

26.07.06

# Deliverable DJ2.3.1,1: Report on JRA2 Pilot Phase One and Recommendations



## Deliverable DJ2.3.1,1

Contractual Date:	30/11/2005
Actual Date:	26/07/06
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	GN2-06-150v3

**Authors:** Claudio Allocchio (GARR)

## Abstract

To increase Security of the GÉANT2 backbone we must ensure that appropriate actions are taken both to detect and to remove threats wherever they appear, including not only the GÉANT2 backbone, but also the networks connected to it (NRENs) as well as the networks of the local institutions connected to the NRENs at campus/site level. Hence, a global coordination is needed among all parties: at international, GN2, national, and local level. A pilot coordination service has been set up and experience has been gained to define best common practices in incident handling; a trusted environment among the JRA2/WI3 pilot project teams has been set up as well, and a set of requirements on how to include new teams into the trusted club has been produced. The initial ideas on the requirements and incident handling tools have been verified against daily operations, thus refining priorities and the actual needs of the security teams. Also, an environment to introduce the new tools created by WI2 has been prepared.

# Table of Contents

0	Executive Summary	iv
1	Security Operations Scenario	1
1.1	NREN National Security Operations	2
1.2	GN2 International Security Operations	4
1.3	At Large International Security Operations	4
2	Pilot Phase 1	5
2.1	Establish trusted communication channels	6
2.2	Establish security incidents level classification	6
2.3	Define default incidents response time	7
2.4	Define information handling procedures	7
2.5	Create coordination procedures with network/LAN operation	7
2.6	Create an alert distribution service	7
2.7	Deploy an automated incident handling service	8
2.8	Create a common trouble ticket system	8
2.9	Give recommendation to tools developers	9
2.10	Define a policy on IPR related incidents	9
3	Proposed Continuation	10
3.1	Service Activities	10
3.1.1	MUST	11
3.1.2	SHOULD	11
3.1.3	MAY	12
3.1.4	Service Activity Building Blocks Architecture	12
3.2	Advanced activities	13
3.3	Further suggested development	14
4	Conclusions	15
5	References	16

Appendix A	Pilot Teams PGP keys .....	17
A.1	GARR.....	17
A.2	IUCC .....	17
A.3	RENATER.....	25
A.4	NIIF/HUNGARNET .....	25
A.5	DANTE.....	25
A.6	GRNET .....	26
A.7	RedIRIS .....	26
A.8	SURFnet .....	26
A.9	SWITCH.....	26
A.10	FCCN .....	26
A.11	ISTF.....	26
Appendix B	Incident Severity Classification and Default Incident Response Time.....	27
B.1	GARR.....	29
B.2	IUCC .....	29
B.3	RENATER.....	29
B.4	NIIF/HUNGARNET .....	30
B.5	DANTE.....	30
B.6	GRNET .....	30
B.7	RedIRIS .....	32
B.8	SURFnet .....	33
B.9	SWITCH.....	33
B.10	FCCN .....	34
B.11	ISTF.....	34
Appendix C	Used Trouble Ticket Systems TTS .....	36
C.1	GARR.....	36
C.2	IUCC .....	36
C.3	RENATER.....	36
C.4	NIIF/HUNGARNET .....	36
C.5	DANTE.....	36
C.6	GRNET .....	37
C.7	RedIRIS .....	37
C.8	SURFnet .....	37
C.9	SWITCH.....	37
C.10	FCCN .....	37
C.11	ISTF .....	37

## Table of Figures

- Figure 1.1:** Security Operations Hierarchy in GN2 and beyond 2
- Figure 3.1:** Proposed building block architecture for a Security Service and Joint Research activity 13

Project:	GN2
Deliverable Number:	DJ2.3.1,1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

## 0 Executive Summary

A backbone is secure only if all networks accessing it are secure. Therefore, to ensure security of the GÉANT2 backbone we must ensure security in all NRENs connected and in all the networks of the local institutions connected to the NRENs at campus/site level. Appropriate actions must be taken both to detect and to remove threats wherever they appear; hence a global coordination is needed among all parties: at international, GN2, national, and local level. A pilot coordination service has been set up, and experience has been gained to define best common practices in incident handling; a trusted environment among the JRA2/WI3 pilot project teams has been set up as well, and a set of requirements on how to include new teams into the trusted club has been produced. Initial ideas on the requirements and incident handling tools have been verified against daily operations, thus refining priorities and the actual needs of the security teams. Also, an environment to introduce the new tools created by WI2 has been prepared.

Project:	GN2
Deliverable Number:	DJ2.3.1,1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

# 1 Security Operations Scenario

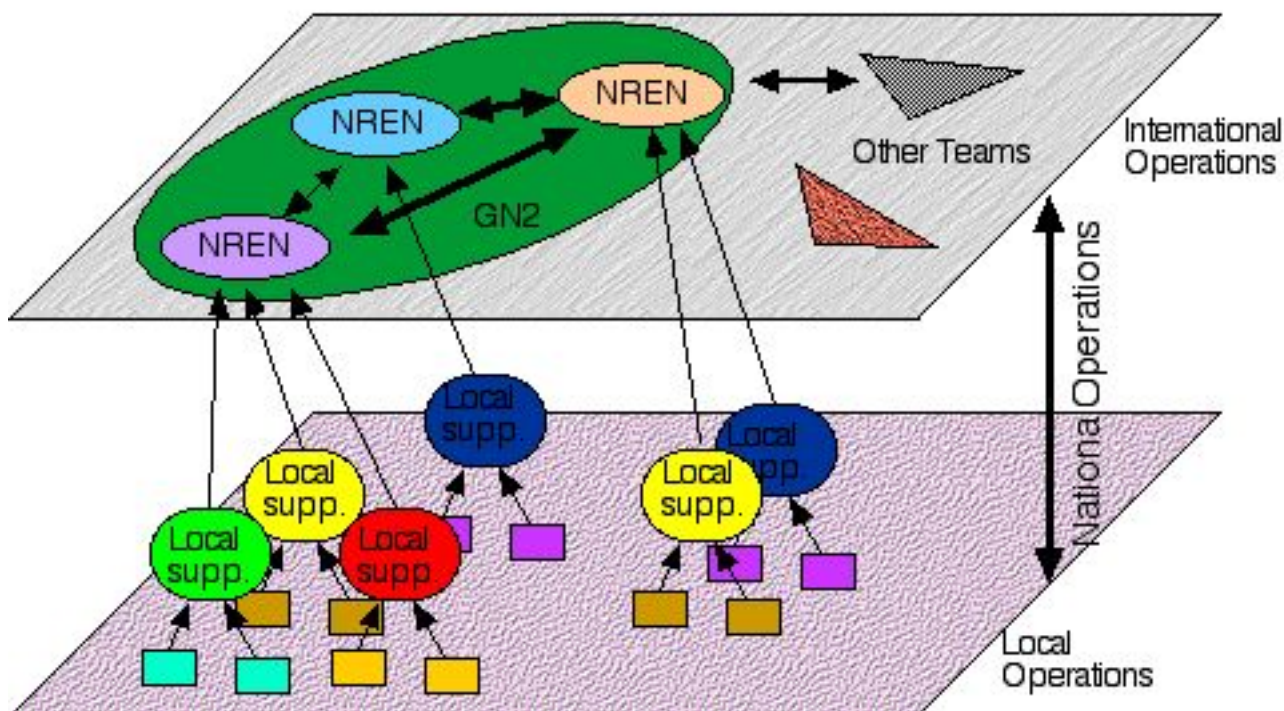
The security of a backbone depends heavily on the security of the networks connected to it, and this fundamental concept shall be extended further, down to the single computers and networked objects that can reach the backbone. As a consequence, making the backbone secure includes a large number of people, 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 centralized service.

This GÉANT2 security scenario is, however, even more complex. In fact, there is not a homogeneous situation among the different NRENS accessing the GN2 backbone: there is a “security old core”, where well-established security teams operate at the NREN level, but also many countries, where NRENS’ Security Services are just starting to exist; and still others, where there is still no security team operating at all. This situation makes the overall GÉANT2 security a tricky process to supervise: e.g. in case a threat originates from an NREN in which there is nobody yet able to handle the problem locally, it becomes necessary to involve the GÉANT2 Network Operation Centre and the GN2 security contact to be established (e.g. the former DAN-CERT) in the process too. That is why it is important to bring up to speed those NRENS that are still lacking an internal security service, in addition to the need to establish the horizontal coordination among the existing NRENS’ security teams. The goal of JRA2 Work Item 3 is to fulfil both of these needs. In the first part of the Pilot Project we have addressed the “horizontal coordination problems”, while in the proposed continuation of the activity we will additionally initiate actions to help setting up security operations in NRENS where they are still missing.

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:	DJ2.3.1,1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3



**Figure 1.1:** Security Operations Hierarchy in GN2 and beyond

## 1.1 NREN National Security Operations

The NREN Security Team usually coordinates security operations at the NREN level. The team is responsible for handling incidents, which originate from or affect users, machines, and/or services, connected to the NREN itself. The security team typically performs the following tasks:

- receives incident notification by the downstream connected institutions and users;
- receives incident notification by external sources (both other NRENs and non-NRENs);
- maintains a trouble ticket system, which keeps information on incidents in their corresponding or assigned states;
- in case an incident originates from one of the downstream connected institution/sites, the security team interacts with the security or network manager of the institution/site in question, providing information and advice on how to solve the incident; the handling procedure is often described in a formal document, which also gives information about incident severity classification, required response time and actions, escalation procedures, and actions in case the incident is not handled correctly locally;
- interacts with the NREN's Network Operation Centre (NOC) in case filtering on the backbone and/or on the local access links is required to block an incident, until it is solved at the originating site;
- in case the incident originates from another NREN or any other external organisation, the security team initiates contact with the appropriate peer security team, in order to have them start internally their own incident handling ticket(s) and procedures.

Some security teams also provide additional services to their NREN community, such as Security Alerts and proactive security network monitoring [CERT.ORG].

The following GN2 partner NRENS have a security team in operation:

- ACOnet, Austria (\*)
- BELNET, Belgium (\*)
- CARNet, Croatia (\*)
- CyNet, Cyprus
- CESNET, Czech Republic
- UNI-C, Denmark (\*)
- Funet, Finland (\*) (+)
- RENATER, France (\*)
- DFN, Germany (\*)
- GRNET, Greece (\*)
- NIIF/HUNGARNET, Hungary
- RHnet, Iceland (+)
- HEAnet, Ireland
- IUCC, Israel
- GARR, Italy (\*)
- LITNET, Lithuania (\*)
- SURFnet, The Netherlands (\*)
- UNINETT, Norway (\*) (+)
- PSNC, Poland
- FCCN, Portugal (\*)
- ARNES, Slovenia (\*)
- RedIRIS, Spain (\*)
- SUNET, Sweden (\*) (+)
- SWITCH, Switzerland (\*)
- UKERNA, United Kingdom (\*)

(\*) the team has fully documented its constituency and operations, and has been accredited via the Trusted Introducer procedures [TI]

(+) connectivity to GN2 backbone is via NORDUnet

All remaining NRENS do not have an operating Security Team.

- ISTF, Bulgaria
- JSCC; Russia
- LATNET, Latvia
- RESTENA, Luxembourg
- RoEduNet, Romania
- SANET, Slovakia
- ULAKBIM, Turkey
- University of Malta, Malta

Security operations at national level are not coordinated by JRA2 WI3 activity. Nevertheless, information exchange among teams is also aimed. This is expected not only to improve the overall results, but also, in future phases, to help establish reliable security operations where they are still not (well) maintained.

## 1.2 GN2 International Security Operations

While national security operations follow a vertical hierarchy, international operations are normally based on peer or multiple partners' coordination actions, which itself depend on the involved parties in each specific incident. Main goal of JRA2 WI3 is to explore the best options to enhance these operations, in accordance with the actual requirements of the involved teams. In the phase 1 of the Pilot Coordination Service the following partners were involved:

- GARR
- DANTE
- FCCN
- GRNET
- NIIF/HUNGARNET
- ISTF
- IUCC
- RedIRIS
- RENATER
- SURFnet
- SWITCH

In the follow up of the GN2 JRA2 activity, the list of participating NRENs shall be enlarged, and the final goal is the inclusion of all GN2 project partners, creating a specific "service type" activity.

## 1.3 At Large International Security Operations

Beyond the GN2 backbone and connected partners, we shall not forget the other similar R&E organisations and NRENs which peer with it, like Internet2 [I2] and CANARIE [CANARIE] in North America, CLARA [CLARA] in South America, the ones from Asia-Pacific region, etc. Coordination and liaison between GN2 JRA2 and these international partners is yet another abstract level which is needed, as GN2 partners and users work closely with them, too.

Last, but not the least, "the rest of the world" is also heavily affecting security operations inside GN2, being often a major source of security threats and offences. Liaisons with external entities dealing with security, when identified and active, is another action that helps in securing better GN2 and all its NRENs and users.

## 2 Pilot Phase 1

The main goal of JRA2 WI3 is to establish a framework where security operations can be done efficiently, quickly and effectively among GN2 partners. In order to obtain this result, both a human and technical network shall be established, where involved elements are trained/prepared for their role, and are thus able to interact with the other elements in the best possible way. We cannot know in advance how and when serious security attacks may appear towards or within GN2 and its partners; the important fact is to be ready to react, stopping the problem, and even better – to be proactive – preventing the problem from happening at all. The coordination procedures, the tools, and the human relationships shall be there in place, tuned and tested, in order to achieve success.

JRA2 thus started with the Phase 1 of the Pilot coordination, where participating teams have experimented with the proposed activities to enhance coordination efficiency in international incident handling.

The list of possible items was drafted at the beginning of the Pilot Phase 1 as follows:

- establish trusted communication channels between CSIRTs by exchanging electronic credentials (secure communications);
- establish security incident level agreed classification (severity level);
- define a default response time, depending on severity level;
- define information handling procedures, covering the information exchange within the GN2 community as well as with liaisons outside GN2;
- create coordination procedures with network operation teams and LAN management teams, defining responsibilities and actions;
- create an alert announcement mailing list including CSIRT people;
- deploy automated incident alarm systems and information exchange (IODEF and similar), built upon the results of eCSIRT.net project [eCSIRT] and similar activities (SMS out of band...);
- establish a common trouble ticket system;
- give recommendations to service developers from the user's perspective;
- agree/disagree on how to handle IPR related incidents.

Each of these topics is described in details in the following sections.

Project:	GN2
Deliverable Number:	DJ2.3.1,1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

## 2.1 Establish trusted communication channels

The participants in the Pilot phase were normally communicating among themselves either using e-mail messages or, for more urgent or complex cases, directly via telephone calls. Most of them, indeed, know each other personally, and the personal “web-of-trust” is the building block of this action. However, mainly because this practice is not technically “trusted” and cannot scale up even if limited inside the GN2 participants, it was decided to adopt PGP (Pretty Good Privacy) public/private keys, in order to enable truly “trusted” communications. The PGP model, in fact, adapts very well to the trust relationship existing among security teams, and can scale up easily to the side of GN2 participating security teams. Moreover, PGP can also serve as an encryption method, when there is a need to exchange sensitive data among teams. This allows for thoroughly protected communications, where both secrecy and integrity and authenticity of the information exchanged are guaranteed.

The public PGP keys and optionally also the X.509 certificates of the teams and individual team members participating in the Pilot were collected. The teams were encouraged as well to publish the PGP keys to the available PGP Key Servers. A list of the collected keys/certificates and/or locations, from which they could be obtained, is also included in Appendix A.

In order to strengthen the PGP web-of-trust, a JRA2 PGP Key Signing party is foreseen to be held at one of the upcoming JRA2 meetings.

The use of PGP is also recommended for the continuation of the Pilot (phase II) and as a requirement for new GN2 security teams (including the step of uploading the keys to a PGP key server).

## 2.2 Establish security incidents level classification

Classifying an incident is a first step needed to decide on actions and priorities in order to handle it. A survey in this area has been conducted among the Pilot participating teams. It was determined that not all teams have their own written document to classify incidents, and many of them rely mainly on well-established common practice for this activity. A table reporting the most common classification and a list of answers to the survey is available in Appendix B.

As a common ground, all the Pilot participants agreed on the classification that was prepared by eCSIRT.net project, which thus became a “reference” classification. The Pilot participants agreed as well that the eCSIRT.net classification is also to be suggested as a base for the incoming participating members to the security community of GN2. Further revisions of the classification will however be needed periodically, as already mentioned by those teams which have not adopted a written classification, in order to be more flexible.

## 2.3 Define default incidents response time

Alongside classifying incidents, defining a default response time is needed for an efficient incident handling that involves a number of teams. A survey has been conducted among the Pilot participating teams, and once again, it was determined that not all teams have a written document in place to define incident response time, and many of them rely mainly on well established common practice for this activity. A list of answers to the survey is also available in Appendix B.

## 2.4 Define information handling procedures

Security Incident handling and interaction between teams (both at national and international level) requires a set of well-established procedures. At the NREN level, many teams already have such well-established procedures in place to handle incidents as well as a trouble ticket system and/or an incident database. The establishment of an international information handling procedure has been examined and discussed. The Pilot team concluded that, given the limited existing number of incidents, which involve two or more NREN, teams, creating formal procedures to define in details how teams would behave is probably premature. It was agreed that the use of PGP signed/encrypted e-mail with a copy to all interested international teams (for example GN2 NOC and GN2 security contact to be established (e.g. the former DAN-CERT)) is enough, and will scale well when the service is also brought to all GN2 partners.

## 2.5 Create coordination procedures with network/LAN operation

As per incident handling procedures, the number of incidents requiring intervention of the GN2 NOC is low enough that the use of PGP signed/encrypted e-mail is sufficient and will scale to the whole of GN2.

## 2.6 Create an alert distribution service

Distributing Security Alert Warnings is an action, which is normally classified as proactive security. A survey among teams has shown that only few of them perform proactive security actions, mainly due to problems of understaffing. And even in these cases, the alert warnings are often sent out in the national language, thus creating a problem in their reusability at the international level.

Given the missing “feeding source” for the alert distribution service, the Pilot participating teams have dropped this action, suggesting a more global GN2 service instead. In particular, the eventual GN2 Alert Service should not be a replica of the general Security Alerts, normally available at NREN level, but instead focus on specific GN2 alerts only, mainly drawn from the results of proactive tools (from WI2), which can pinpoint GN2 specific anomalies or suspect activities.

On the other hand, The Trusted Introducer for CSIRT in Europe, an initiative to improve the "web-of-trust" between CSIRT in Europe, provides to the accredited teams special services that should be taken into account in the context of JRA2 WI3. These special services include in-band alerting using e-mail and the crypto mail gateway and out-of-band alerting using voicemail and SMS.

## 2.7 Deploy an automated incident handling service

The final goal to study the possible deployment of an automated incident handling service is one of the most important items in JRA2 WI3. This is also the core study inside many NREN teams; indeed none of the Pilot participants currently employs any kind of automated incident handling at national level. All of them use tools to facilitate incident handling, like databases, trouble ticket systems, helper applications; and some also tested the new tools made available by JRA2 WI2. However, incidents are still handled manually, mainly to control the resulting actions and avoid the risk of false-positives or over-acting decisions. An additional element, which has shown up clearly, is the need for interaction between the Security Teams, the NRENs NOC, and the local network or system administrator (or even the end-user). These management domains are still not ready for any automated action happening within them if the initial cause originates from another domain. Eventually, administrative domain boundaries prevent automated actions as well, already at national level, and even more at international one.

The Pilot teams thus concluded that the international automated incident handling service is premature at the moment. It is however suggested to introduce semi-automated handling tools between international teams if and when the number of incidents handled internationally will rise beyond the current manual handling on multilateral and bilateral teams.

## 2.8 Create a common trouble ticket system

Most of the Pilot participating teams use a Trouble Ticket System in order to control the status of their incidents. However, there is not a commonly used TTS platform, and the tickets' descriptions/keywords are often stored in the national language. In the Pilot phase it was agreed that each team should therefore send its own ticket in its own format, but in English language, to all the other teams involved. The other teams will then just re-enter the ticket in their own TTS, sending back the newly generated ticket number. All communications will keep note of all the ticket numbers generated by all involved teams. Given the limited number of incidents, which involve international teams, and the even more limited number of incidents, which involve more than two parties, and also the fact that many teams have well-established procedures and systems to handle tickets, it was agreed not to set up a common TTS. Translation tools from one ticket system to another will be investigated during the continuation of JRA2 WI3 as a possible helper application. A list of TTSES currently in use by the Pilot teams is available in Appendix C.

## 2.9 Give recommendation to tools developers

Most of the tools developed by JRA2 WI2 were aimed for proactive security, and not all the Pilot teams perform proactive security. Thus, during the Pilot stage there was a limited testing of these tools, and only by some of the teams. However, important feedback and suggestions came from all of the Pilot teams, which experimented with them. For a detailed list of tools and test results, see DJ2.2.1,1 deliverable.

A fundamental general recommendation was made regarding ease of installation and use: the existing security teams have consolidated internal tools and procedures in place for their daily work; therefore integrating a new tool into the environment requires compatibility or at least the availability of an easy set of Application Programming Interfaces (APIs). Also, portability, and hence ease of installation inside different environments, is a fundamental MUST for a tool to reach success.

## 2.10 Define a policy on IPR related incidents

Intellectual Property Rights related incidents go beyond the simple security handling, and have legal and philosophical implications, which are different in each country. Moreover, among the Pilot teams there is no common policy even about the fact that these incidents are to be handled by NREN security teams at all, given the debate about “handling content” of communications inside an NREN or internationally. For this reason it was agreed to drop this item.

### 3 Proposed Continuation

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

Another important result from the Pilot Phase 1 is the quite strong distinction, which should be made between activities useful in “production”. Security Operations and experimental or pure research activities, which might become useful in the future, but are not yet ready for the real life. We thus propose a structuring which is divided into a “Service Activity”, including the basic activities required to create a GN2 safe operational environment, and “Advanced Activities”, which should continue the research part of the JRA2 Security Activity.

#### 3.1 Service Activities

The basic activities for the NREN Security Teams are listed into categories. A formal definition of MUST, SHOULD, and MAY is also described in RFC2119 [RFC2119].

- “MUST” category lists activities which are essential and strictly compulsory for the teams participating in the GN2 Security Operations;
- “SHOULD” category lists activities which are strongly recommended to the teams due to their usefulness; participation in the GN2 Security Operations is however possible even if not all of these activities are performed;
- “MAY” category lists activities, which are truly optional; they are regarded as useful add-ons that do not influence negatively the GN2 Security Operations if not performed.

The proposed list of MUST, SHOULD, and MAY activities for continuation and the generation of a Service Activity is listed below.

Project:	GN2
Deliverable Number:	DJ2.3.1,1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

### 3.1.1 MUST

A Security Team MUST be “accredited” inside the community. The Trusted Introducer is a well-established service, which 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.

A Security Team MUST provide its team AND/OR members PGP Public Keys to the other teams. The keys MUST be available via one of the PGP Public Key Servers.

A Security Team MUST acknowledge incoming requests generated by other Security or Network Operation teams within a reasonable timeframe. The acknowledgement MUST be sent also if the team itself cannot handle the incident. If the Security Team contacted will handle the Incident, a Trouble Ticket OR a Unique Incident Identifier MUST be included in the acknowledgement. In any case, incoming Trouble Tickets OR Unique Incident Identifiers MUST be preserved in the acknowledgement and all subsequent communications.

In case some unexpected relevant information is discovered during incident handling, affecting the domain of the team, which signalled the incident, the security team MUST inform the external team.

A Security Team MUST send the “incident closure” information to the team(s) which sent the original Incident handling request.

If the information exchange among Security Teams handling an incident involves sensitive or personal data, the communication between teams MUST be non-disclosable, e.g. using encryption or other content protection methods.

All incident information MUST be considered confidential and must not be disclosed beyond the scope defined by the information source.

### 3.1.2 SHOULD

A Security Team SHOULD document its Best Common Practices (BCP) and make these available to the other teams.

A Security team SHOULD make publicly available its Communication and Authentication Policy for the keys and certificates it uses.

In the acknowledgment to an incoming incident handling request, a team SHOULD state its own severity classification for the incident and the default handling time for the incident itself. If the incident is a known incident, it SHOULD point to available documents describing this information as well.

A Security Team SHOULD inform the team which signalled the incident about the progress of the incident handling if this influences the expected incident closing time significantly.

Project:	GN2
Deliverable Number:	DJ2.3.1,1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

A Trouble Ticket system, or a similar tool, SHOULD be used by Security Teams to keep track of incident handling.

A Security Team SHOULD sign with PGP keys any e-mail message, which it sends out. The PGP keys of each team or team member SHOULD be counter-signed by other teams. New Security team members SHOULD participate in an appropriate Key Signing Party at least once.

### 3.1.3 MAY

A Security Team MAY inform the team which signalled the incident about the progress in solving the incident itself AND/OR the internal escalation procedures which is being adopted.

In case an incident cannot be handled directed by a Security Team, the latter MAY redirect the signalling team to another appropriate team.

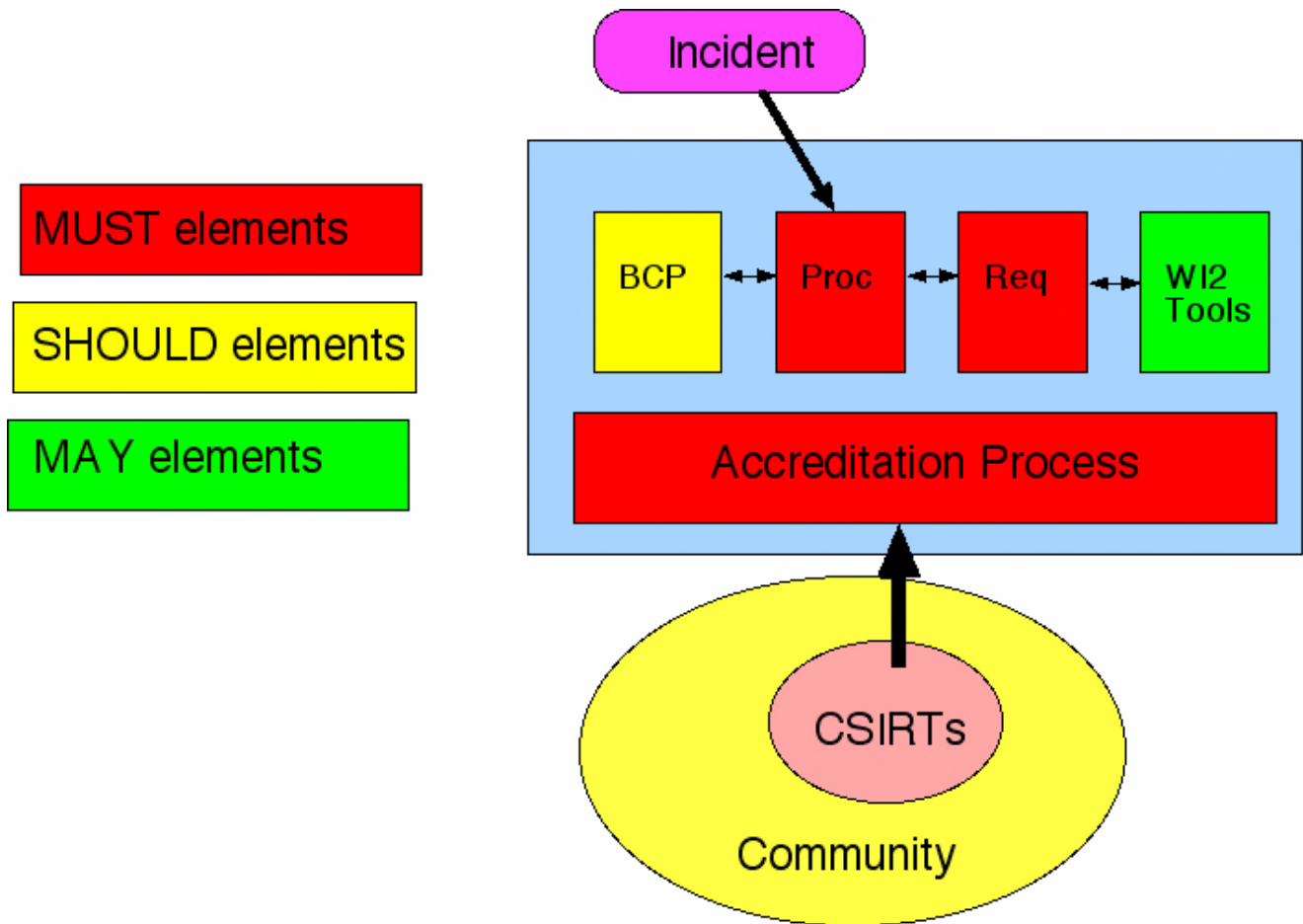
Whenever available, security tools MAY be installed and used to enhance incident handling operations or create proactive security functions.

A security Team MAY include automated information (like IODEF formatted information) in the reports exchanged with the other teams.

### 3.1.4 Service Activity Building Blocks Architecture

During the Pilot Phase 1 it became evident that a monolithic approach to security services and research cannot be done. We need to provide a “building blocks” architecture that easily allows elements to be added, 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 fulfilment. Addition of optional blocks enhances the status of the participating team and the global security of GN2, but is not a (strict) requirement.



**Figure 3.1:** Proposed 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

### 3.2 Advanced activities

In Pilot Phase 1, a number of advanced activities have been prototyped; others need more testing. In particular, activities like automated warning systems based on traffic data, existing honeypots, etc should be installed and tested further, before they can be used in an operational environment.

Some experiments on automated operations, based on incident handling, should be performed. Procedures, which can automatically establish/remove counter-measures for some kind of incidents, may be implemented in a controlled testbed environment. It is also likely that interaction with some networking equipment manufacturer, in order to support this kind of automated handling, will prove necessary. Integration with

automated alarm systems should also be prototyped inside these testbeds. A first list of possible advanced activities includes:

- NetFlow based automated anomalies detection;
- automated XML incident data exchange tools (IODEF or similar);
- automated counter measure tools to handle equipment;
- collection and analysis of binaries found in the wild in the incident and response world (malware gathering and analysis);
- compromised system detection by security event correlation;
- experimenting “unwanted traffic” automated removal techniques.

A number of Security Teams should dedicate advanced research resources to the above activities.

### 3.3 Further suggested development

In order to expand the Pilot test, the current list of Pilot partners should be enlarged, including at least two or three new ones. This action will also test the procedures needed to “bring into the Security Team Service” new teams, which is a fundamental operational activity when expanding Security Operations to a GN2 Service Activity. Bringing new teams on board means not only accreditation, checking of existing compatible procedures, or pointing out initiatives to help them start (for example the TERENA CSIRT Starter Kit initiative [STARTKIT]): it normally involves also training. The TRANSIT [TRANSIT] project, and now its continuation in collaboration with FIRST [FIRST] and ENISA [ENISA], produced a relevant set of training modules and a relevant experience in setting up courses and hands-on laboratories. It is probably needed to add some GN2-specific modules to the existing training material and experiment the training in setting up new security teams in those NRENS, connected to GN2, that still do not have such in place. Using the experience provided by TF-CSIRT can prove very helpful in this activity too.

The toolset produced by JRA2 WI2 should also be brought into the coordination infrastructure, with the well-tested and stable components pushed towards the production environment.

## 4 Conclusions

The Pilot Phase 1 in WI3 activities have explored the feasibility and experimented with the use of a significant number of existing and innovative procedures, actions, and policies within the Security coordination scenario inside GN2. Some of the items proved themselves useful, and we have defined them as viable building blocks, which must or should be included into a future Security Service Activity. Other items have been classified as ongoing research, which shall stay inside a JRA-like model. Eventually, some items may be entirely dropped from the activities, either because they did not prove their usefulness, or because there is no common perception about them and hence cannot be coordinated.

A path to extend a future SA to all GN2 partners, possibly as a requirement for GN2 membership including support for new incoming security teams, has also resulted from the Pilot Phase 1 of WI3.

## 5 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>[TRANSIT]</b>	<a href="http://www.ist-transit.org/">http://www.ist-transit.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>

## Appendix A Pilot Teams PGP keys

Here you can find the list of the PGP public keys of the Pilot teams. In case the keys are available and kept up to date on a WEB page, the URL is listed instead.

### A.1 GARR

<http://www.cert.garr.it/PGP/keys.php3>

### A.2 IUCC

NOTE: IUCC is in the process of publishing their PGP Keys on their WEB server. For the moment they are just listed here explicitly,

Yehavi Bourvine

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i
```

```
mQCNAzK1QyWAAEEAMnK/MTTHwNqyvLqr8LAJvW2uXeHNj6x3H55miymwqfiZ/hj
Ec00rFw96qHd8mq7E3fcB1EuJ0sk9Om0QU2IVdFHF/kP7F2LW/4zElcUd0U1h/Vz
Pn47PNN2B0rgTpJD7zIvsRd/0rDlHEtXj0JxjriARtZNdn+x3UzltDT9PhjJAAUR
tBc8eWVoYXZpQHZtscy5odWppLmFjLmlsPokAlQMFEDK1UtVF7olX4zT+YQEB1K4D
/Aiv4TD0VyHfksFjGZXXYt5X2NKi9AeuhTwJ0c5L7GZoGEvcqdTcGLOcMKs6TU1u
yRnmZP12D3Xy9jIsDT7TQLYM5kwkV0lBvdaGZTEj+JH++/mASoaJ7b98955svPL
kaps8n8DS1CzFhF1iUiRCeRseyu2wIREGGWZOKTjdh31iQCVAwUQMrVDMEzltDT9
PhjJAQF2LAP/dA+KAtm7srV2NlycOn79uNAdxD3yyJ1jbe3EC4r9cVf9Ct0LIGQm
794WY4NvLh6OhuIjlv2mkkolJCbwet0R9aGFPh3nYCMfq2j5s4hYztnQnxMKqRSZ
kGtxKso/hVkgPYWj8yH6BgAaWrguE14PrcngVyGkNFq9PRSy5AyD5niJAEYEEBEC
AAyFAjhDTbYACgkQVfe6KqApYZrWnwCgpZ6Kxkw0VkrnCTFpS5kIxuJvd5UAoIOw
Uu+rmLVZsn8edjNnyxuaFi+1
=xMR7
```

```
-----END PGP PUBLIC KEY BLOCK-----
```

Dani Arbel

Project:	GN2
Deliverable Number:	DJ2.3.1.1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: PGPfreeware 6.0.2i

```
mQGIBDtpanQRBACegwqTGFh6ftWX1EZ4/XyXmODXA3Lp2gUK1MwPY3sW1lrDv6H8
tu+0/CqsHcFKKZDOKcUwP8a2QUz+SahfIJ70P4g4CEA8BjU4GL35J8Bbiv9p+mN7
r5JMpP3Veu6fj12XSX+4nlERzxfutLVJqLCCNQzus46HAGtapdvVWFWHIwCgiw+a
RA1QuPxztkpUXV7FJFWq8r8D/jROKfMVuPYVPA/PozGRzOFNjgyt7tfxq+v3uv7s
SWE7At1aLB15wGJ2K01g89H7bd6x2Kk4ZP59/OmGEJ1ZA+yIodasXJ6ycLWmo8uU
YFZwXx36CCDJCQ9CmefRU8oRP0NIetk1N/Qijwy4KSBe7G8401LESjRrgoMRPAOY
cWtUA/43E7XsmHlpwE/dkb6Y7YdX+bXzDzJLsUqNvPB2TkfHPL1MuIToafnbgRssr
oQI+v2eE/NeNKj/nTQH/SVhceWerMdsHbj04PmRkZ6s/01WDaM44EaVbGrfVsx32
mHvqsssNQVVqnhyjf8hptrFuZP330epLzDaVYAIAISKVTxJBvKLQnRGFuaSBBcmJl
bCAobm9jKSA8ZGFuaUBub2MuaWxhbi5uZXQuaWw+iQBxBBMRAGAXBQI7aWp0BQsH
CgMEAxUDAgMWAgECF4AACgkQO+dFGMFQ740j9QCgg63Ej9sEM9VUQca5lI5IHarr
lyAn3y9d3m1A+4RUPQkGUmfqUuu9ABbuQENBDtpaoQQBADZLlFTkakteARFCpgl
Fh9dnIpBn/O51Lz+BzFgfU5SwpjVj+9o1YL1z0mnjtqjxJ5vBFx1zBh87KalhH/w
0kkFi+oK8KBbc7w/RWYy2+qkvsj44Eq6CjG/qVtJ+zxJj2hmDPNULBqg1JynwQMd
t0i9zfUrNbSLBfZD50sIUcCq0wADBQP+JHc0hXAB3PIE7OC1U3KKduhW7WoVz9ob
PHtQ/MURoof5vEJwJwzgfBnSUIkBLPZ3YHXjiTQ4uP2g//HWNpRi9NZhhTU4qf/O
qWI088YSAIT3iVvQS+IbfAecminHdgYUuJkDFxgHT2op+FBbVApGTaknoXaoVEzb
0s+ToXb3UXOJAEYEGBECAAYFAjtpaoQACgkQO+dFGMFQ74Pc3QCeK0i/kRGEHBvB
MStOY65NEFijrroAn2nJnzx+RdVAG7LLaFcI/Goi8BoG
=K0Uv
```

-----END PGP PUBLIC KEY BLOCK-----

### Hank Nussbacker

-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: PGPfreeware 6.0.2i

```
mQGIBDb1++oRBADzPAI10GsZnG0oXXXKqvG4J5dt+NVQxAIh4SMmGDjy0CLyFQ1/
Q+LM5jdEqiKjve4q5KPGtmdLcNC/R9vuSyQDYWXom0tDLt0ddIG2702nVuOWskzI
BckG3sTJopEjklQjh+Tn/ofTR/MAmR3u5cX7gwfDa2XW9/De3EEDfFRiYwCg/3H3
0aHM8WLuqGdIoPnN4iJVxB0D/izo8hlqLn3r8CNyDdodURLL0AtajSd8sxKPeCo0
SkGKHJjXoyPN9Nah5AEI+hFcdE7pKtO8vqiTRPFTW+RAzq+SUWSjzL656INqO5a
juwqSghgD2v+Gp2eQ27F19LkE8TdHnun/VvGZs4geXO8pMfKpCNhe83A3QmY6A/+
18/2A/9ERJv78DH0QCRO74RLVdkwCrUdDEMlnDUMcpAxvasqOzIxOyiDS/p0KkZk
4APwWBgRCAIzB7ePp56YjixZsFfdCWuni/qZ5eiiZ/crDdtrb/FYmmD5qG6dz1BP
BEg50dKNXQ55Cu2dtmH7yhPduNjrj57MFwXERYp2tNLd2OT97QlSGFuayBodXNZ
YmFjaGVyIDxoYw5rPh9D1L9c5mhiL9C0ldtWz492e+xxzDimSEkHtM5yJBZnDCPptl
qwdSgn5+N+PgZLEdgFqIo2el0niIgyV2fnliZwLWZ+o9Mzu6Y6G0qn50voQmLTu2
Y2Je7U3rlaXs1EVxp+2cyqgHsxS0Ao/upbq6zcyYcZ00iQBGBBARAgAGBQI50yQF
AAoJEB2gnDEW5AIHWXAAAnAlWW+qkg9A8HZRL+AhCUAwVztfPAJ4mT+zi0ttDY8B5
gbi04h05tncn0YkAnAQQQAQIABgUCOv/oxgAKCRD1Snyxx1ig7aaTBACTCnspTPMP
kyzPmrktPSnc/QmTkWChOpSwekTwPYnpZHLhNZ2JvYZa+gOmLPJYE8bWqhB99dvv
kz524BGqCoIx0tyU3hazapa+E2ld+kt5D5OqQWSYjdEZdkBBNyCEImG95PpuDbK
cGkHGUGalMwkhhfVogABTrqxRfiKp4fJW4kAnAQQQAQIABgUCOxUzhgAKCRBM5bQ0
/T4Yyf8ra/sf8oyJT2uxKOWEw01dNwmAmgfn+ErleBfYx2uiuzohz9uWynCI10KU
v9bamdfnIUpi20UN5MDP0VvDCPrsCLx6HXgQsyJr7lYHatLE4qMN2j6yZNMxAYrI
Stk+tAvve/kLx3F64w/dS6lKPlBq1qYyDFcrm6LRSYDPTnNkrOY4u4kARgQQEQIA
BgUCOx1MbgAKCRDvJ2GPYPheJOXoAKCVIqGYb9ePfUNYL2H9x510U/gvfwCfsikT
MwciFHzKQmPzL3egk8mh7maJAEYEEBECAAYFAjvVCKsACgkQSVpuS2QF2NWJxwCe
J9U87N81hnpNtco6zAEJCgZG/1Man19WJ48hMTAE22KEYSyNhYtOHVkuIQBGBBAR
AgAGBQI716oAAAoJEDKnfhgS/wx7L0kAnjZP5tpUsvGtSoc12MjmJPBgHNKAJ0e
l3Ux5AM8IzsfWZq5OXelipevm4kARgQQEQIABgUCO9WxcQAKCRCl0UIKM7R8y+/i
AKDJXQsWdBNhI7kzAYIEHbZaag4DCQCgn0k04nY3Ai/xf1RmZY00tF/k6VyJAEYE
```

Project:	GN2
Deliverable Number:	DJ2.3.1.1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

```
EBECAAYFAjvYuUMACgkQwSzt/UffIu1LJQCdEYYcfx/eoNCHozVmUoeMVtiLdvcA
oIiqMaSW6jDAorx+sdRu1JvZNVWriQBGBBARAgAGBQI72goKAAoJEBxRJvM+ooYD
gm8AnOAdrM424WqnPHUyIQJSJSaz5PSFAKCDM7BLhBCFi9juPBed13i5bccojrQh
SGFuayBODXNzYmFjAGVyIDxoYW5rQGf0dC5uZXQuaWw+iQBLBBARAgALBQI4ZYXh
BAsBAWIACgkQVfe6KqApYZqVBgCgmCPzLI0w2KdbFU/S5mc+Qf/hK5IAAn1SIhIF3
txlHT/HezFFCJD0I2xARiQCVAwUQOv59gdpUImfG1B/9AQH2tQP+MtfT5e4rprS4
9pR4hHPC7+jagKQu6rXhlvuIaoj3i8rDuBh91pKN4xU1hAtQTtuy/x5rYZBAz+CM
N6IIQm8TlC5CDGpFq2KLnyrnrbJbZfIwcJ52F7Ap+AdsPkvjkVSWY1Ka3XJz20dg9
Nc7J1UQA6Kt27uK3O2mQqmdPt/JbMcCJAEYEEBECAAYFAjnTI9MACgkQHaCcMRbk
Agdg0ACghh6VTk6gq1sZUwU06HJZmVyfEqEAnAxzv9PhUIQyfGeMPC11uNbNY7VQ
iQCcBBABAgAGBQI6/+jKAAoJEPVKfLHHWKDtsMwD/2220/iMYe/ci1onEH3j1je+
Tc4OnputqGCRNRiK4jmW2WmVku56DnAkj8EbKY0+ov6aFh7gKouQ3CZ5dzTY8mzm
11kaUYeYcIj5AhntINQSu/zt1Y1GUY9gpVxwDt3olQ3sWWanY/0wPc5Z9upwbQoO
En3MhKNjLwy2SIBy57dbiQCcBBABAQAGBQI7E5vKAAoJEEz1tDT9PhjJjLID/A0T
kSDQLrCdWfuRnKLJr2b70ALQNVMLmbkxUkyHB1yR0UtVRZAt81nz9If5ZsJ4ZPm
8jQfQkGpILUnwtQC5zIB/9eYH7NaY/3OmzfYsaw4NhVp4KmlvTa09c8yI6222y0x
127bZlCOQdQh0Q3oGmPniBJol4S3aLu8H4G5srB6iQBGBBARAgAGBQI71QiwAAoJ
EEr6bktkBdjV7WAAni8PrVfqJB0v+XwVICyhoI8+gmY6AJ0XsOGBAkFkShMCCa2H
Y/2N3nOn14kARgQQEQIABGUCO9eqEgAKCRAyp34YEv8Me+HmAKDDnux1QVFjGqvK
lPYkTgPeoRCBZACgyHM/ovsW9L9kcg08ppsfvAG3vwCJAEYEEBECAAYFAjvVl3cA
CgkQtTlCCj00fMuCBwCfZxGBHozB8ijJAAMx4Ikd75DhF3DkAnAyqNDRiYx0wSVvg
X6ppprmlYQNUiQBGBBARAgAGBQI72LlHAAoJEMES7f1H3yLtbGcAoJwc7MHhg5QS
s7bajLka8J1Ss1rXAKCcA91+08Z0d7KkeB1HZtEICApjMIkARgQQEQIABGUCO9oK
DgAKCRACUSbzPqKGA24UAKCYPHMBxtZdrhI/M7az/FsNiUfGqACfc2b/eS5ZW0BA
zrHUdmc/DtTneTq0IUhhbmsgTnVzc2JhY2h1ciA8aGFua0BpYm0ubmV0LmlsPokA
SwQQEQIACwUCOGWGEwQLAQMCAAoJEFX3uiqgKWGat10AoIWSFnQgnNrT4MKjdRAG
23vRHkrkAKDKNEj66+1fsmQBENpVuNZ5J5IR8okAlQMFEDr+fYraVCJnxtQf/QEB
MIMD/0TKxp+aWyLmEC97A6aKrc/LHCyGJQiEbrNZg1Lcs764hJePN4FgXWRABdiU
M7F223t505RUozGzIHsWDcsd+5ub1g+Sg0tpq4RzKZd5vKQHWYXv/bUAAKV6UwaR
2KwmWos3fp3irkbftQdZ4gcSeBXsI2kP7zz7+HJpFUKIwJ+8iQCcBBABAgAGBQI6
/+j0AAoJEPVKfLHHWKDtsMwD/3FBabPwDe77CeicQ7rYfxme/KUyp5ocdgldeKXM
MGCGzt01IQfIHX2D1CfrJZVFEhnXgPProSoj5dkG6I9AyM/PdNvWn68ij9J9D/uj
eN3pODfhVBP6ulsqm5PlD/904dcCLxB0D80JoyIJDHXKYCh7s0Dt/BM/2E4J5rIM
WptjiQBGBBARAgAGBQI71QiwAAoJEEr6bktkBdjVWL4AnjqtMmx4zPBNXRirqrR
CXesALLDAJwJAlY1XG0XWK1ZTaG2dz09t7pZyokARgQQEQIABGUCO9eqEgAKCRAy
p34YEv8Me9aSAKcZuq5gT1niMb4XBHUN59J2jm4CWQCfWjg21sB+SUMKno9Xag3K
9cboXLOJAEYEEBECAAYFAjvVl3cACgkQtTlCCj00fMtyfwCdHujMBqrZcxoardAU
YnnvzMcNxxQAni+zB1X91ZfxKmaPLX7DwHaU7hh+iQBGBBARAgAGBQI72LlHAAoJ
EMES7f1H3yLtbJ8AoLozMQpy7Ea4EX6HbzkDuEnrLUD1AJwOcTEUDq9FkZ7CAAGD
xyGa+dxUPIkARgQQEQIABGUCO9oKDgAKCRACUSbzPqKGA5/yAKCL6zgZYss1mHUu
az32H9Re9QsfQQCFQNV2baE0Abt7pWXYp74wJQpZ425AQ0ENvX7/BAEANWZWLvg
1PZ328dQ7jhdez8FpOQxsuHWEfCOSyV6IHDYjG1/Rt9XpsQJHlXkWhhT8XqQsxhk
o7NaBgZGcSyYm66hObEsngNotf4xTz79KuhFZnygCa7fPhlCwK0ixQrTLu2D+3nr
6ccrvM2IhypZBnv3bmnRe8EXZp5NryhetJebAAICBADSWI/XwmC1pL3c/3zBAHzS
o/TU5y9LCzdtkOkGHDpP/9x1+0sOJ/yvHGezesZ02fAgXQiZOS+TUpW1rgRI3N7
6YCRak7CESa+UHVLLXXGIEv7rqtvxEcpSrmYxkU11JxPkQVgS1DoOfb/1BHdJXWsO
2Afpr9u49VofEgTroDzi7IkARgQYEQIABGUCNVX7/AAKCRBV97oqoClhmmhiaJ9+
E+IQfDrpnuQFLHj7TK3fVK75+QCbByQcZP6Ghk88cXjOsJ/iKYZ01lw=
=tqxm
```

-----END PGP PUBLIC KEY BLOCK-----

### Rafi Sadowsky

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: PGPfreeware 6.0.2i

```
mQCNAi6vqMMAAAEEAMI7S82MWUhbB19+gfYv7L4VUfZpYEJ+GwSRpf11v1qrIRMB
9lKv/ssKHcXqgZ6JrsKxrtYntCFr67TtccsTfh97J/RNsp3bET4hcdagPvhzntkB
sXHvi3etj+Sd1hQHB7GCs+o4Pgck2qTCM4t2cPITnCVSQATHVAcVt9E+5ZYFAAUR
tCZSYWZpIFNhZG93c2t5IDxyYWZpQFRFTEVNLm9wZW51LmFjLmlsPokAlQMfEDT+
23wHFbFRPuWBBQEBroAD/1151feqCBa4B6t6+OyMT85EHEE1HUHJ3+X3pBIiXX6l
zQHRD9F5bjgEX0EkaLkDclqFXfkJDwGJ/38M9JkHSD+c+43wn2KlBFe8N+zPFXWA
```

Project:	GN2
Deliverable Number:	DJ2.3.1.1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

M2FEMgX6fHpDg7I9RvLVcnxN2jBzgQSt2m9wMaaWyH8g8K2HQNNNDUE+54a/DAyy8  
iQEVAWUQNbybsoMaFj9I2PatAQEYfggAtD5tBG53tXc9VVF4r3i4SPO+ASFC3v04  
aR6o3r7nfrR+8zBNh93g16+KDL+g4GDKkz8XWkqsxj++peARL6dF4VeZKNA2yI/EG  
5QsT6zNtFvgJ9vw71it7N6hk9g+oO0N6c3pizOeSRKhm/9gh45rCANFiCqqX5XzG  
oEvh/yPtVPMBVOEPJKLJFgc/mmr3cZMgXHBFLtTcPd9VuTukl3jAns7jD7yJdeQ+  
JLkvJ6slTxGX39bUOW96WZKl1f1G5xKMazCIyvP69HDS726mEMH4m7mAKAWcN11dA  
J7KctiM2moYwfjMTFa4XtFd70zE6jXOS3mndHaUjJknCIkh20XQqOIkbFQMFEDW8  
Va8OmezLlPcVdQEBpKMH+wXUOLor5mBRRGHln9H88AOEtC8OGrdAWndx76dKTv11  
JY3ZHxxt6+pdoiKbO+zhkiLt9Od17YYxVTIEzyVdyTRdIa/VVHtrKnUHLRgr43q0  
7abKGGJHny4lptoYRNJI ZH0WaYgoMmEhAEjVJVI4mOK2uDd8DmheB82uOtIkfoSB5  
leWJVnzFeJp4KcNrnw/YLcifiNsnxUzNJY44zgDwMZ8WbMM3Xdygt8ePPJJtC28t9  
J83HOZmYqQkMLKoti/E7Jaor6RpFZlYsFNv0m9i0jABQzuyUYicV4p77Flirn0Ej  
DdWVOHQfJvveZsX8elQBwad32eUYmMvgrobzLW2eWyJAJUDBRA1s+Gvm+MTbTMO  
N3cBAXksA/0eKji9yhgiG1UweaIt6tAqf+Au1Al4uEqmI3ZTJkX3JZZOIZi+PvEc  
oeBACuX+X/tRt2GE/dss+9Rqv0z5+K87Cf2srniPLad4+CJJCWnWIoEcQpEJ+TKT  
bgInVorkTpgGagIaqgfIz/EsZLeYvY9eaCGI1jO2WmGRsjLEnXs2LYkBFQMFEDXh  
FJKlLq8nJiH7iQEBglcH/jXC7QHMePq0LP+LUXSRFBVpwcaVoEVoCtmwLPyQTFpi  
QlXinEs7jYMz2YRQ8KIOlC6zw5zXP8x75qN1uu3xmNh11McuViv3WldjZmVjB  
+zVE8KR9CW9Quw1HXmx00WNXxA3msRuJ0sQFZz8JpnigIkYlKDD5AnF11LQZ8j5  
Zxa47ubN36EkTu9ytYEUvA3wTErh0QNYDhlcDgVarCL00BOSV2IQNDZu4q79NQ8  
1GTDWKOyph/VPbZ0BQFExoZ8uJ2a1lBmZ5v1I4XIe2wu0dpMQ10IyQGLBTfLBI  
8SXBdZs6T793rwT2IOBJ/g/K9qWGrniKiRUK7w26xSJAJUDBRA14YBRQDHURb0R  
ewEBAwbwA/4/xqx6Tb3u0pXkVsFJ5GY6HJuOwo8AB4m5xS1+djQvhZj7GSteTbR8  
w8d6SW59wwAq9Ph2SlKifMPmNlJGXTZiKMO8OT95gouIoYT79nEtT0UUV4embpOs1  
nhQp0TETkYjyUKM+nut9QaexXGqf04iwdMeZn8jppNEKL37k4729i4kAlQMFEDW9  
pmaK/zAeErMIvQEBc4gD/AxVBQNGeHR4ha+x+uUD7BTkCjkmUSvp6imhWFpivst  
+XY/jDmkiO00cNCzcP9B/gCZiArGcw33eAlJvMu7HG5vrtRw2kClwm3o+43lG9xk  
FMkWEiQZBXAeLibKOCOgqWFZD5pwQSQ4WMf1ZyEyNaQ5jd1POGz2nHGabvd0Snag  
iQCVAwUQNb05zY4CzbsJWQz9AQEsCgP/YPKYxHkoVuxYQpWlm2vAEsBvPPL6glgf  
4j1DMt5DARMqEc+F69aJyvn41f0Y5oBJShtkQqj2+cwzv2sHAqoIuWJjbT5rtwMJ  
RUB+E3KJl1c18pVZXkca4XenW45+ANEMdzdOF/XO5NJknK8B4TGpvr811tRftv/Tk  
MuYtW03pBg+JARUDBRA1s7kznd8MItGCKEBAVJaCAC9gwfTrmBeEEEFiUMj792B  
jGiSGZsQ4glcQ6hnxaxZCUEdcno3mdRRWjy3yAZf3It+8AbKcZ8QpLigHmfYasO  
duQhZz0yWRVca4ZDTIP07SiKRf5hy92EjzQ6U/2xNQsxhxJd1vPUdVURZPJXFeMB  
YC5UM03DazHbGASot14kXQnzfQgLBnfMyasbddOoTciXgpEh8v05x4iRjBwGazkD  
vWAoDWeJHaQn6No28h8IXRwMWTB7aGa+7/5wMkQSZpc7PE/pbrDOI75miqTby8B7  
NLOxpzUFSH3jMxZy9uxKhMmFU9X5wEvRuTF5ZLb6s9IG2BdroBT6G9EMCBh90qkG  
iQEVAWUQNbYrqrceMj/eqW1lAQFYkqgAowu8vKJGOpF+5ZuKQsf2J3k9EpFp1HQ  
T81vLvlk0iDORULWdQSBY93RjFqcc95A7qMnopicXed76T5BenDPC7M6U41TLF0  
2ale723GCTM95/qKKrXmA/qc6l+7wfetnLBhhLw4RV+m56n/YNlIE+3dH6r6BtvL  
Cm6vqKKSYPNDvbW2kywWF6Par0hxuIhta7woJ1AdZsrVndt0QKj5TU4UB+2pHS90  
kQGMq0SPu5/qteoeqJqXqHP4TNrvtIruEnrAQTEMoN7rz/Gw9fL0u/GjoNAaY2od  
AhHXpW05GIppuhtcUxvOGRyotNLafdizRvPEDYxTW7nem5w+jyf4okAlQMFEDXO  
3qrqip0r11TozQEBLUsD/2GhcxtgAnXEBsAOaW500u9h04biJoeydL62sVyYFwq6  
QbdUGAXkHPLN3/GxOR62HhF6JrRBIqDg+g9SvW0TvoCHEMkKqByLTWHvKlvq7vZL  
eIZPRP+EknzUs2G4fVihOcU4C4lxL9dhIlyzMxrnN5216w/R9SIsAUq1uSHKtT6D  
iQBBBARAGBQI4Q04iAAoJEFX3uiqgKWGaATkAn3daIUwHeTUwsfnho1MPi3jD  
YKVxAKDC11ij82BanXvaojsZ8wcuA7rviLQWcmFmaUBURUxFTS5vcGVudS5hYy5p  
bIkAlQMFEDT+2y8HFbfrPuWwBQEB0BYD/1in7as1tRDj9u+SLXQ7qi/Cdly/5wvK  
pH1BOB2Djk4Dh4AHLsB/F2WUDUKWfs8QLacFxpdiENak9Uf1sofav+qIqOSdfOY  
1TEQJL1J4mahMKox9aE3c/pzXT0nAYNngp20ZL3HCQphhWQJl86wOBltCwYAHjWIF  
ReQ8Cv+JGCg1tCBSYwZpIFNhZG93c2t5IDxyYWZpQG9wZW51LmFjLmlsPokAlQMF  
EDPhRV8HFbfrPuWwBQEB/iMD/iiLkqi6f8GuV++U/hV6ZfSD0mqAArOeIaqbwzG0  
27WzBnPpiK+YUyLHh9TItQ6nWLY7BLwbzdfU0MUI2/CI0xnmGIuAdo7huNw4r/PA  
Tygli9wQNYKJHSy3fQ7ePd6cemJxScRjQWg6dnWtEOhX9xtudNORo+6iAgbuud1r  
79mrtCdsYwZpIFNhZG93c2t5IDxyYWZpQG91bWfPbC5vcGVudS5hYy5pbD6JAJUD  
BRAzstHMBxW30T7llgBAZHF5za/0V9LRCRwBFEVcFjqWVklqB9P8DGIS73h1GK4vS  
uXjVN44U+jTxf0yq3udk1F+lzqt1GA/zedHmjJO3gV7YJ+HB8iJBzHxgVj/iCNJ  
a6DM5eJCWWLPptxFHDMagLmZtBIQqQhAD+PB8/8G+c5bJZB7qj+qvZFGmdtvpLMj  
DQbGV4kAlQMFEDWun+W0As27CVkM/QEBhgYD/3xLBC8DMuVRmWPC15xRIbWRNcO2  
LdKTA0kNGr6P16/DVwxrBfKvXxZsLdITRziKxtNetEDhnH11AoLYwH/XsI+v80x/  
TsK+/cbpOhZXubjwSbz98x8YVHY2eJlW9Bb+vnWZEgWgMNS8Z2kMTDqubndtx6v2  
UXb0Ec83RX7LdaXQiQEVAWUQNa6G53fDCLRgihAQF2Kaf+JOMXM9M2us1TBQGG  
0xPvXLxtDX2eWxoQ3cjawerBDz7+yOYOFksA0KVXCuzQMiF/jdsrsQ7+SYFiaY+K

Project:	GN2
Deliverable Number:	DJ2.3.1.1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

```
HsNfiz6T6ghOmSQTMKKh3Way4zwQixPvJfL0iHLIsfKWdb3SGbPP8AQmzCxlGt8c
Q707jSOWkgCoyrgezdgvx/AIhGnXCH99PzZJH42L4S0of7JQ1CGoWH+9anzAIs1
uZehkaQBiGqdpQGHZ0ZlnjzDLM3Wi7TGHHCaQSK/i6UktPvjIj93oNogJ7qVJFq
AiCnmCn30Stu4l+xJJBzCJRhtIibyiKZkiyoc+i5p6XCXiAWcxTDhEH5yQd2vfJ9
tou0JrQmUmFmaSBTYWRvd3NreSA8cmFmaUB0YXZvci5vcGVudS5hYy5pbD6JAJUD
BRAzuV5GMcobg4UaSREBAXowA/9vkQkMph43T5P/4HAHxPZB53fe0482NSjq/F+X
5e9zbU6d8MHBA5jZ2g7jiTW+pF4g2XHJJE0Iz1FvZ7x233Lt3rfgay2MYNbnG2OQ
Crep/4OC6VJfYdk5bj0pzKv8ahvb7MBAwLVG8NgHJRHE3NwLT42o6JX5z0+CuLNA
gCG8kIkAlQMfEDGjjgf1Snyxx1ig7QEB0GWEAJdZm3hVGB86vzvK5RNUAy0cEXR
jPIY1drg6pSiSzfeJh8ycTtGc3V0R4MHLACFr2HjiVBOmIMbwdiO+xEqAhUAtmH
diWftqpid70z2ZtYRscEzdnvIcU+mccaCr3YYMSb/k0Y99LtgJlRO1Y48xyT9+hG
pm+rTPSdGeUCrGuliQCVAwUQMRi3wUXuiVfjNP5hAQE5tAP9GNKf1aRoYbiD/2um
aIYP11clhyxofJTWxM3YkrrExsbr56cvuTokvG0vTmrboT+90UvT8u8+saCPmcBT
fNxs/WkNIMTlgEeTiXoEvEUtChwHxrDRN24eIGLcQKWrvZAdPbjH6xu+dK1BGgUo
Jus6ysknQcQrnAvOTDZA4Y+EximJAJUDBRAVSD83Ecxuqco9f+UBAXqja/9SACkh
s9UaO6mRMudaioe7toI5mMP7cTSGCadNPdlk3ZR0h75l6362v6103xMvM2/Ousit
C7Wzsf6E3jppj31x3GX7CYeawBqk78f8ELkBMx6afGveuIjedwszNwAuObbluNLZS
1nqsheS0STp0ZgEZigz0eH+Euti76yWbCoQblokAlQMfEDWjZuArT9AGN1kshQEB
7REEAMEZglM/ykIF816CjBdyBLuwCDJPWarsQWkCIypqdZ2ebjkoYQHB63WvBUOT
RjWYSTb4YrJN4VUXRitCQRN8QfTFJ/CEi+HwoGn4IYBtoZacG1bfnll/dC/yzftB
8FGH1FIppRNpCmGkfpJ7F00ze1cNw9d3aOHi5BqtDEGAUa8iQCVawUQNaF/DvOO
YELgELPVAQFfx+QQAmRRNxqyLXXhu/K+QBKVL39Kmn/bkW+WUvPohYCRUodumul4L
wv4KvrLO7/KV9v64p6V4Phk7IFrs+Udvg3tvHIXbzGI2DopxNlA7kaeDGynC7jbU
V63Qx0dRHFSjICAL5BGC8o/G1Xn4N5heKh86es1VgdXVksBgYcO5Qg2mNlAJAJUD
BRA1s7oTjgLNuwlZDP0BAVkiBACXn/Ffacw2AKqR8F87Y/7BDjFfXbuss7+NX0cp
/2cfYqmf342dYXgfB3Dop4RjBBQoe224rwQj6xXRfWPZt23B0djw/cVU9YdeRoo1
k4ht4C4UIvbw1xHMULeQWkMR9gVVQQTl3FUJJK488U+TtKPY4nM7tvJexFBD08zQ
X+BEZYkBFQMfEDWzujGed3wwi0YIoQEbuXcIALBQRGtDDnV55hKEVE3giRmmJ7M/
ELxCunYYZBujW8ghwDD0Dp2tdLQc2mYHbAs/0sdKjpsktAIdoMWKe5IiRwSohXqq
P7D4WL83lbyIBB2ouhha3niaEJj+yPNZB+zK0XYsmbKqhhf6v8ofORa34sE98aKR
itmsKQ4iUoYI/vZJMqzJKSQaIhWTwge5meKyEzpjFRYwKrB4PeU/yt37LUgtXot
PHYj5oTCjpcgWCQN2MLWNgDA2nlRPNGmQitRy5ak7GoX4KTubPpi90IqQ2GvQn9o
1MFqek1OmAcUega59p1SqWRtZC7qQDgB+aVOKgoIANipsalkTiW1kCHVH0aJAD8D
BRA1vxx8x5cazNGJhdYRatILAKDLBI6F5fnh2QvUa+2Vb36f+thZdQCdH3WNDWJL
qp5ax4jOs9Gh4m5XM/u0D3JhZmlAY2VydC5hYy5pbIkAlQMfEDV2r5wHFbfrPuWW
BQEBelYD/RAi8gmS1lFnx205sf+bqxkm8a/CIR3HYb8p7osbxODS45bAeadHBAnt
KXzrsJDODEULZ4JJRrWjF+3GPDCDwI96HFdwH7uyHPKI5hjx9fqp/DQ+8lLctgSW
b9++timlRcF30gv5aviWL5HX1mNb64WZ2X4lIZ+mq5ASUfPfwEj4iQCVawUQNbO5
cY4CzbsJWQz9AQH3NwP+NyKGLi0ABGYWfVfn+RkGQ5H3QTBtuT04/u6ke+3hnSc7
QfYHHGRJF3Tzilgih0dorCURc6A6J+FSrk476UDKYbw/Je9q8wMxxR0XXTAKWyMY
vuLU45LnNqjNdVLUamV+S9P0Vw3xt4NLz59Tm9l9v07lur5q2mfHbx/e44zwa0OJ
ARUDBRA1s7mannd8MItGCKEBAeFcCACFJayGT6lqnHqDU5xTejzy6PGbbI2/EWYi
zdWBvIzZXIJ5BJ1+j/dnv4TKqMJm/dhJtrKsZ8lpCq0jagT3uYEaREjioKddmJI
2tIqbN/HTA98gMablvg/hb9S4FpUmuhZdOemEvaQiaOpyCxoIGxmmXXbRvFI46/r
b0ApHezVmJGHGEECG+a+5g/fxQjyxy+dw3YJK8Pvwh+8YhdKsXKLzm5+FEBatrDF
poJv6XSXxBvVb+/3o9oP8dJqTTyPQURURbTSGoIShqk3gLFb/jaAckEn7WvN0fMC
1bhD8pNKXUagBa9PvgH6HP6TjBueYGCfTn2X8TU7/yNR9Kdfs2d9
=vK1K
-----END PGP PUBLIC KEY BLOCK-----
```

Simon Sickman

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i
```

```
mQCNAzCg6BQAAAEEMixVQCA3gTU+3vOhjrazbRC6oUzwmB05YbJFpYaZcilUmdC
TxoIcPrSMWRnDablml+ysj5tAM3pRtv+6oG1HUA+nyHQn1fbh0yutQSB/kZJLtn9
MQeXZkC2DXwe69Q4XKEFvqNmbBp0EMxbkdhfNT8N/Pu01oEv7kXuiVfjNP5hAAUT
tCxTaW1vbiBTaGlja21hbia8c2lbt25AaG9yaXpvbi5jYy5odWppLmFjLmlsPokA
lQMfEDJU+6XU7RKSiwU0LQEBz8YEAJ79XesvjbkvlRAYpzLtOyWYv/0Cft9kh4IR
DpA6MV1CH19RGv4g7kcjFY/Aaa5ii+Z15yTbFU8pvMNVcOpmMyf1dZdvFULf5SYw
CTqy92Hn4P8qErtEzcv5eq8j1RmCU8AolXz3hc8Q1bsk/7RJdjJYUVjLjhN2Dauy
```

Project:	GN2
Deliverable Number:	DJ2.3.1.1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

XCcNSBGFiqCVAwUQMgJtz/KmgBGt1kwZAQGd+AQaihVtF5vVpjqcGKBfmNMYg2YU  
M8EwvBdwrScoaFstn6203ce99NxcerKw12G4dlUBj2xQzub6MA9b0xUHW6P8T0rA  
T7dqSx/ooxBzzKPAxigwtuI2jwp0LknkAcfPGLDsZ5jXLe71GF+gmj0n0vDox5U5  
Hwu+HJmSfejVJZepXpaJAJUDBRAYE5PH+MxVdc+ocgEBA51A/9QSAUoZr+40P/k  
pgXLpSCcakbbi+Jf0i+BcmNwa8MUlUlu4HELcrjaVmbKWXxmHbzX2GQRv2YeyQfC  
hkWh5iyVPWwtS5lepBImTXXdk4b54UDC2b1A/+gunYWbiRnrAMkzog8DU0okY6N3  
+INhKyJr4u8gdjY7u/W8v6GStA/S0IkAlQMfEDIunHyVfucR9lOShQEBy/cEAKf4  
P0UiqPnYV4TtttcvDya+L5/AJ70AF0DgD0jUzs1mlI2UgeX13Gou96nyNbkgp1Dv  
gLRzG/EfERIKLfyIP9yU/v5sVyHvZVKMhYLbBbH0KrMxMQL11wQAL3qKlgNjsUG  
cKG2yzYJhvalT5VGCaUC8xeUlKHgP27akborKptciQCVAwUQMi19o301WId/gr5x  
AQEKfGQAkdXQ+js/lHPouxcmg5Kh6vYziK6stQ1/QbV9AYGs7hvmOyXQkf1KMVGz  
k2Cc7YMA5KwMdJ1QkCxlR2up+ewkDfmqeqTtwGLWfYIIWpjRw824o2qW88AkGuRq  
U5+k/JEYG+GqfW28RvbywFtFe+fx6y/nDTQyZtFBRBJ7HjnVPHSJAJUDBRAYLXU1  
krMiaqBYUwUBAZzdBACphN9U6IP7281ZKRALK8XG3jtmzWCikPLL2Wmz50eDDMWz  
3FcyWlnxjcnqnnU1dzJtvMNTpoIlqnIgpPNq/BBuZzdzWVXh0Xyl1gpTLv1JtSqzE  
41/k/2c+DDZ/GW3P+LQZqIL0sopHqv3ESThWEAIEbetugEWINSLbpKzD7CJWUoKA  
lQMfEDItbeKEREDx/yP+bQEBzLgD/ArPhV+EPx4BF4Eoa0jOqQnlwI74EDjGNu5p  
GdlSAsID0Ikfe3rLbLxGa+6Vo5Fp4niEmGBPU6kXLGP2qspe/KnIXOVSES0prfaG  
roUmp5CA/k3U/zUslpsYPN9HlweY4qAyk2pAIL20DTMKzqj+wjzh+L53YHR7JEWp  
PsxH/yCIiQCVAwUQMivaVs1PERkvjVA5AQFa3QA8GAPUZBZGDQ2mcjeRv5thwD  
8UeWBiZDo5LuD+7V9w7gSfQxCqFYy3UuAAZzEJNBuUhd0dKl3wKQNKNUbdXwFKS  
yGn6EsKpZM4Uh8M4tiS1BPNGYAJ/JB3Rb+x+GUaa9Sn8AwbTD3R7ngjCnwym6x  
qyTZRH1OAVEEzZbBQPyJAJUDBRAYHTXVcU3B1QFxcMUBAdYpA/0aWEqAyQGVWUZQ  
yicdBh4MFhziCujtM/V28HWC9ZJ/Ph0HScpFQW+K8Go+FPvdodxc2HARjun572aX  
UMpvUEIvRRqhoLtIQZ1bFT2Zhb7pwQTcbNu/gQaFwRWJjWPPSj0WwqLZ8/89kb2  
GwsGQP5J/1NQ0MuB9ohu0gX8RX0iBokAlQIFEDIS/AzghzhMod6d1QEBH0cD/j1w  
Qom/g2WvcdI3U5ByRz4+qnz2bXRY8k6jTDYVI43ktiR77ohnjJEGP60aYxo7LqJb  
iic8Q0qy5uaPT5jLJHuxbpsA0M/FffoGFYeFlqwlMMGbtBcKkNn2pWYr3yEJq8yj  
/2ka2Vffghjcnf+Mer9rNOAES9Ak902kU7QNucbZiQCVAwUQMi5dHZITSRnppfh  
AQERrgQAiXVG51/CMz3/GSKxok7+ghVpjiOc9tEhPGs6l2Ks1osJp965zUaDfCna  
cz47LYyS32ZXQOogeGgo1P09Tt6eEjpeB5J/svlr7V9IG+uEC/Fp2lq0/QBo08Ur  
SqqaO510RqI+F3RtxI6IQEYlhy3NPAMQXwiqnWyNe5RuWId1mJAJUDBRAYJqpW  
hA790iDnbl0BAS1LA/sGYTEYHcqnYBNVxcWPA1VBk3Schj6FoyPA/pyv0Uf2Jq+wE  
DrR2bPgBG+rFe+GbXk6irN63DstZc8oC7yvs4AKJ7Bf3492IkkxfG52G0XokqlnVA  
+r4osy70ruCcGQVizYWkn/zpIB4vN50DharZhCj22nVI4fqs0s4P/52xrDroL4kA  
lQMfEDIZiqkI1LZzWyibbuQEBdvMD/RnsTu+PFGHZV1DSt9C10IzdgUKE2Fo2Quka  
8MJkQzfaZ11TRw3HfPYOia3LFoPo8w7Nuu7h9K5n2db3rlm7j9TjDJX8NGkqTUyS  
7hwUsKg56LrgeXOESdirAj7k142XkGseLPPUpV4kpmKkl+VXu8jcnIE3uVF9SM1  
c28EM/CpiQCVAwUQMiIUotxothpQbsLQHPJQQAkwk7i2Dq901fAyOPBJafGfL  
F96MyvEdNnakTlr861P9kgxAOGLAMKTAJSH23aDjzPza464Zy5rH6ZLKWnem50G  
6+9y6bRwizCiW4VrNDw0lxX8Kr15+php20cIW8jjOAOBvjynw4dNx5X6jKEanprk  
TB19HBImB0KpWh67Si+JAFUDBRAYEwrMMYSWxuuNrM0BATT5AfsHQLDuBLpm3xa/  
AGxlgLjKn9wIpDutHhbLnSXctIwMW7RqPN7I0r8ZsFW/9i9EWZAbNceRCh0+/KLY  
29OdvEXdiQCVAwUQMiImi3K004+Hq6WpAQE/mwQAIwQ3oMO7BKdwd02OIHfyEVjz  
HzMaVVBH9OuXWxcBdyfYFMUzqZ2a7lu53ikL6l0zmFveuleBEiYOPBZZSVX8ryg  
9DkyKaQHGF4LpeV6/Fcpr7w3CfecxagcF1A3MrGgkci4MZrpgL890x93AJfSvK9w  
OEdKUG4PX2dpvJYKJhQJAHUDBRAYJbqwsVgrKIQ3mQ0BAfBkAv9DEXPnzVqjGJ5R  
wHLvBziOvlpY+67xhrAuK2y007SXCbs47WC3xgN8n4fAWkUL0W5GZbLbRzTa43wm  
KUqk16PlKSE6j6nG+XKgdRyJVpklvr4aCVNQDYhpbWJwbxR6QkqJAHUDBRAYIVnD  
vVQklbvk17EBAQGVAvwJjkeGZU1+Zjb7XINyJYwYtYVw8j3+EkHs3fyMwfc+gJ3R  
8preukca6ViPUBXL3qZHSltFPAZ3y0rGkU8SKxzBwC3IkCoeG5RYFe5q5HWggeSV  
KGXaqieKkXN1I0BPZN+JAJUDBRAYEjHG+K8y+54aU6UBAV7oA/sGKWB/+RgAet/0  
N8r7/QI1JDL5Eb4Madrf1JVKTjJzk3x2toaGaVgtonnZ0IeIz+uVm8LoMsOHZiv5  
pLZhrQo3VoducQOWwd4PNWHUSQd85WtH/C6yO0yM727RHMLlCsE5L2JvHPxIkvTC  
4uxbE2rbVUVz6jc/EQJEZrn83svB5IkAlQMfEDIay7wx/7eDRBO2kQEBbMwEAJxV  
AgEEpcSGwX3Y+P1B6hNGoVMuOXBnk/33R1JATknd1jUOPFUpLAmEFikJ4NUQuM1g  
1B33e5MkjZNLg9q6278D9awHMBTq+1EyuLc2k1kmp2YMetPsfuj75y4MGw5A9+w  
t3PVN5MKq00hnZDVtY6q68SQNeiJ01Co3V4VeY0BiQCVAwUQMhixYILa4wSAFaEJ  
AQE1HAQAL2NarFDh8pJzNn+JS/Wy7lgHQY9yiDov4R9T0tmAowkpeWg0/g4HpiYj  
8fXy5ZxejwuUHANW7yl6xM1yF6XDqnsDeJQUMGHYkNin1A+w7YbH8WI1RxBZBFU8  
ADfy0YXyAlhej8aF6WB0AwvKpIyHY0MIIASqhbQXzTweKZ36/I6JAJUDBRAYGdjh  
1ocrpT8NmN0BAaHNA/9YeWcWAnMESHp+9gDPKij+hpwzyUKZQ/7Gjgz3DUJuDJDA  
Wspk2G4ehzZUX25E0ZJgiFR+hz610T96eTMDObNyicnmdMsXLoegNtsNxTfe4xjm  
rsYw9wOgyS9LGQUY9guHPMHQpNvR5/4inWkRoHMuCQmqQt4a93E1a0ro0/QDeIkA

Project:	GN2
Deliverable Number:	DJ2.3.1.1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

```
1QMFEDIzWfQ7f8e8znZrHwEBk4AD/ArzrpK8jGoaeV1EJuRvfD69jGTTQRg1290t
5CtpHrcV2lz7VziGdIp1Sxwu4UUEFh9QjuzZUIHptMD+aokrI8gbhRY14QYUHxa0
dk75bLw6YupFafDUWQklrGlE0xe+SroHoGh2DLikr6bzbj2GFGGYZzRzXtHrnw7U
oY6j08eriQCVAWUQmhl86mQoyhyTCFzJAQH0VwP8CnfVpxseToFrokLegCD61x7p
h0ngaMwI5Ay39jH8IJyU2+IH8IRcw5cBBC0Rq5ptbygiviVgB70iqjJYoYWrwSWKyA
ggQPCQRTkCJMawPrZGuR05VvC46tz6REOQu0B8BJckdFS4s04eapni8WAoueTuLw
FxC2OFoYeiooqHoQeisiJAJUDBRAYGacZjgLNuwlZDP0BAVPeBACuuKouiP2uvUao
6MMb+HdbNP4IQp6wAKLho+eVerJJcK05oKQZTK2J587L007pmwsZj7oCeCBuhu9
e8yi2QmdkPNA7bNfSdj25AkDx6WVxjgk0fUOJVw3pDclG4stQFE4IkBYQ/dKR3A/
yIiIFk9yfoNe8FbFi2pc06lSzSyxYkAlQMFEDI SCKCr/we0RvMhLQEBqHcEAIRk
R68Y5vBCXE4/gGy9QCQwARMV/rUhSo8b4/NmDJJR9Dain5W35eZ79AJq0Aszak
5c+/5Yvig/LcAtlKpfgWj0W8nKU0sTphWHAHv+VvlYngyyj/ARqUsdAUrPX+aOdQ
RzesuR/8F3+dSAPjgomh5B5wHLLIor5vODUqstCKiQCVAWUQmHq9NOglSuMPTJd1
AQQG5gQAlVyqyjaEKlZhbGhd/HBA7+FKVuv+bGIKW4T733ZxCO7RTa5yC16EgqA
wfgtWKsezEGRe2r2mwfQkf4G8I fbdOcsTrSWVOGHngfiqXa021iY8IzOkXrdrB/Q
nsStQ3YTMpfFoLrhRcuB8MzSnXenhPtqBoh1kKmHEIhKXCKNC2JAJUDBRAYEwwp
KG4sKaQ69XUBAfFkA/9+TPN9QtjwYyUwztssE5BXnVmXP4Rr1j+w+DSM0clUedo
2dBQ2xlEBIOQHDwZnIMSVsKuTCVbvmeF9qNYjLxkykw+eK32MhC1aTeG/PXz006
EuBF8vJniG79NirFqyKo6oyp4grrlcj+CaUfPqnws9QvX1YrExlV40bkiUCFx4kA
1QMFEDIUOBTABXqtD54luQEBwysD/RhNPmoXXlBj7+MIcHh2oC04LrHkhKsWQeV6
kMnK7KrQyHzKqrdJBK4zik3bcgnmlcxFEeEji7ejxc/llD8fRBqAP4PK+64bFT
BfQdeyG3VkmZHHH2GHo0Ffc17+U5U3kmJyc364WVQCs6XbaB2/OVnPd3pSjB0Tmj
KQhIRI+giQCVAWUQmHjWlUA9vVUYMjNJAQF0IAP/Vf1M6cSirdeHKNQcuxAy4CvX
2m/y1SkNrtAk1bWVChaB1Rn7ehWPsPRWhnVhEJrZv2ah7Q/OI/dihWpxU3LcNvyY
HhmPzazjUwX+v/6XcdUv4JNVW/ZKld+4sJG1jNTt3coYp9SDzkySas0Cky/dhOry
L2OMeE7cgK/dIm04NVOJAJUDBRAYE3vNiNG5F26PPVUBAWtDA/9V3HmlE/K/xZcR
F5ju/PakdTzNWx/IdbzPFrbGRj21CclDgBjlpTh2ZwrNw8QFKcHDSYBqYc+I8sMP
3eP4DaLNXiRBzk5ggTDb9cmLHERz8dmRXe7LduwSb2Vw+d37Zoo7R6RoXQy42m66
lzHasp4jQWYTs6wEeeJMEMTgqIQFIkAlQMFEDITY+4cCIJbhc/GQQEBXxkD/2dZ
90z1O51Td27WvgIudMs9CqN/WoZOFARSFY28vDjgSRz3jCcrAJz0UrQg3vK0NGBl
UfOIYE3JGK8unKLjAkVbVAVvx7ID2UVA5AM9Lp3ILviL9679ftam8GxQApH0D+y
C1ScG+GT5f+Wh6HV+IZGgw+3fbOTLqp8zLYKaEaaiQCVAWUQmHMD8yh9+71yA2DN
AQFb/gQAguxR1sLvq0GuEugrhPMwkaql7KTib6VoWCpQdXYDQfmSnwcZyz5nvdMt
v49ZySswNE6xjzPRHJPTTg+N44xZ3IcCe9QoLG+ZLEaK+pAVoXk01hxKx7YMBZF
hyrjvpXuaUuwqhIYdGRpw3sB/C5vDfjbkuQVHoa9qv6Vn/7B1ZSJAJUDBRAYEv8A
H9vgQ8ZSyXEBAUxgA/9rkTrp815ypKyvWf0xtjBEGuzQcHIUdS7FH7UtBcYXPSwY
VVvIy2h9kPAMZSGFT8+LP9z/dbMvRen9gZM08PO6VDrVCje+CNREYBTyYp4d0H5M
rOortmtXxQZ8HQWBalTIhAmZgnZbkvL74vD2D/dJtPaA400vjTOU+MH//5o4kA
1QMFEDISGwEJn15jgpJ0QEBEvQD/jv96wv9PFf8+ObMABvFQD01dG9Gxcm9kiVE
kXkUnio5+sSyd/tFz75lBiyoVsXBhlagSRi8115MxKC6faXwlQk1uhaWvIzZJISQ
G5x4XjAde1Z/yEIH12lhDAGFB267p/5+1T2/OjVgAJegWVQlPafbh0TWiyQBbJc
qzEM+Q59iQCVAWUQMa+ck/VKfLHHWKDtAQG+RAP/YiyTH8VCjyCpsJFIyauWvaBj
89kntQB+7s4W55jeuk3F06m4WEr56ng16ZmUwgnQRAQxzw+eYpfrbFrm4XnARSS2
41E2Vv5wrntCoPsAxuta/aOp3LUS/5Rr20ybay3cz+toM6x5bXEGHsGCglKh0G11
nzLsP3yVY1xW51ycmgyJAJUCBRAXGFF00T0f3h0/fEEBAUbtBACZSQ23ccH1k2Q8
0mdrAf/xuNQ/WCcxZwulLeJrLAKAPQIOM6u4ZO1TPPTEwmtFsCvagHgbZBCW4Mz
wcuK22aa+Ntm1qMgrC1MosZZCUGb9Ut+ui6bV4o8pnWtGE4JsV4j6O4WJ60wc/tb
M35/8STTln3F4qNZJ7txmYruEonyUIkAlQMFEDeYbuNF7olX4zT+YQEBD2AEAIzg
LVwH6GE08BlLggrPxNdGah8UdPQlyy7W0gflyolywfmfbftoly8cjh/te3+6qOCyL
0/ijSLKRm9KUCVORGOS40F7jjMY375/4NPmsES36QpL+e+OLS4t3Joe6yggQ9Kw
6588DmXlb3kIKg2ZY70e035oeGAGecFGwAPal8AQiQCVAWUQmDfLENH6sbnW3Io9
AQE23gP+PKs7HyMv/QO1vGAIwJ35yWzY0EadGmnpWareUA6LdWAjfK9pCfagKUac
Ztm4bKdhKGBLES0ayKvLRDnxaIRoreB1qYc11CdQKm9K3qQkzmeqiZEGjWlCuAoy
z2fH1HT2Y7X8aMfELxHRdzy4up+J49TlZrZ+2Z0Yksh/dhYbvv2JAEYEEBECAYF
AjhdTf0ACgkQVfe6KqApYzpp9gCfTG30iR04XvuTpZjCEpacvJolfdMAnj+Bqkq1
mCY1u/C8x7L9MBh7WxERtAVzaW1vbg==
=F3pU
```

-----END PGP PUBLIC KEY BLOCK-----

Yaron Aristo

-----BEGIN PGP PUBLIC KEY BLOCK-----

Project:	GN2
Deliverable Number:	DJ2.3.1.1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3

Version: PGPfreeware 6.0.2i

```
mQCNAzhC9a0AAAEELDer0NLOWFv/s+vuXHQefeCLOJVB/L/dQVaTaqDutPvDAiOd
rUoyflo/1tWrhiwSF23glGOvzDirClKkaj/w5Nzx6IF0GrkyTQVyex+47bdbX390
tZ3mnrkoFplpoUsQ/yXm2E4LatV8AXcN9OL3u9FJG3xq+04wo5JmXDbYOvqNAAUR
tBZ5YXJvbkBhcmlzdG8udGF1LmFjLmlsiQCVawUQOEL1rZJmXDbYOvqNAQH8ugP9
Emn0KhqEYSjik+nfFDL0ZF7CsJ4pWf20MAz0pB3DMMLzb7X1eLsgkfV7zd6dHI8S
bRmqjJMDnQyddX9AvLGMijxIXYFxB5zviCKIwwfW6JpZBlFTof4vEBWbpf/qFoe
h/ZJj9BN3zh7rrX25Vn9pkKQTYCbWdDpRIAhihyfeo+JAEYEEBECAAYFAjhdTaoA
CgkQVfe6KqApYZr+9wCgyCyd9Ie3K5lHdcVGVZVCYTBM3EAn1jSYFp99L/SWEIp
aclju8gLyLjJw
=Dhdy
-----END PGP PUBLIC KEY BLOCK-----
```

Ariel Biener

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i
```

```
mQGIBDqz+hURBADRRbNSFanUB1te2xT8HJ18CP0FtKTnp1U6d3qh3jpr2ALr62Rk
St5O5oi9qyVXC38ZB1YzAR50hcGPqAQJyXtXcC4BqeLNoWtDzZmPqgK5H4U6jZgU
2pHcAOu4RcNN6L4PCDVpuLFu6n7nRVfTK0zuNDV2bSncO31sgeiKJ4M2vwCg/56p
xTnEM2u3BXRxs1HhYw3o9UD/jfj11HBFlecKL4YuHR8QfnxElcBB42g2iRsgcTt
iJ4e5AoDycLA7QVKJJD6K051xCCbndEqQ8o6iEDY9DcRmKeQWmbJYq9WpwW7Jzti
gDYpJ7gCYrLm3A87gb1oBoXsQXAUyGRvAgMAVxrl5ePCGllmhRGMUk1o1YY1Phs
KYz9A/9hygwEY4XEBgROEyq4RFdknssBDVfg1gudd7SUP2poHHWnaQtXI3TOZ0lx
gpmi6f7t/pfdDXbaPfundUTA4KkC06JXA67k9nbcWs9EUpc0N72H6MZLBe5UukZZL
/LxDZF7ZmaOHeO92/X4KY18c1q4DCPIiObOfgSmQjwzYRLKxcrQjQXJpZWwgQml1
bmVyIDxhcmlbEBwb3N0LnRhdS5hYy5pbD6JAE4EEBECAA4FAjqz+hUECwMBAGIZ
AQAKCRBzpsXlc8Ek1itbAKDiuv+ouws6kp8Pyh2JMXYSH++B5wCepKGFfsEzS2C0
1GavH35HjRu88ziJAEYEEBECAAYFAjq0T8QACgkQVfe6KqApYZoZdQCg5v5GhyWB
QhuUpO3+nR/FOj57q10AoNXiDx47XOgCxa6Xc5acB91W/DfniQCcBBABAgAGBQI6
tPjJAAoJEPVKfLHHWKDtKRMEAOEaT1UQG7Ml6O1XaVE8NFNOkpbphsbgI4iPXX
9+PvfGgHx5b18//NG/s4BY8YwtBktVbnRYy3lg3FL5qnlgcXu0ThzajFUTLTI/K
D671Z/cBT06OfiCZa4590sCPSjuRtkten7lk0IYVoC3RGafqp6m5rpowld5/CGsh
Z2FriQCcBBABAQAGBQI6tRAKAAoJEAvt9E+5ZYFrWcd/3weTUp76eaA+bemN5kZ
Pl/PBZj85ojnzAsuNBWTTTlu/axunfX6kN9ns2k6O5dLonj1rdhg5Wb14uaXkzej
9+hDnOhYu1PhNhbXThLsd6TJN1CeQgFkYHUyl0eFkVGORVE2X3BKvt3/Kmpul5H
wE8jjzqQBukn/1rCOIfoyFeciQCcBBABAQAGBQI6tRA3AAoJEDHKG40FGkkRQUwE
AL5FH4vEJYW3pNL75DO8KbD8vIMd7MCptt3PrXcARYBrdLhbNRVAhtXkCKePfUe/
Cwk6oiNiMzj4NiZ+ez8y+8/OcuWzwPS02UuOWDgTAbOQzTC/hOUmd0090HunZHSn
j1SdvXiQY6ijp56VkrLY4xJaGc3a4qRhhzGhaEVwCUT3iQCcBBABAgAGBQI6tPwF
AAoJEDHKG40FGkkRSGwD/3hFyoQiVNZw4ZL8/NDw0dH6ghgczpNch6zEicDEpsGd
5xoVIrvIta6Tbsp2XHREvVLGTGJlKMkxq8HTGxIemxrSxz2wy7MPKJK0j/2Lrzh3
+dsA+fULHIoGDM5aP3MiQSwcHOFScxen3fSnETWicVFQPO8WPx1N+Zz0cq4eeQO2
uQINBDqz+hgQCAD2Qle3CH8IF3KiutapQvMF6PlTETlPtvFuuUs4INoBp1ajFomP
QFXz0AfGy0oplK33TGSgsfgMg7116RfUodNQ+PVZX9x2Uk89PY3bzpnhV5JZzf24
rnRPxfx2vIPFRzBhzJZv8V+bv9kV7HAarTW56NoKVyOtQa8L9GAFgr5fSI/VhO
SdvNILSd5JEHNmszbDgNRR0PfiizHHxbLY7288kjwEPwpVsYjY67VYy4XTjTNP18
F1dDox0YbN4zISy1Kv884bEpQBGRjXyEpwpy1obEaxnIByl6ypUM2Zafq9AKUJsC
RtMIpWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAICCADwvGluYsKqzJUxQrxEruxe
```

Project:	GN2
Deliverable Number:	DJ2.3.1.1
Date of Issue:	26/07/06
EC Contract No.:	511082
Document Code:	GN2-06-150v3