EISPP, has been considered by the workshop audience as valuable and useful. It was judged as

- a model to be considered by CERTs that want to start writing advisories.
- a model that includes features that may be used to enhance the format currently used by some participants. Typically, these participant would like to add the features found in the EISPP common format to those found in other models.

However, as explained later in the present report (see F04), the advisory common format has not been seen by the audience as a prerequisite for CERT cooperation on advisories.

**F02: Vulnerability classification and assessment is considered as one of the most important points of the common format.**

Some participants are mainly concerned with forwarding advisories of other issuers, and they usually just complemented them with some header information. Such participants pointed out that rewriting all these advisories into the common format is not feasible and also raises legal questions (copyright, liability, etc.) It was agreed, however, that the EISPP common format contains features, that are worth being used also in such a situation.

The **vulnerability classification scheme** proposed by the common format is an example of such a feature: vulnerability information that conforms to the EISPP common format could, for example, be included in the header attached to forwarded, original advisories. Several participants proposed ideas to improve the assessment model. If further resources are to be spent on developing the common format, this area appears as the most promising one to investigate.

Another feature that was discussed is the "**system classification**". Currently, there is no fixed model within the EISPP common format to indicate which products are impacted by a given vulnerability. Designing a unified "system classification" model would be a valuable enhancement of the current EISPP common format.

## 3.2. Conclusions about collaboration on advisories

**F03: There is a general consensus that there is a need for more exchange on advisories between CERTs.**

All the workshop participants agreed that there is still very little amount of exchange between CERTs in the area of security advisories. There was a general consensus that there is a need for more exchanges between CERTs (and other "white-hat" sources) about advisories.

There was, however, no clear preference regarding the nature of information that should be exchanged between CERTs and the topics that should be discussed. The expectations largely vary from one participant to the other. Suggestions were made to exchange information regarding, for example,

- *vulnerability analysis*: freshly discovered vulnerabilities have to be investigated, product vendors have to be contacted, etc. By exchanging information, CERTs could collaborate in this very early stage of handling new vulnerabilities.
- *advisory contents*: once a vulnerability has been analysed and the first advisories started to appear, discussion would focus on advisory contents such as tests of patches, possible workarounds, etc.
- *incidents*: information regarding incidents caused by the exploitation of a given vulnerability could be shared and analysed.

The focus of EISPP, up to now, was clearly on the second item. While the first concern, collaboration on first-hand vulnerability analysis, probably would fit rather well into the EISPP framework, the third concern is probably out of scope.

**F04: Exchanging knowledge on advisories is a prerequisite to further collaboration.**

In the opinion of the workshop participants, there are two steps (or two levels) for CERTs to work together in the area of security advisories :

- First : exchange information about advisories (see F03)
- Second : exchange parts of advisories, or co-author advisories.

The audience clearly supports the first level. The second one is seen as a step that has to be addressed after the first has been achieved.

**F05: Collaboration on authoring advisories can occur only between CERT with the same "writing style".**

One of the problems with collaboration that was put up for discussion is that, even though a common format is used, advisory styles still can vary considerably. This is a practical problem for collaboration within EISPP, as no two EISPP CERTs' advisories could easily be substituted for each other: there are concise vs. comprehensive advisories, advisories with links to every single patch vs. advisories with a single link to a vendor site, etc.

All in all, sharing parts of advisories or even co-authoring them is very difficult as long as different advisory styles are used. This is another reason for the assessment made by the workshop's audience that cooperation by exchanging information has to be attempted as a first step. Once the network of expertise has reached a sufficient number of members, it should be easier for one CERT to find another one that authors its advisories in a similar writing style. Then, close collaboration between CERTs with the same "writing style" should be a real possibility (see also F08).

## 3.3. Conclusions about CEISNE

The CEISNE is a network of expertise to be set up after the EISPP project's completion; CEISNE implements the cooperation model to be defined by EISPP. Because all European CERTs will be invited to join CEISNE, the expectations of the workshop participants with respect to CEISNE are very important for the EISPP project. There is of course a close relationship between findings about the collaboration on advisories (as presented in Section 3.2) and the expectations for the CEISNE (listed below).

**F06: CEISNE must provide first a way to exchange know-how about advisories.**

This conclusion is the natural continuation of the F03 and F04 items.

CEISNE must be a forum through which participants can share information on security advisories. There is no strict guidance on the nature of the information that has to be exchanged, and every participant is welcome to post any information he/she thinks is relevant to help other in the matter of security advisory.

A mailing list (or a web forum) dedicated to security advisories might be a possible way to implement that capability.

**F07: CEISNE Code of Conduct must not be too coercive.**

The code of conduct to be obeyed by all members of CEISNE must be rather loose, containing only a minimum set of rules such as responsible use of information, obligation to inform about issued advisories, etc.

It has been stated that it is too soon for establishing more strict rules (e.g., to regulate "fair" exchange of information). As a consequence, CEISNE members must decide themselves whether the gain they draw from CEISNE justifies their contribution to CEISNE. Whether more elaborate rules are feasible can only be established after CEISNE has been operative for some time.

### F08: CEISNE size must reach a critical mass for close collaboration between participants to be possible.

During the discussion it became clear that the number of teams who join and participate in CEISNE is a key element for the success of the network. If the number of participants is too low, benefits from being part of CEISNE would be too low. Only, if "critical mass" is reached, i.e. there are enough members actively contributing with information, CEISNE can be successful. Also, if many members participate in CEISNE, chances are that some of them issue advisories in a comparable style, which opens up possibilities for closer cooperation (see F05).

### F09: CEISNE must allow participants to share only parts of their advisories.

Expecting that all CEISNE participants will provide to the others a raw copy of their advisories is not realistic. For example, a commercial CERT cannot give for free to CEISNE members the services it sells to its customers. CEISNE must take this aspect into account. A possible solution could be for a CERT to provide to CEISNE only part of their advisories or to release them only after a certain period of time.

As pointed out in F05 and F08, CEISNE should bring together participants that have a similar view on security advisories. Such participants might want to establish a closer cooperation together and make private arrangements for that. There was no general agreement, however, whether CEISNE should promote such cooperation, or they are out of its scope.

# 4. CONCLUSION

When designing the EISPP project framework, we did consider the CERT workshop as one of the major milestones in the project performance. This is because getting the feedback from non-EISPP CERTs, about the network of expertise EISPP aims to set up, is rather important for the success of such a network. The workshop held in Warsaw met our expectations, and it will definitely influence EISPP future work in the area of CERT collaboration on security advisories (EISPP work-package #3).

Because of the announcement program we had before the workshop (see chapter 2), almost all the European CERTs that participate in international exchanges were aware of the EISPP CERT workshop event. It means to us that the expectations collected during the workshop are representative of most of the current expectations of European CERTs on security advisories.

From these expectations (further described in chapter 3) we derive the following directions for EISPP future works:

- There is a large demand for more exchanges between bodies such as CERTS on security advisories. Such exchanges must be first implemented as informal exchanges, with no strict rules on the nature of the information exchanges, and light regulation procedures. EISPP must cover this requirement when designing CEISNE.
- We are also convinced that, when the number of participants will grow, the demand for efficient collaboration processes will also raise. This is the reason why EISPP must continue to define and to experiment with such processes.
- Finally, some very interesting suggestions were collected about the EISPP advisory common format. Incorporating them into the format will of course improve it, and it may also promote its adoption by other CERTs.

# ANNEX A: CERT WORKSHOP MINUTES

The EISPP members who were present are:

- Philippe Bourgeois (Cert-IST, France)
- Bernd Grobauer (Siemens CERT, Germany)
- Domingo Cardona (esCERT-UPC, Spain)
- Manuel García-Cervigón (esCERT-UPC, Spain)
- Joan Ramon Patón (esCERT-UPC, Spain)

The attendees were:

- Francisco Monserrat (RedIRIS, Spain)
- Jan Drömer (Phillips GmbH, Germany)
- Marius Urkis (LITNET CERT, Lithuania)
- Cathy Booth (NISCC, UK)
- David Parker (NISCC, UK)
- Mark Oram (NISCC, UK)
- Rolf Gartmann (SWITCH, Switzerland)
- Karel Vietsch (Terena, The Nethernalds) (partially)
- Przemek Jaroszewski (CERT Polska, Poland) (partially)

After welcoming the participants and a quick round of introductions, Philippe Bourgeois (PBo) presented the workshop agenda:

| | |
|---|---|
| **9:00 - 9:30** | **Registration & Coffee** |
| **9:30 - 9:50** | **General introduction**<br>**- Agenda (Philippe Bourgeois, Cert-IST France)**<br>**- Introduction of the participants** |
| **9:50 - 10:30** | **Introduction about the project**<br>**- Project status on the CERT cooperation aspects (P. Bourgeois)**<br>**- Presentation of Common Format (Bernd Grobauer, Siemens CERT Germany)**<br>**- Introduction to sessions (P. Bourgeois)** |
| **10:30 - 12:00** | **Session #1 : Cooperation process (Domingo Cardona, esCERT-UPC Spain)** |
| **12:00 - 13:30** | **Lunch** |
| **13:30 - 15:00** | **Session #2 : Establish fair exchanges (P. Bourgeois) (*)** |
| **15:00 - 15:30** | **Coffee break** |

| | |
|---|---|
| **15:30 - 16:30** | **Close-up session**<br>**- Review of sessions**<br>**- Discussion regarding advisory format**<br>**- Any other business** |

**(*) In substitution of Peter Bivesand from Callineb Consulting (Sweden) who could not attend for personal reasons.**

Philippe Bourgeois then generally described the EISPP project and summed up the results that had been achieved up to that point of time. After some general had been answered, the workshop proceeded following the agenda.

## Presentation of common format

Bernd Grobauer went deeper inside the common format and the way to use it properly. The fact that the exchange format uses XML to structure the data was seen as a useful tool by the workshop attendees

It was stated that it may be difficult to reach the same risk in an advisory if every participant uses different ways of writing the advisories. Bernd Grobauer said that the designed scheme (requirements, expertise, exploitation…) should lead to the same risk. A future feature might be to distinguish between workstation, server, etc., even belonging to the same vendor. Philippe Bourgeois added that it's each CERT's responsibility to say for example that an attacker can take control of a machine, but not to decide which consequences it can lead to (this is a decision of the affected organisation).

It was doubted that a CERT can re-evaluate every vendor's security advisory (the person who raised the point deals with about 1000 advisories per year). Philippe Bourgeois said that the classification scheme used in rating an advisory aims at reducing the time needed to perform such a rating.

There was a question regarding the procedure to follow in case an advisory is re-rated a short time after having been released (for example if an exploit appears). The common format does not prescribe whether to issue a new advisory or to update and republish the original advisory; for both approaches, the advisory format provides containers for useful meta data

## Session #1: Cooperation process

Domingo Cardona focused on the way advisories are circulated between the EISPP members and on how to collaborate in rating vulnerabilities and writing advisories. One of the main issues is the trade-off between extensive discussions about advisories and the CERTs' response time in issuing an advisory One possible approach is to send out *urgent* advisories immediately, performing necessary updates afterwards.

It was agreed that a central repository where to put all the advisories is necessary such that all useful tools for getting an overview, grouping advisories, collecting information, etc., only have to be written once and then used by all participants.

Talking about rating a vulnerability described within an advisory published by a vendor, Philippe Bourgeois clarified that the assessment process carried out by CERTs is likely to be different from that performed by a vendor: as a consequence, any advisory usually needs some extra research to be carried out by a CERT. In the case of EISPP, the comparison of research and rating performed by several EISPP participants constitutes a sort of quality control for this process.

The discussion then returned to the common format. Two important conclusions were pointed out: (1) the common format is a good start, but does, of course, not solve the problem of how to co-operate sensibly; (2) more important than issuing advisories is the information exchange between the EISPP members.

Asked about whether they would use the common format or not, many participants answered with a 'yes'. Some went further and suggested that may be some vendors would be interested in using it, too.

Bernd Grobauer gave a short overview over the eCSIRT project, which tries to share and co-operate on incident data. There seem to be some similarities with EISPP, mainly with respect to designing a common format; there are, however, also significant differences, especially with respect to possibilities for co-operation based on the exchange of data in a standardized format.

### Session #2: Establish fair exchanges

During the last session Philippe Bourgeois closed the presentations talking about CEISNE (Co-operative European Information Security Network of Expertise), a network of expertise that is intended to be the continuation of the EISPP project once it finishes. Ideally, such a network should ensure fair exchange of information, so that each CERT would gain as much from the network of expertise as it contributes.

Free exchange of information may become problematic as soon as two or more commercial CERTs that are part of CEISNE have overlapping markets: Obviously, such CERTs would not want to share all information with a potential competitor.

Several attendees expressed the expectation that the rules and regulations that govern CEISNE cannot be overly strict: CERTs themselves must decide whether they receive a fair return on the information they are sharing. As a minimum, participants should share within CEISNE what they would make public, anyhow –CEISNE would just serve as a forum to collect all this information. Commercial CERTs could, for example, only share parts of their new advisories and make the complete data available at a later point of time when no commercial value is associated with it anymore.

# Document management information

| | |
|---|---|
| *Title* | CERT workshop conclusions |
| *Identifier* | EISPP-D2-001-TR |
| *Confidentiality*[1] | PU |
| *Status* | Approved |
| *Creation Date* | 2003/07/29 |
| *Version* | 1 |
| *Revision* | 0 |
| *Revision Date* | |
| *Deliverable Reference* | D2.01 |
| *Authors* | Philippe Bourgeois, Bernd Grobauer, Peter Bivesand, Joan Ramon Patón |
| *Keywords* | Workshop CERT Warsaw EISPP |

# Approval Section

| *Company* | *Alcatel CIT* | *Callineb* | *CLUSIT* | *SIEMENS* | *UPC* |
|---|---|---|---|---|---|
| *Date* | | | | | |
| *Comments* | PGP | PGP | PGP | PGP | PGP |
| *Approving Person* | Pierre Forget | Peter Bivesand | Claudio Telmon | Udo Schweigert | Manel Medina |

[1] Confidentiality indicator according to the following table

| | |
|---|---|
| PU | Public |
| PP | Restricted to other programme participants (inc luding 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) |

# Document History

| *Version* | *Date* | *Reason for modification* | *No. of pages* | | |
|---|---|---|---|---|---|
| | | | *added* | *modified* | *deleted* |
| 0.1 | 2003/06/20 | Creation | all | | |
| 0.2 | 2003/07/07 | Major changes in the document skeleton | | all | |
| 0.3 | 2003/07/10 | Chapter 1 and 3 added | | § 1, § 3 | |
| 1.0 | 2003/07/29 | All comments merged | | all | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |