

21.06.07

## Deliverable DJ2.3.2: Security Service Specification



### Deliverable DJ2.3.2

Contractual Date:	31.10.06
Actual Date:	21.06.07
Contract Number:	511082
Instrument type:	Integrated Infrastructure Initiative (I3)
Activity:	JRA2
Work Item:	3 (Infrastructure for Co-coordinated Security Incident Handling)
Nature of Deliverable:	R (Report)
Dissemination Level	PU (Public)
Lead Partner	GARR
Document Code	GN2-07-127v3

**Authors:** Claudio Allocchio (GARR)

### Abstract

The Security of the GÉANT2 backbone relies not only on the ability to ensure a well operated Security Service inside the GÉANT2 backbone, but also to the networks connected to it (NRENs) and the networks of the local institutions connected to the NRENs at campus/site level. The pilot security coordination service run within the JRA2/WI3 activity has helped to evaluate the various elements of the Security Service (see DJ2.3.1,1), giving them an extensive field test and creating the specification given in this document. This document specifies the elements needed to run the GÉANT2 Security Service, and defines which elements are either optional or mandatory.

## Table of Contents

0	Executive Summary	i
1	Security Operations Scenario	1
2	Security Service Framework	3
2.1	Service Activities	3
2.1.1	MUST	4
2.1.2	SHOULD	4
2.1.3	MAY	5
2.1.4	Service Activity Building Blocks Architecture	5
2.1.5	Escalation Procedures	6
	Mentoring Scheme	7
3	Conclusions	8
4	References	9

## Table of Figures

Figure 1.1:	Security Operations Hierarchy in GN2 and beyond	2
Figure 2.1:	Building block architecture for a Security Service and Joint Research activity	6

## 0 Executive Summary

The Security of the GÉANT2 community relies not only on the ability to ensure a well operated Security Service inside the GÉANT2 backbone, but also to the networks connected to it (NRENs) and the networks of the local institutions connected to the NRENs at campus/site level. The pilot security coordination service run within the JRA2/WI3 activity has helped to evaluate the various options (see DJ2.3.1,1). After this extensive field test, the current Security Service specification has been defined, with the JRA2/WI2 toolset becoming part of a well managed Security Service and integrated into the service requirements.

This document specifies the elements needed to run the service. It defines which elements are optional and which are mandatory. It is expected that adherence to the requirements in this service specification will enable all GN2 partners to run their own operations at an acceptable security level and thus contribute to reach an acceptable security level for the whole GÉANT2 community.

Project:	GN2
Deliverable Number:	DJ2.3.2
Date of Issue:	21/06/07
EC Contract No.:	511082
Document Code:	GN2-07-127v3

# 1 Security Operations Scenario

The following statements from DJ2.3.1,1 give the background for this document:

“The security of a backbone depends heavily on the security of the networks connected to it, and this fundamental concept shall be extended further, down to the single computers and networked objects that can reach the backbone. As a consequence, making the backbone secure includes a large number of people, each one with his/her own “security domain”; even the real end-users, like those using a Personal Computer or perhaps a VoIP telephone, are thus part of this scenario, too.

For these reasons, coordination among different security domains is needed: vertically, at least from the NREN level down to each single end-user; but also horizontally, when you reach the inter-NREN relationships. The current hierarchical model has indeed proven to be very effective at national level, where many NRENS have established their own national security service (often called CSIRT or CERT). However, at GN2 backbone level, a horizontal approach (where NRENS’ security services handle at peer multiple-partner-level incidents) seems to be more effective than a single centralised service.”

“Outside the NRENS and GÉANT2, there are of course other entities comprising the Internet, both as Research and Education further partners, but also including Governments and commercial users/providers of the network. All of them belong to the global security scenario as well, interacting with the NRENS and GN2 security deployment.”

Project:	GN2
Deliverable Number:	DJ2.3.2
Date of Issue:	21/06/07
EC Contract No.:	511082
Document Code:	GN2-07-127v3

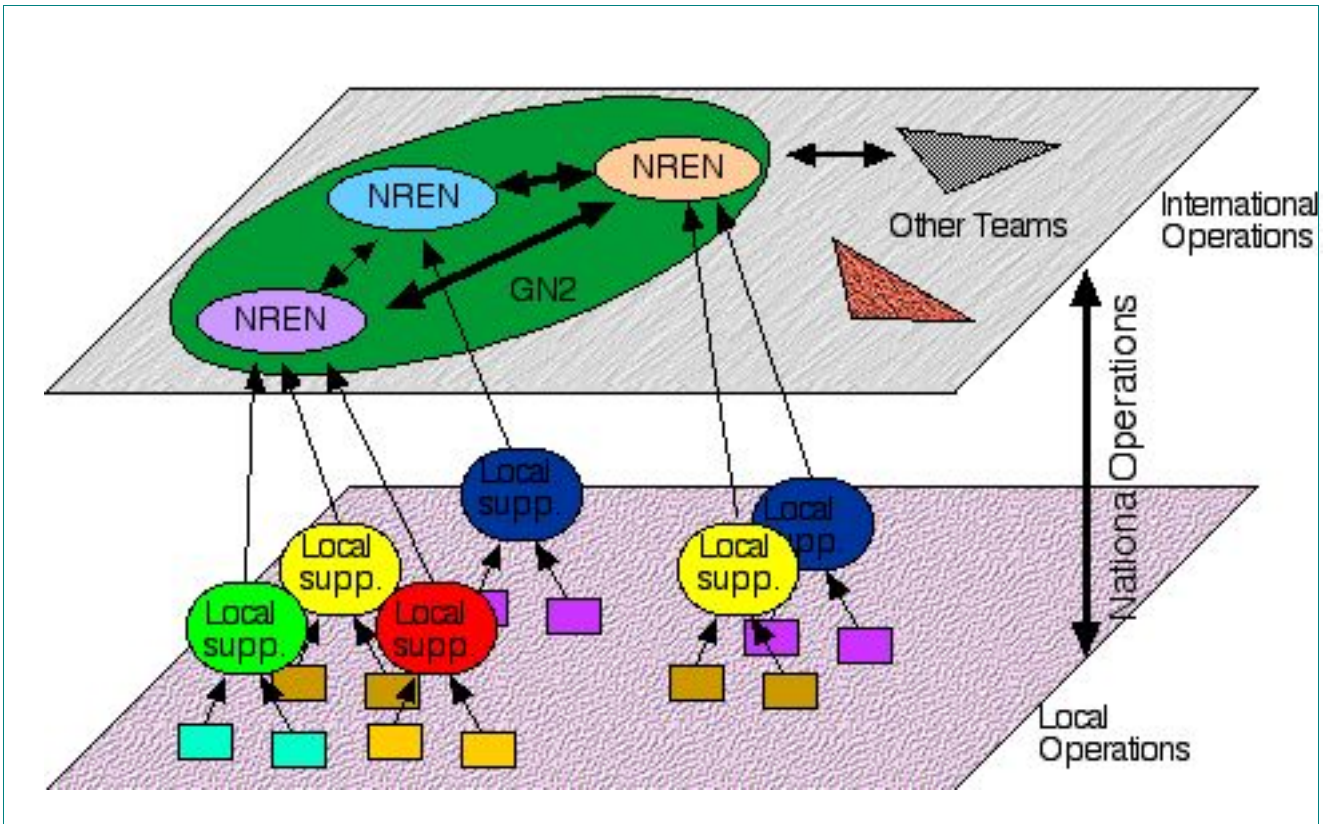


Figure 1.1: Security Operations Hierarchy in GN2 and beyond

The GN2 Security Service is the “glue” that ensures the operations inside the top green area of Figure 1.1 work smoothly, and allows the safe coordination with external bodies. For further details, see DJ2.3.1,1.

In general, security handling is managed directly by the security team(s) who take care of the domain(s) involved. Also, the DANTE security team will provide utilities for facilitating the distribution of information and handling of security cases that affect most or all of the GN2 partners.

Project:	GN2
Deliverable Number:	DJ2.3.2
Date of Issue:	21/06/07
EC Contract No.:	511082
Document Code:	GN2-07-127v3

## 2 Security Service Framework

Security operations can be performed efficiently, quickly and effectively among GN2 partners by using a joint human and technical network. The elements involved are trained and configured (respectively) for their role, and interact with the other elements in the most efficient way. In JRA2/WI3, the Pilot coordination service participants have experimented with a number of activities to enhance the efficiency of international incident handling. Please see DJ2.3.1,1 for a list and evaluation of the specific elements.

The Pilot Phase 1 proved that a more modular approach towards security handling coordination is needed at the international level among GN2 partners. In particular, there are some core requirements that must be fulfilled by all participating teams, while a number of other activities are just recommended or are useful optional add-ons.

Another important result from the Pilot Phase 1 is the distinction between activities useful in “production” security operations, and experimental or pure research activities that might become useful in the future but are not yet ready for active service. While research activities should continue inside the research part of the JRA2, this document focuses only on service activities.

A “Security Coordination Service” is envisaged. This will consist of a mailing list containing all the GN2 security contact email addresses, and of regular meetings of all the GN2 Security teams to exchange information and discuss matters specific to the GN2 Security Service. These meetings should coincide with any existing meetings that many GN2 partners already attend (for example TF-CSIRT or JRA2).

### 2.1 Service Activities

The basic activities for the NREN Security Teams are divided into the categories MUST, SHOULD, and MAY. These categories are defined in RFC2119 [RFC2119].

- MUST contains activities that are essential and strictly compulsory for the teams participating in the GN2 Security Operations.
- SHOULD contains activities that are strongly recommended to the teams due to their usefulness, however participation in the GN2 Security Operations is possible even if not all of these activities are performed

- MAY activities are optional, and will not cause adverse effects if not installed

A minimal Service Level Agreement (SLA) must be signed by all partners of the Security Service Activity and must include all the items listed in “2.1.1 MUST”.

### 2.1.1 MUST

Security Teams must:

- Be accredited inside the community. The Trusted Introducer is a well-established service, is recognised by the global Security Operations community at large as the “accreditation service”. Any Security Team must perform the TI Accreditation procedure, and reach the level of “Accredited” team. A Security Team must remain at “Accredited” level, and update the information listed there.
- Provide its team and members with PGP Public Keys to the other teams. The keys must be available from the PGP Public Key Servers.
- Sign any email message related to an incident with PGP keys.
- Maintain a documented web site about itself, containing (as a minimum, and in English); team contact information, team PGP Keys (or a link to the PGP key server), and information on how to open an incident ticket. This web site must be kept up to date.
- Acknowledge incoming requests generated by other Security or Network Operation teams within a reasonable timeframe. The acknowledgement must also be sent if the team cannot handle the incident. If the Security Team contacted can handle the Incident, either a Trouble Ticket or a Unique Incident Identifier must be included in the acknowledgement. In all cases, incoming Trouble Tickets or Unique Incident Identifiers must be preserved in the acknowledgement and all subsequent communications.
- Inform the team that signalled an incident if information comes to light during the handling of that incident that affects the domain of that team.
- Send the “incident closure” information to the team(s) that sent the original Incident handling request.
- Make information non-disclosable (for example, by using encryption or other content protection methods) if the exchange between Security Teams handling an incident involves sensitive information or personal data.
- Consider all incident information to be confidential and not disclose incident information beyond the scope defined by the information source.

### 2.1.2 SHOULD

A Security Team should:

- Document its Best Common Practices (BCP) and make these available to the other teams.
- Make its Communication and Authentication Policy for the keys and certificates it uses publicly available.
- State the severity classification of an incoming incident request in the acknowledgment to that request, and also the default handling time for the incident. If the incident is a known incident, the acknowledgement should also refer to any available information relevant to the incident.

- Inform the team that signalled the incident about progress if the expected incident closing time changes significantly.
- Use a Trouble Ticket system, or a similar tool, to keep track of incident handling.
- Counter sign the PGP keys of each team or team member by other teams. New Security teams and team members should participate in an appropriate Key Signing Party at least once.
- Install security tools whenever available, and use them to enhance incident handling operations and/or create proactive security functions. These tools should be the toolset itself or have functionally equivalent functionalities.

### 2.1.3 MAY

A Security Team may:

- Inform the team that signalled an incident about the internal escalation procedures that are being adopted.
- Redirect the signalling team to another appropriate team if an incident cannot be handled directed by a Security Team.
- Include automated information (like IODEF formatted information) in the reports exchanged with other teams.
- Make information about the X.509 Certificates its member and/or the team uses to sign/encrypt information available. If the Certificates are issued by a Self-Signed Certification Authority (CA), then all the information about the CA (for example fingerprints, CRLs, OCSP) should be available.

### 2.1.4 Service Activity Building Blocks Architecture

As proved during the Pilot Phase, a single, all encompassing approach to security services and research is not achievable. We need to provide a “building blocks” architecture that allows elements to be added easily, as well as the addition and growth of entire new teams inside the service.

The basic elements of the architecture are those marked as MUST blocks, which are the minimal entry requirements. The addition of optional (SHOULD and MAY) blocks enhances the status of the participating team and the global security of GN2, but is not a (strict) requirement.

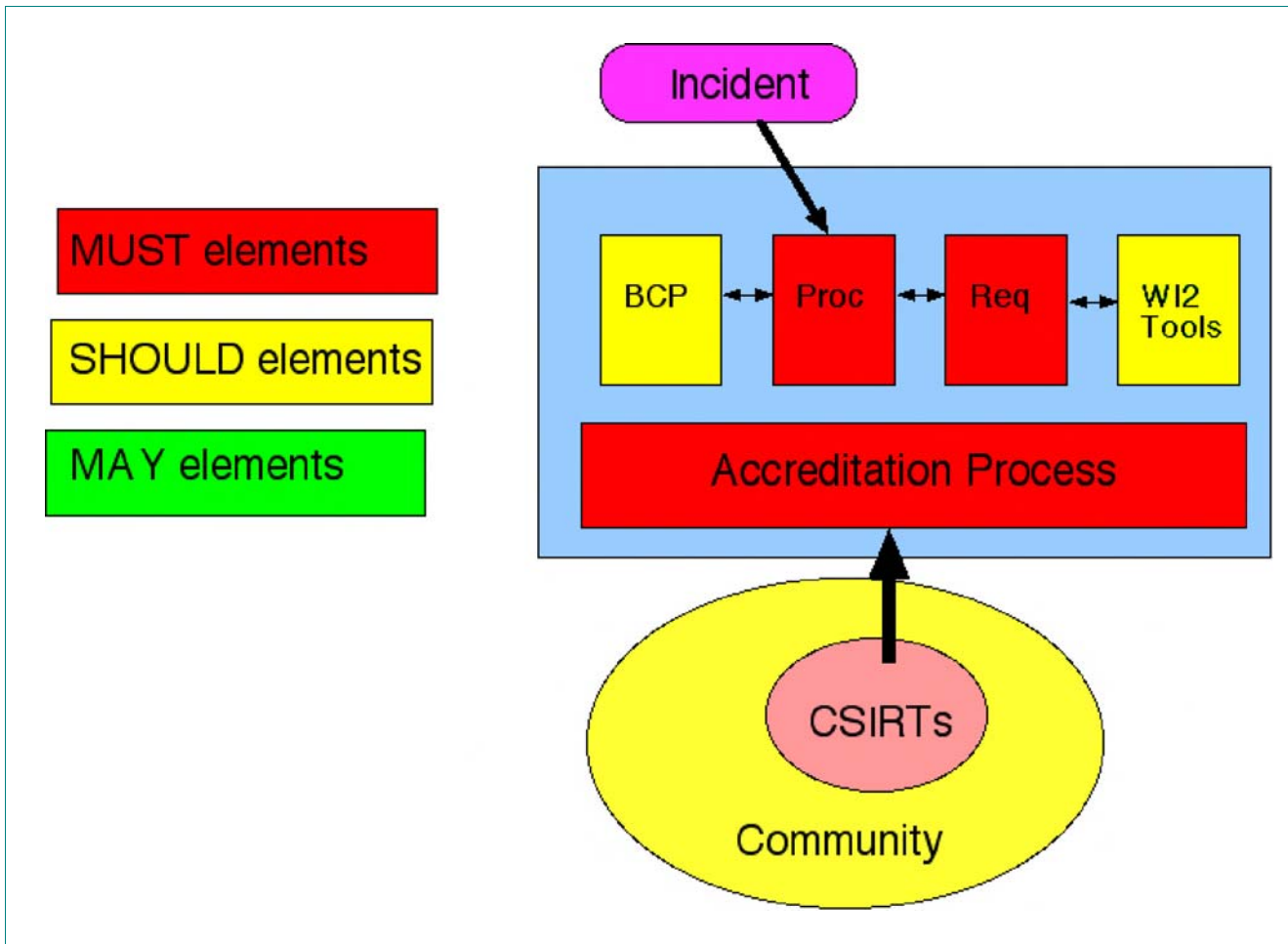


Figure 2.1: Building block architecture for a Security Service and Joint Research activity

Legend:

- BCP: Best Current Practice
- Proc: Procedures
- Req: Requirements on the capabilities of CSIRT teams
- WI2 Tools: The JRA2 Toolset

### 2.1.5 Escalation Procedures

Although there is common agreement on what is to be considered a “security incident” (mainly based on [eCSIRT] results and described in DJ2.3.,1), there may be cases where there are different interpretations of an incident, resulting in no common response strategy among different teams. In case an escalation of the incident is needed, the specific case shall be escalated through the management of the relevant partners.

## Mentoring Scheme

The GN2 Security Service provides a mentoring scheme, using the members of JRA2/WI3 to support the creation of new security teams, and help existing teams fulfil their requirements.

Bringing new teams on board not only means accreditation, validating existing procedures and pointing out initiatives to help them start (for example the TERENA CSIRT Starter Kit initiative [STARTKIT]); it also: involves training.

The TRANSITS [TRANSITS] project, and its continuation in collaboration with FIRST [FIRST] and ENISA [ENISA], produced a relevant set of training modules and experience in setting up courses and hands-on laboratories. Some GN2-specific training modules concerning the toolset produced by JRA2/WI2 have been developed and field-tested. It is planned that a general module pointing out the value of traffic monitoring tools for incident prevention and handling will be developed and added to the TRANSITS training material. That new general module will refer to the tools produced by JRA2/WI2 as examples .

In order to obtain the best possible results from the mentoring activities, a road map will be created in collaboration with GN2 JRA2/WI3 and GN2 NA4 network activity (managed by TERENA). In this roadmap, information from NA4 is integrated with security specific items, and specific actions for each NREN are described in the mentoring plans. In general, mentoring activities can include both NA4 specific visits to the mentored team, or training support for new teams from one of the JRA2/WI3 participants. Collaboration with NA4 (and, if needed NA8) also includes financial support, out of NA4 and NA8 already existing budget.

Mentoring is not limited to MUST activities, but can also be used to help teams improve their ability with SHOULD and MAY actions.

Any mentoring activity should be accompanied by a specific “action plan”, describing the items involved in the action, and the target results. This plan shall be used by the teams involved to help achieve the expected results.

### 3 Conclusions

The definition of the GN2 Security Service elements makes the operation of a coordinated Security Services within all GN2 partners possible. The Mentoring Scheme will bring GN2 partners to the minimal level required for Security Service. The Security Service should, however, increase its target minimal level of service, migrating SHOULD elements to MUST whenever possible, and adding new MAY and SHOULD activities as advanced research inside JRA2 progresses and produces new tools and suggestions. A strong collaboration and integration of GN2 JRA2/WI3 and GN2 NA4 and NA8 activities is required.

## 4 References

<b>[CERT.ORG]</b>	<a href="http://www.cert.org/csirts/services.html">http://www.cert.org/csirts/services.html</a>
<b>[TI]</b>	<a href="http://ti.terena.nl">http://ti.terena.nl</a>
<b>[I2]</b>	<a href="http://www.Internet2.edu">http://www.Internet2.edu</a>
<b>[CANARIE]</b>	<a href="http://www.canarie.ca">http://www.canarie.ca</a>
<b>[CLARA]</b>	<a href="http://www.redclara.net">http://www.redclara.net</a>
<b>[eCSIRT]</b>	<a href="http://www.ecsirt.net/cec/">http://www.ecsirt.net/cec/</a>
<b>[RFC2119]</b>	<a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>
<b>[STARTKIT]</b>	<a href="http://www.terena.nl/activities/tf-csirt/starter-kit.html">http://www.terena.nl/activities/tf-csirt/starter-kit.html</a>
<b>[TRANSITS]</b>	<a href="http://www.ist-transits.org/">http://www.ist-transits.org/</a>
<b>[FIRST]</b>	<a href="http://www.first.org">http://www.first.org</a>
<b>[ENISA]</b>	<a href="http://www.enisa.eu.int">http://www.enisa.eu.int</a>