GRID SECURITY WITHIN French NGI

France GRILLES International Advisory Committee
15 & 16 MARCH 2011

Dorine Fouossong, NGI security officer

Table of content

GRID SECURITY WITHIN French NGI

- Security problem description for french NGI
- Security Policy
- Security Operations

Introduction

Grid computing aims to involve everyone in the advantages of resource sharing and the benefits of increased efficiency.

According to the french government notices on information security management, resource provider should protect resources against illegal use. As special case, there may be usage restrictions in the context of non-proliferation rules.

How does NGI France guarantee that non-proliferation regulations, are applied?

- **Security problem description for french NGI**

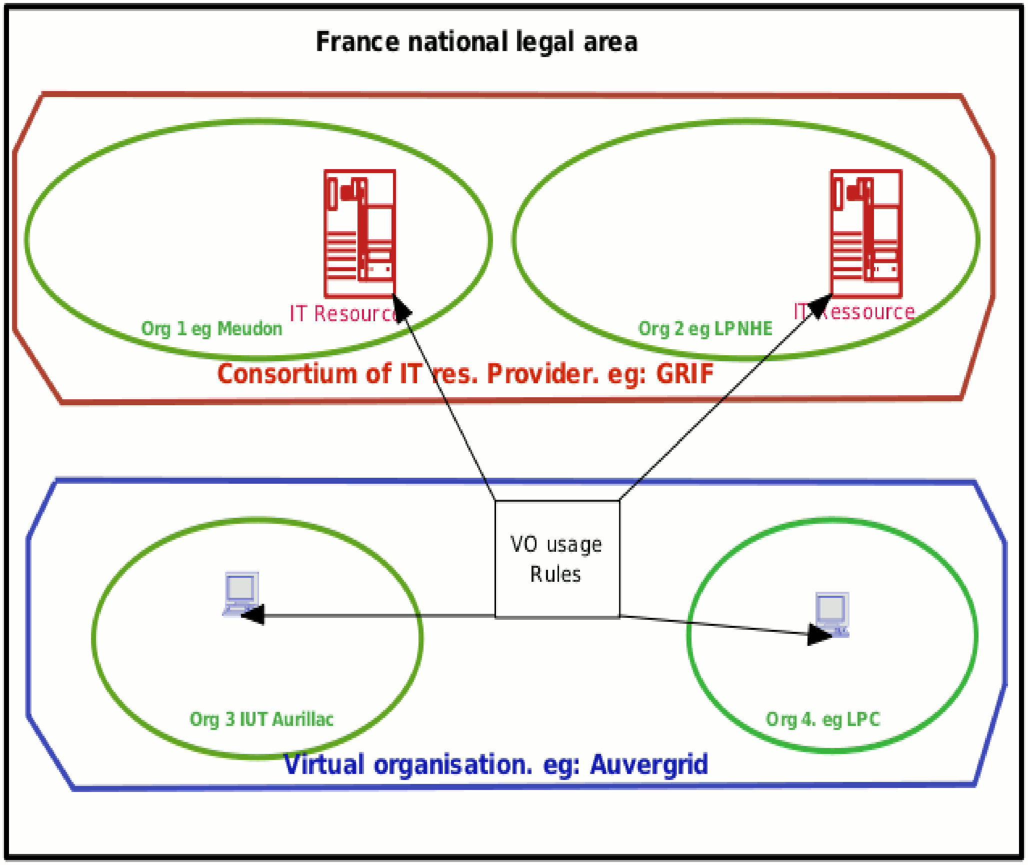
Non proliferation issues for the NGI

The distribution of computing resources can be described in three scenarii:

- Local distribution. IT resources are under the governance of one organization within the country. (ie cluster of the University of Lille).
- National distribution. We consider all IT providers participating to France Grilles. They are under the governance of several distinct organizations within the country like CEA, CNRS, INRA,etc
- International distribution. The scenario corresponds to the participation to EGI : IT resources are under the governance of several distinct organizations distributed among EGI partner countries.

The first scenario is not specific to grids. The two last scenarii are more specific to a distributed environment and we will see that they raise some problems.

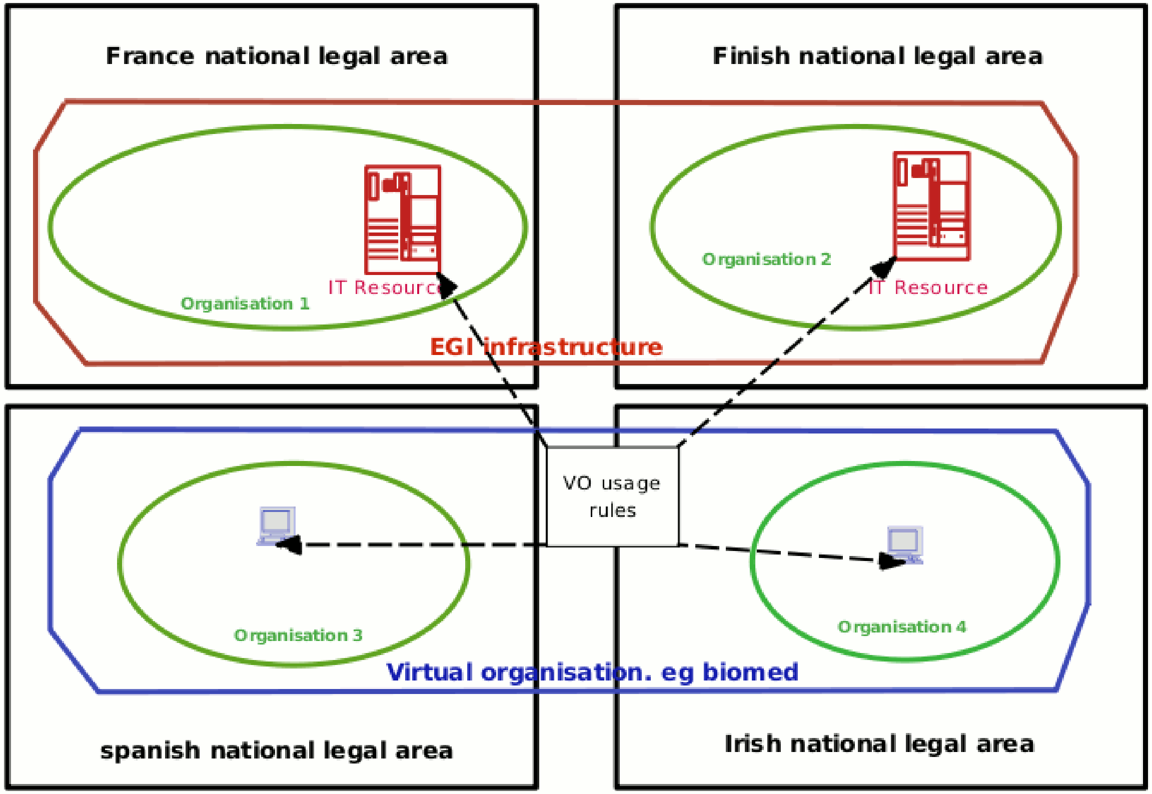
Scenario II: National distribution


France national legal area
IT Resource
Org 1 eg Meudon
Org 2 eg LPNHE
IT Ressource
Consortium of IT res. Provider. eg: GRIF
VO usage Rules
Org 3 IUT Aurillac
Org 4. eg LPC
Virtual organisation. eg: Auvergrid

Dealing with non-proliferation rules would then be dealt with the contractual relationship between the VO and the consortium of resource providers.

The final responsibility for ensuring the compliance with non-proliferation rules lies with a VO « responsible person » . He/She is the only person who can evaluate whether user activity comply with the scientific context of that given VO.

Scenario III: International distribution


France national legal area
Finish national legal area
IT Resource
Organisation 1
Organisation 2
IT Resource
EGI infrastructure
VO usage rules
Organisation 3
Organisation 4
Virtual organisation. eg biomed
spanish national legal area
Irish national legal area

Non-proliferation rules would be addressed through the contractual relationship between the VO and the consortium of resource providers.

The final responsibility for ensuring the compliance with non-proliferation rules lies with a VO « responsible person » . He is the only person who can evaluate whether user activity complies with the scientific context of that given VO.

Problem arising from scenario II and III

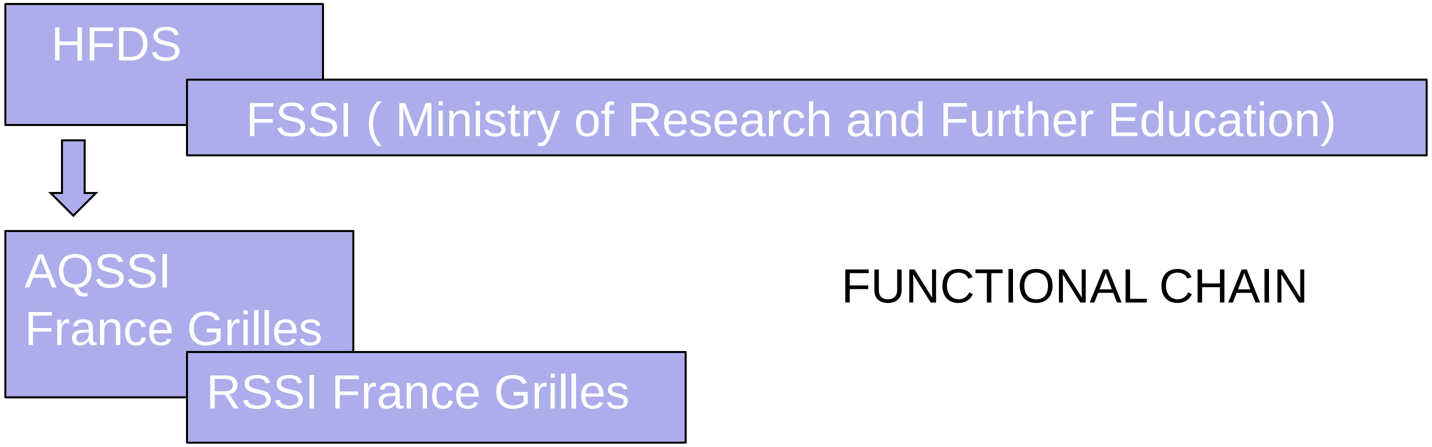
What does in legal terms define a VO? What is the liability of a VO?

What is the minimum necessary for the formulation of a common legal framework for the contractual relation between a VO and the consortium of resource providers covering UN Security resolutions and embargo decisions?

What is the liability of a « responsible person » ?

- **Security policy**

National landscape of information security



HFDS

FSSI (Ministry of Research and Further Education)

AQSSI
France Grilles

RSSI France Grilles

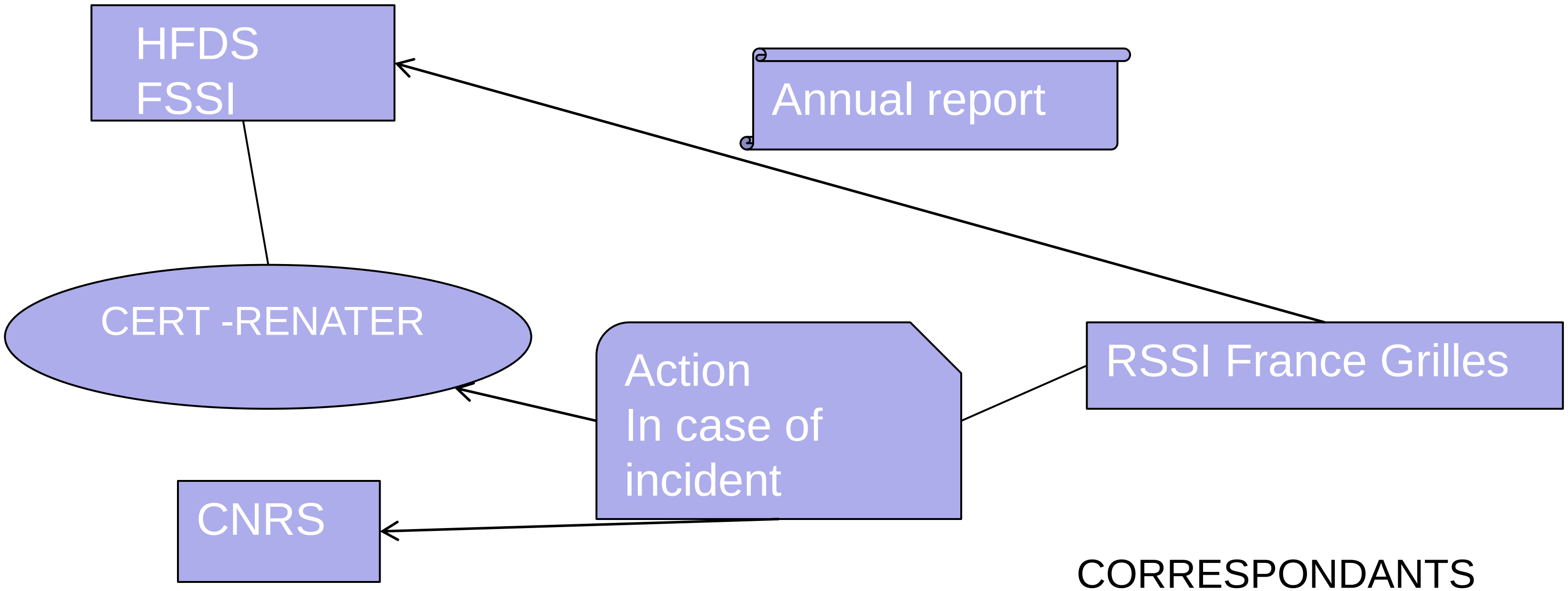
FUNCTIONAL CHAIN

HFDS: Advisor for the prime minister on all matters related to defence and security.

FSSI: appointed by ministry to work with HFDS. She ensures security policies are well applied (France Grilles).

AQSSI: In legal terms, he/she is responsible of the security of an establishment (CNRS).
RSSI: Assist AQSSI. He is in charge of management of information security.

National landscape of information security



CORRESPONDANTS
IN INCIDENT HANDLING

CERT-RENATER is also our national NREN.

Key objectives

Mitigate the risk inherent to grid technology.

The following risks are not acceptable and should be avoided:

- (K1) A criminal gains political profit from the misuse of computing resources.
- (K2) The project can’t manage a widespread security incident.

The following risks are important and should be reduced:

- (K3) A France Grilles partner gains evidence that its data have been hacked through the grid.
- (K4) Disfunctioning or unavaibility of Incident communication channels.
- (K5) Lack of resources involved in grid security activities.

Key objectives

Ensure alignment with GIS priorities:

- Build a safe and sustainable infrastructure
- (K6) Improve support to scientific community
- (K7) Promote and integrate cloud computing

(K8) **Cooperate with EGI security teams:**

- Collaborate to grid security incident handling
- Help improving security policies
- Contribute to development of security tools

Organisation

- **Security board**

A forum for information security coordination. It includes representatives from all France Grilles partners.

Mission:

- Set security direction, make key decisions and provide final approval of NGI policies.
- Conduct periodic meetings to monitor progress and issues
- Coordinate approval from executive committee when necessary.

Organisation

- **Security operation group**

A forum for information security operation. It includes security contacts from all NGI’s certified site.

Mission:

- Develop and maintain security policies and procedures.
- Manage and control security services.
- Support incident management activities from a security perspectives.

Status of NGI security policy development

There are some NGI specific operational procedures

- (M2) CA distribution update procedure which addresses non-proliferation issue.
- (M3) Security incident handling procedure which addresses our specific workflow that include CERT-RENATER (the french NREN) and the NGI security alert channel.

Plans for next year are to

- (M9) Document a formal NGI security policy.
- (M10) Develop a groupware for NGI security team.

- **NGI grid security operations**

What has been done so far?

(M1) **Security communication channels have been set up**

- A channel for discussion, 30 members from all the 17 production sites.
- A channel for security alerts handling.

There is a separate channel for alerts so that we can ensure messages are processed in time.

What has been done so far?

(M4) **Improvement of the site certification procedure**

- Security verifications are handled by the NGI security officer.
- There is a security drill that tests the knowledge of incident handling procedures, logging policy.

What has been done so far?

Improvement of training tutorials

- (M5.1) Materials for security sessions should be approved by the security officer.
- (M5.2) Agendas now include dissemination on grid security risk and policies. There are differents focus basis on trainee function.
- (M6) Dedicated session for system patch management.
- (M7) Focus on proxy renewal management and data encryption with glite-hydra..

What has been done so far?

(M8) **More resources are dedicated to EGI security**

- Involvement in security monitoring group : development of the EGI security dashboard.
- Involvement in IRTF : duty rotation, operational security procedures.
- Involvement in security drills: communication/documentation.
- Involvement in Security Policy Group.

Plans for the next year

(M11) Deploy a central pakiti to monitor patching status,

(M12) Deploy a central argus Policy Administration Point to control access policy.

(M13) Participate to a NGI of cloud computing study group.

(M14) Prepare an EGI security training as part of EGI-CSIRT activities.

Conclusion

We have made many progresses in the last year.

- ✓ The number of incidents is decreasing.
  - Hosts affected by an EGI-Critical vulnerability decreases from 2 per month to ¼ per month.
- ✓ Critical Patch application delays are decreasing.
  - Delay decreases from 10 days to 4 days.
  - Number of sites having a patching status monitoring tool installed increases from 1 to 5.
- ✓ A query shows that sites are happy about communication channels.
- ✓ New sites find the certification drill useful to gain experience on grid security administration.
- ✓ The cooperation with CERT-RENATER makes great improvement in support for security administrators.

Conclusion

The following matrix shows how measures taken fit with our key objectives.
In blue, you have the current status. Improvements scheduled for next period are in red.

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14
K1		🟦	🟦	🟦	🟦			🟦	🟥	🟥		🟥	🟥	
K2	🟦		🟦	🟦	🟦	🟦		🟦	🟥		🟥	🟥	🟥	
K3				🟦	🟦	🟦	🟦		🟥		🟥		🟥	🟥
K4	🟦		🟦	🟦	🟦			🟦	🟥	🟥				
K5	🟦		🟦	🟦		🟦			🟥	🟥	🟥	🟥		🟥
K6					🟦		🟦		🟥	🟥			🟥	
K7					🟦			🟦					🟥	🟥
K8	🟦		🟦	🟦	🟦			🟦					🟥	🟥