

01.05.07

Deliverable DJ2.0.1: Plan for Implementation of Security Standards for GÉANT2 NRENS

Transition of Parts of JRA2 into Production Service



Deliverable DJ2.0.1

Contractual Date:	31/12/06
Actual Date:	01/05/07
Contract Number:	511082
Instrument type:	Integrated Infrastructure Initiative (I3)
Activity:	JRA2
Work Item:	0
Nature of Deliverable:	R (Report)
Dissemination Level	PU (Public)
Lead Partner	SWITCH
Document Code	GN2-06-253v4

Authors: Christoph Graf (SWITCH)

Abstract

This Deliverable addresses issues around and plans in place to bring parts of JRA2 into production

Table of Contents

0	Executive Summary	iv
1	Introduction	1
1.1	Environmental Considerations	1
1.2	Relevant Products of JRA2	2
1.2.1	Policy Maintenance and Enforcement	2
1.2.2	Training Services	2
1.2.3	JRA2 Software Products	2
1.2.4	JRA2 Hardware Products	3
1.3	Current Status of JRA2	3
1.4	Success Factors of JRA2	3
2	Process of Transition	5
2.1	(Main) Stages of Transition	5
2.1.1	Stage 1: GN2 Security Service Specification	5
2.1.2	Stage 2: GN2 Service Roadmap	5
2.1.3	Stage 3: GN2 Service Roadmap Implementation	5
2.2	Conduct and Sequence of Transition	6
2.3	Development and Deployment of NFSEN Software	6
2.3.1	Release Management	6
2.3.2	Support and Maintenance	7
2.4	Development and Deployment of FlowMon Probe	7
2.5	Possible Main Issues	7
2.5.1	Issue 1: Support and Maintenance for the FlowMon Probe	7
2.5.2	Issue 2: From Recommendations to Policies	7
2.5.3	Issue 3: Training Material Delivery and Maintenance	8
3	Resources	9
3.1	In the Transition Process itself	9
3.2	Estimated to Operate the Service	9
4	Conclusions	10
5	References	11
6	Acronyms	12

Table of Figures

Figure 2.1: GANTT chart of security service deployment

6

Project:	GN2
Deliverable Number:	DJ2.0.1
Date of Issue:	01/05/07
EC Contract No.:	511082
Document Code:	GN2-06-253v4

0 Executive Summary

The ultimate goal of JRA2 is to make the GÉANT2 community as secure as required. The security expectations towards the partners will be defined in Year 3. The gap between the individual partners' capabilities and the expectations will be assessed and a roadmap drafted to fill this gap. Covered in this deliverable are efforts to reach the state, where security expectations are met.

The term “production service” applied to the context of JRA2 means therefore adherence to agreed upon expectations. The main focus is on enabling all GÉANT2 partners to assume responsibility for the security of the elements they own of relevance to the GÉANT2 community.

Several issues are brought up in this document relevant for the process of implementing security standards for the GÉANT2 community:

- From Recommendations to Policies: The security recommendations proposed by JRA2 (DJ2.3.1,1; Report on Pilot Phase 1 and Recommendations) were to date not discussed enough outside of JRA2. Efforts need be undertaken to gain managerial support for those recommendations at large. Discussing Deliverable DJ2.3.2 (GN2 Security Service Specification, due in Month 26) will allow those bodies to decide on “how much security” is required for the GÉANT2 community.
- Training Services: Training material for “The Toolset” will be developed. While the first workshop will be organised by GÉANT2, we will study whether the training material will in the future be delivered on its own, or whether and at which stage it should be integrated into existing training events relevant to the CERT community.
- Support and Maintenance for The FlowMon Probe: The current solution, where the core developers of the FlowMon probe provide release management, support and maintenance is not satisfying in the longer run. For reasons of scalability and sustainability, CESNET is currently studying options to offer sustained and professionalized release management, support and maintenance, including transferring these tasks to a new legal entity. CESNET will present their options shortly.

1 Introduction

This Deliverable will define the basic package of services to be developed for production within JRA2 and a description of the environment. It will include a description of the features and technology choices for the proposed services, tools and the production framework. The Deliverable will also include a service rollout plan for JRA2.

1.1 Environmental Considerations

Several aspects of the environment in which JRA2 is acting are of crucial importance to understand the way JRA2 is operating:

- The hardware, tools and services (and to some extent also policies) being developed in JRA2 are primarily developed to support the security teams themselves in their work. Often, even the developers themselves are members of security teams. The users of the products under development in JRA2 are therefore well integrated into the development process.
- Security teams are usually pretty open to collaborate on security issues with peers, but only if the environment suits well and mutual trust between individuals is established. Several initiatives exist to foster such collaboration. They are usually not open to participation for everybody. The following initiatives and organisations may serve as examples: FIRST, TF-CSIRT, TI (see [FIRST], [TF-CSIRT] and [TI]).
- Security teams have to prepare for the unknown. Tools and services need to offer adequate flexibility and ad-hoc extensibility to be useful in fighting completely new forms of security incidents. CERT staff members need to have a very broad knowledge of issues around computer systems and networking.
- NREN security teams do usually not offer services directly to end users, but only interact with the security contacts of their respective customers.

1.2 Relevant Products of JRA2

The following subchapters are devoted to four products of the works carried out in JRA2: Policy maintenance and enforcement, training services, software product support and hardware product support.

1.2.1 Policy Maintenance and Enforcement

The initial writing of the GÉANT2 security policy and its associated best common practice document (DJ.2.1.1 and its updates) was carried out by JRA2 and it will be maintaining those documents during its remaining lifetime with guidance from the GÉANT2 policy bodies. This security policy deals primarily with securing the provisioning and operation of the core services of the GÉANT2 network. The GN2 security service specification (DJ2.3.2) is broader in scope and covers the security expectations and requirements of the GÉANT2 community towards its partners.

The task of maintaining those policies can easily be taken over by working groups initiated and mandated by policy bodies of the GÉANT2 community as seen fit.

1.2.2 Training Services

The security recommendations in DJ2.3.1,1 (Report on pilot phase 1 + Recommendations) propose minimum security recommendations, which will be formalised DJ2.3.2 (GN2 security service specifications) and revisions thereof are expected in future phases of GÉANT2. The need for action will differ from partner to partner; it will obviously be highest for those partners not yet hosting a security team and will be assessed during Year 3 of JRA2. The development and offering of training modules on the JRA2 Toolset is part of WI-3 in Year 3.

1.2.3 JRA2 Software Products

The analysis tools NFSEN and NERD were studied in greater detail in earlier phases of JRA2 (see [NERD] and [NFSEN]). Out of those, NFSEN is currently the only analysis tool in “The Toolset” which is recommended for GÉANT2 community-wide adoption. This choice may be extended in future phases when new functionality is added to “The Toolset”.

Sustained software support for NFSEN is crucial to the success of “The Toolset”. The same applies to all other and future products forming together “The Toolset”.

1.2.4 JRA2 Hardware Products

The development of the FlowMon netflow probe is part of WI-2 of JRA2. First prototypes became available early in Year 2 of GÉANT2 and were subsequently trialled by members of JRA2 (see: DJ2.2.2: User and test report of the NetFLOW collector). The FlowMon probe is now part of “The Toolset”.

Sustained support for the FlowMon probe is crucial for the success of “The Toolset”.

1.3 Current Status of JRA2

The main achievements of JRA2 to date are:

- GÉANT2 security policy: the security policy of the GÉANT2 backbone (also affecting GÉANT2 partners involved in providing services to GÉANT2).
- “The Toolset”: A set of tools (hardware and software) relevant for the operation of the security teams within the GÉANT2. It is ready for deployment beyond the participants of JRA2.
- GÉANT2 security recommendations: the expectations (operational standards) towards the security teams of GÉANT2 partners.

JRA2 provides the tools and policies for security operations of GÉANT2. The main contributors to those achievements were the twelve partners formally participating in JRA2. The remainder of GÉANT2 was largely not involved, but adherence to the security recommendations by all partners is crucial for secure operations of GÉANT2.

1.4 Success Factors of JRA2

In short, the ultimate goal of JRA2 is to make the GÉANT2 community as secure as required. The means to reach this goal is adherence to the security standards established for that purpose. The term “Transition into Production Service” - as it appears in the title of this document – is in the context of JRA2 to be understood as the process of establishing, implementing and enforcing those security standards within the GÉANT2 community.

The law of the weakest link in a chain applies to security, where a partner below standard poses a potentially unacceptable risk to the other partners. The way JRA2 wants to achieve an acceptable level of security is by ensuring that all partners adhere to an agreed-upon security baseline. This includes the availability of appropriately trained security staff in all partner organisations; they need to be appropriately supported by tools, interconnected with a co-ordination infrastructure and must know the expectations from the GÉANT2 partners towards the GÉANT2 community. JRA2 may consider itself successful, when all GÉANT2 partners meet this security baseline.

Another important aspect is sustainability: to ensure an appropriate level of security on the longer run, new security measures, which might become relevant only later, must be identified, developed and piloted for potential future use on a larger scale. This activity does not require the engagement of all GÉANT2 partners and is currently addressed by JRA2. JRA2 may consider itself successful, if “The Toolset” remains relevant for the partners of GÉANT2 to meet the security baseline.

Operating centrally managed services may be found useful as a means to help reaching the ultimate goal, but they are neither an obvious requirement nor a goal in itself.

The remainder of this document is addressing the issue of implementing the security baseline. The further development of “The Toolset” remains a research activity and is not addressed in this document.

2 Process of Transition

2.1 (Main) Stages of Transition

The main stages of transition will be in this sequence: the agreement on the GN2 security service specification (DJ2.3.2), the GN2 service roadmap (MJ2.3.3) and – overlapping with the previous stage - its implementation.

2.1.1 Stage 1: GN2 Security Service Specification

The GN2 security service specification (DJ2.3.2, planned for Month 26) will be derived from the security recommendations contained in DJ2.3.1,1. This service specification will set the security baseline for all GÉANT2 partners and may require additional interactions with the GÉANT2 policy bodies.

2.1.2 Stage 2: GN2 Service Roadmap

Based on the GN2 security service specification, all GÉANT2 partners will be contacted to come up with a list of actions and a roadmap on a per partner basis to meet the GÉANT2 security baseline. The planned date for this milestone (MJ2.3.3) is Month 32.

To prepare for the next stage, training material for “The Toolset” will be developed in this stage.

2.1.3 Stage 3: GN2 Service Roadmap Implementation

The implementation of the service roadmap will take place on a partner per partner basis and will start once Stage 2 provided a list of actions and a roadmap for that partner. It will – for many partners - extend into Year 4 of GÉANT2.

2.2 Conduct and Sequence of Transition

The stages will follow one another in the sequence above, with Stage 3 overlapping with Stage 2. Timing information is contained in the GANTT chart below.

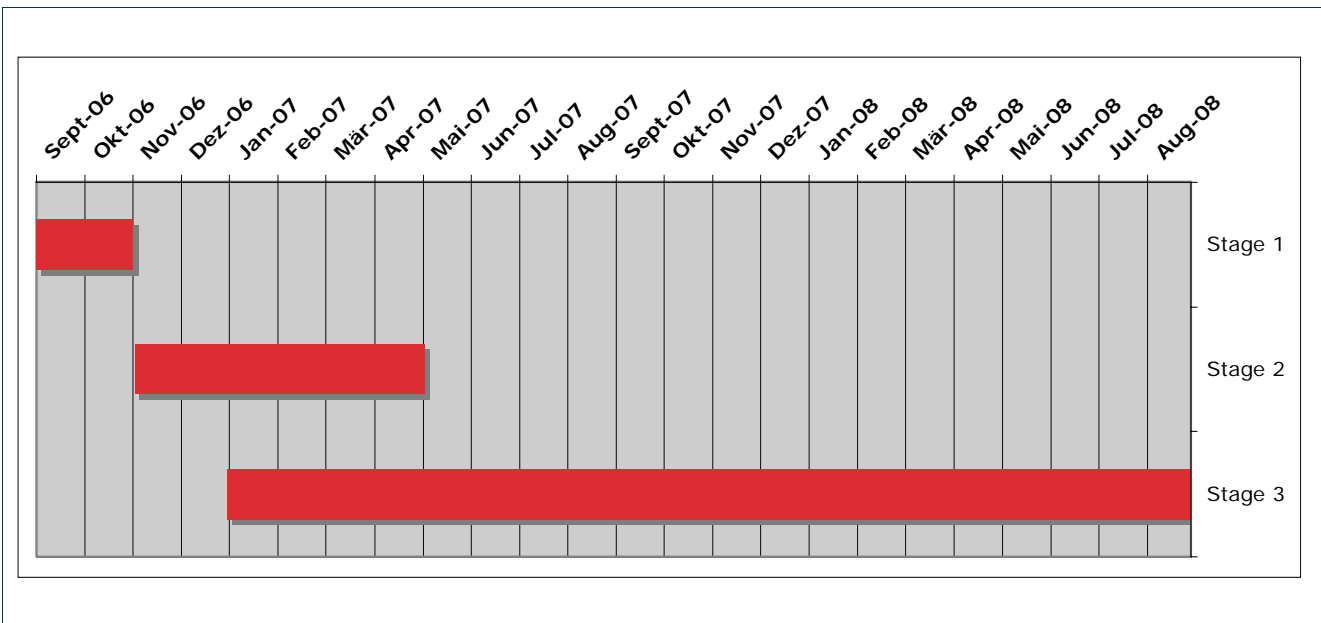


Figure 2.1: GANTT chart of security service deployment

2.3 Development and Deployment of NFSEN Software

The NFSEN software is written and maintained by SWITCH with contributions from users. It is published as open source project on sourceforge.net under a BSD-style license (see [NFSEN]). All the customary features such as bug reporting, support requests, patches and feature requests are supported on this platform.

2.3.1 Release Management

Releases are grouped into two categories:

- Stable releases: Usually about two releases per year. Regular users are expected to install those releases and keep their installation up to date.
- Snapshot releases: Testing releases on a more frequent basis. This category is targeting advanced users and contributors to the development only.

2.3.2 Support and Maintenance

As it is customary with open source projects, the main support is provided by a mailing list populated with the developers and users of NFSEN. This form of support is well suited for experienced system administrators, which matches well with the expected level of expertise of CERT staff. SWITCH is dedicated to provide support over this channel on a best effort basis and is prepared to offer GÉANT2 users priority over other requests for support.

2.4 Development and Deployment of FlowMon Probe

The FlowMon probe is a development project of CESNET. Release management, support and maintenance are as of writing this report performed by the developers themselves. CESNET is at the time of writing studying options for professionalizing release management, support and maintenance.

2.5 Possible Main Issues

2.5.1 Issue 1: Support and Maintenance for the FlowMon Probe

The current state, where the core developers of the FlowMon probe provide release management, support and maintenance is not satisfying in the longer run. In particular, it does not scale well and does not offer the required sustainability.

CESNET is currently studying options to offer sustained and professionalized release management, support and maintenance. CESNET envisages transferring these tasks to a new legal entity. This raises IPR issues, which need be addressed by appropriate processes at project level. CESNET is committed to continue to develop and support the FlowMon probe further and will present their options shortly.

2.5.2 Issue 2: From Recommendations to Policies

The efforts of JRA2 yielded security recommendations for all partners of GÉANT2. They are contained in Deliverable DJ2.3.1,1 (Report on Pilot Phase 1 and Recommendations). At this stage, the recommendations therein represent the opinion of those partners participating in JRA2. Efforts need be undertaken to gain managerial support for those recommendations at large.

Deliverable DJ2.3.2 (GN2 Security Service Specification) will be based on the recommendations in DJ2.3.1,1 (Report on Pilot Phase 1 and Recommendations). This deliverable will be brought to the attention of the policy bodies as a deliverable affecting all partners and setting the security baseline for the whole GÉANT2 community. It will allow those bodies to decide on “how much security” is required for the GÉANT2 community.

2.5.3 Issue 3: Training Material Delivery and Maintenance

In Stage 2, training material for “The Toolset” will be developed. The first workshop delivering this material will be organised by GÉANT2. It will be studied whether the training material will in the future be delivered on its own or whether and at which stage it should be integrated into existing training events relevant to the CERT community.

An interesting candidate to deliver and also to maintain our training material in the longer run is TRANSITS (See [TRANSITS]). TRANSITS workshops are the de-facto standard for training courses of new CERT staff. TRANSITS trainings are delivered by senior CERT staff and fit very well the CERT environment as per chapter 1.1. The training material of TRANSITS can also be used to deliver additional courses, e.g. it allows GÉANT2 partners to train the security teams within their own constituency.

JRA2 will study the option to integrate the course material being developed in WI3 in Year 3 into the TRANSITS course material and expects the following benefits:

- “The Toolset” is already a de-facto standard for GÉANT2 partners will get additional visibility outside of GÉANT2.
- The maintenance of the training material is organised within TRANSITS.

JRA2 is prepared to find other options, if an acceptable solution with the entities managing the continuation of TRANSITS cannot be arranged for.

3 Resources

3.1 In the Transition Process itself

All partners need to assess the resource requirements individually. JRA2 staff (WI-3 of JRA2) will support all partners assessing the gap between the security expectations and their respective capabilities. This support is covered in the efforts of WI-3. It amounts to 13MM in Year 3 and includes the preparation and delivery of training material. The efforts in Year 4 will be based on the results of the GN2 service roadmap (MJ2.3.3). The following partners are contributing to WI-3 in Year 3: DANTE, FCCN, GARR, GRNET, HUNGARNET, ISTF, IUCC, REDIRIS and SWITCH.

3.2 Estimated to Operate the Service

While the transition process is part of JRA2 as explained above, operating security teams and maintaining the security baseline should be covered by the regular operational budget of each partner. Therefore, operating the security service does not require centralised funding.

However, proposals may be put forward at some point in the future for centrally provided or co-ordinated service offerings to support our partners' security teams. Such services would produce operational cost and appropriate sources of funding need be secured. Currently, GEANT2/JRA2 have no plans for such services.

Project:	GN2
Deliverable Number:	DJ2.0.1
Date of Issue:	01/05/07
EC Contract No.:	511082
Document Code:	GN2-06-253v4

4 Conclusions

The goal of JRA2 is to define and maintain the security expectations towards all GÉANT2 partners and help the partners in getting ready to live up to those expectations. The transition process covers all efforts in reaching that state. The transition should be finished during the lifetime of GÉANT2. Once established, the partners are expected to keep up with the security level and its revisions over time.

5 References

- [NERD] http://beveiliging.surfnet.nl/info/artikel_content.jsp?objectnumber=33426
- [NFSEN] <http://nfsen.sourceforge.net/>
- [TRANSITS] An EU funded project to promote the establishment of Computer Security Incident Response Teams (CSIRTs) and the enhancement of existing CSIRTs. Since the project ended in September 2005, TERENA and FIRST have joined forces to organise further training workshops across Europe and beyond based on the materials developed by TRANSITS, with the help of financial support from various organisations: <http://www.terena.nl/activities/transits/> and <http://www.first.org/transits/>
- [FIRST] <http://www.first.org/>
- [TF-CSIRT] <http://www.terena.nl/activities/tf-csirt/>
- [TI] <http://www.trusted-introducer.nl/>

6 Acronyms

CSIRT	Computer Security Incident Response Teams
FIRST	Forum of Incident Response and Security Teams
JRA	Joint Research Activity
TRANSITS	Training of Network Security Incident Teams Staff
TF-CSIRT	Task Force on Collaboration of Security Incident Response Teams
TI	Trusted Introducer