|  |  |
| --- | --- |
| **Meeting:** | Security Policy Group (SPG) |
| **Date and Time:** | 31 August 2011 – 14:00-16:00 |
| **Venue:** | Telecon |
| **Agenda:** | <https://www.egi.eu/indico/conferenceDisplay.py?confId=575> |

Participants 2

AGENDA BASHING 3

MINUTES AND ACTIONS FROM JUNE 2011 MEETING 3

ITEMS OF BUSINESS 3

Editorial team: VM endorsement and operations policy 3

AOB 6

Date for Next Meeting(s) 7

Actions 8

# Participants

|  |  |  |
| --- | --- | --- |
| **Participants** | **Abbr.** | **Organisation** |
| **David Kelsey** | DK | STFC SPG Chair |
| **Damir Marinovic** | DM | EGI.eu Policy Development Officer (Secretary) |
| **David O’Callaghan** | DO | TCD |
| **Riccardo Brunetti** | RB | INFN |
| **Romain Wartel** | RW | CERN |
| **Tiziana Ferrari** | TF | EGI.eu COO |
| **Steven Newhouse** | SN | EGI.eu Director |
| **David O’Callaghan** | DO | TCD |
| **Jules Wolfrat** | JW | SARA |
| **Antonio Perez Perez** | AP | CERN |
| **David Durvaux** | DD | BELNET |
| **Christos Kannelopoulos** | CK | University of Thessaloniki |

AGENDA BASHING

DK presented the agenda points. The main focus of the meeting will be discussion about VM endorsement and operations policy. There were no objections or additional points from the participants.

# MINUTES AND ACTIONS FROM JUNE 2011 MEETING

Minutes from the previous SPG meeting held on 14 July were approved.

DK checked with other SPG members the action list from the previous SPG meeting. Closer review of actions will be done on face-to-face meeting in Lyon. Several actions were closed. See the table at the end of the minutes for more details.

Concerning action 04/01 Check *what would be the most appropriate time to address changes to SPG ToR* DM provided an update on this action. First ToR amendment we already discussed and agreed upon on the last SPG meeting. The suggestion was to add one more sentence to ToR Section 5.1 Membership original article: *Each participant and associate participant of EGI.eu is entitled to nominate one voting member of SPG.* The suggestion is to add: *In addition, legal entity representing external Resource Infrastructure Provider that signed MoU with EGI.eu is entitled to nominate one voting member of SPG.* Second ToR amendment requested by SN is to include possibility for a policy group to appoint task force. Therefore, suggestion is that within Section 3 Purpose and Responsibilities we replace point: *SPG may create special focused sub-groups to tackle specific issue* with introduction of subsection 3.1 Appointment of a Task Force.

DM will send proposal to SPG members and to give them time to make comments until face-to-face SPG meeting in Lyon. DM will send ToR with draft amendments to SPG mailing list ***(action 05/01).***

# ITEMS OF BUSINESS

## Editorial team: VM endorsement and operations policy

DK: Aim of this meeting is to finalise the "external" draft and get it ready for wider distribution

RW: We got feedback from SN, JW and Andrea Chierici. RB had earlier answered most of the questions asked from Andrea Chierici.  He was happy with the feedback he got from RB.

1st SN comment - Endorser Definition: I see endorsers being appointed by the the infrastructure in addition to VOs and Sites (resource centres now...). The comment was accepted as valid and clarification was provided.

2nd SN comment - Third Party Definition: This is used in the document but not defined. RW: It’s a Valid point DK: It is extremely complex , I do not how to simplify it. JW: If it is third party acting as a Resource Center (RC) why should you have different policies for third party? There is no difference. DK: VM operator is VO person, RC is running the services. Third party means anybody other than RC. JW: Suppose I am user I will have the same expectation and same obligation whenever I am running the job. RW: Third party cannot be bound to our policies. DK: According to draft [Service Operations Security Policy](https://wiki.egi.eu/wiki/SPG:Drafts:Operations_Policy), they are bound by our policies. Third party could be anybody. RW: How would you define a Third party? DK: Third party is not a RC. RW: They are not bound by policies like RC? DK: It is better not to say it explicitly in the draft, it will be defined in other policies. JW: Only somebody who behave like RC can be a third party;  should you not require from the VM operator in case of a third party accepts the same agreements and policies as a RC? Third party is not a legal entity and RC is a entity? RW: Party does not have administrative control. DK: We must also include the case where one RC produces the VM image and another one operates it.

3rd SN comment - In "Endorser: Third party, VM operator: resource centre" reference  
is made to section 3.3 which is not clear where this is. RW: It is fixed. DK: In 2nd use case do we need first sentence? In all use cases first sentence does not say anything more than title. 2nd use case still involves case when third party can be RC. Definition of Third party as an entity not RC, where images are operated. Definition is finally agreed - *Third party: An external entity other than the resource centre where the VM is operated.*

4th SN comment - In Policy Requirements point 4 - what is the Image Catalogue document? Where is it defined? RW: There is dependency order on some other documents, it is difficult to track. DK: I would just delete reference, ICD is procedure I would just delete it. RW: Agreed.

5th SN comment - The phrase "full list of OS/packages/versions in VM Base Image and VO Environment" seems to be tied to a particular OS types and VM usage/preparation model. It is not clear to me what is  
the policy requirement that needs to be conveyed here? DK: This phrase came from some old policy documents. DO: I agree with SN, it would be very difficult to enforce, if it is a big list. We probably don’t want to include full file listing. RW: We really want to know where are the images we run. We don’t need more than revision of OS. DK: Endorser needs some endorsement, they need to know version, if it is part of their endorsement. They just need to keep audit over this. I suggest to define it as all OS and other installed software security patches. DO: They are not VM images, it’s not a VM. The sentence is rephrased.

1st JW comment - I have a problem with the different use cases. I think that it makes a difference who is taking the two roles, so I don't think that the same rules can apply independent of the use case. For instance a resource center can be a legal body and already can have agreements with NGIs, etc. about their obligations. In another way expressed, should you not require from the VM operator in case of a third party that it will accept the same agreements and policies as a resource center? Then I can agree for instance that a team will be responsible for the VM operator role. It is in the first place the user that must trust the VM Operator. JW: We already discussed this issue partially. Whole policy framework is first addressing users of resources, not RC, just have a user agreement with Third party. RW: It is important to notice it is complementary with other policies. Other policies still apply. JW: There is no reference to other policies. DK: Maybe we should put text to each policy referring to other policies and mentioning them. We should define General statement in introduction part of every policy ***(action 05/02).*** JW: As a user I want to know what can I expect and who is providing trust. DK: Purpose is to enable RC to run VM endorsed and operated by Third parties. JW: Normally RC have agreement; could provide access to other users RC needs; different contract agreement with users. DK: Much of this is covered in different documents including other draft we have - Service Operation Security policy. Have a look at this draft policy. RW: Perhaps the solution would be to make more generic version and to apply it to more generic framework. This version depends on other policies. Maybe some more generic version is needed next to this one. DK: It is all covered. We need some additional text in introduction. JW:   
Who can use this, who is suppose to accept this. It should say that it provides obligations to the end users, maybe it is addressed in other documents but than it should be clear. DK: I don’t think it is about end users. JW: If it is not for end user than we need separate documents between user and provider. RW: This is very valuable feedback and this discussion would be more suitable for the upcoming Security for Collaborating Infrastructures meeting (SCI) , not an SPG meeting. DK: It also very much depends how do we define users.

2nd JW comment - Rule 8 for the endorser about the requirement for a security vulnerability assessment process in place: what requirements are there for this process? There should be some minimum requirements for this. JW: We should have an example or minimum requirements. RW: As long as you have something in place we are fine, process that is publicly available and on demand. JW: Vulnerability assessment is different subject, but there can be examples. It must be documented that assessment is published, what is the outcome. DK: We have in mind that you need to check whether there is most up to date version. RW: It is not assessment, it is about patching. We should replace assessment with patching. JW: Yes, I agree. DK: OK. It is done.

DK: All known points addressed. RW: Yes and we had very good feedback and discussion.

DO: We need to discuss whether the Endorser must sign a list of endorsed images or can the metadata for each image be signed. I would like that this policy change to also allow digitally signing endorsed images not lists in order to be in line with the StratusLab implementation; this has a deprecated field in the image metadata to allow revocation. RW: My proposal will be to keep everything in the policy as it currently is. DK: Signing the metadata, not the image itself; sign a list or metadata. RW: By having a signed image list it is easy for the consumer to check that an image is still OK. Metadata signed by endorsers is more difficult. DO: HEPiX implementation is compatible with this implementation. RW: All the users are reasonable and security aware. StratusLab cannot provide these capabilities. Everything in the list is up to date. DO: With an incompetent endorser, I don’t see the difference between he/she not updating a list of images or not updating the image metadata. DK: Is there an assumption that we only allow **one** signed list per endorser, if not, perhaps we should enforce that. RW: I am concerned that any change to the wording will weaken and undermine the policy. I am not happy and operation people will pay for it. It opens possibility for endorser to leave some very old images. DO: There is a policy engine you can specify which endorser you trust and any other requirements you like based on things from metadata. You can stop trusting them. RW: In theory yes, but in practice it will be difficult **(**

Point 5 is finally agreed and changed. We agree to allow for a list or signed metadata and we do not limit to just one list per Endorser - *Either the list or each individual image's metadata must be digitally signed by the endorser.* Point 11 changed to *- You recognise that if a VM operator runs an image which is no longer endorsed, you are not responsible for any consequences of this beyond the time of your removal of the endorsement.*

DK: Shall we go for external draft? I need to put it in MS Word format and store on EGI document repository. External feedback doesn’t stop SPG members on continuing to make further comment on the draft. Do SPG members agree that the draft is ready for external draft? It is agreed. DK will produce word version of the draft and upload the draft to EGI document repository ***(action 05/03).***

## AOB

DK: Are there any additional points?

TF: Yes. We have a problem is that VO DREAM can’t be registered in Operations portal (http://operations-portal.egi.eu/) because VOMS server where VO DREAMS is hosted can’t be registered to a GOCDB registry (<https://goc.egi.eu/portal/>). This is because it's located in US and there is nothing like NGI\_US. VO DREAM can’t be registered because their VOMS server where VO DREAM is hosted is in US and Operations portal of EGI (VO registry) pulls VOMS server automatically from GOCDB and VO DREAM can’t find their server in that list because they can’t register they VOMS server in GOCDB by mentioned reason already. If you check GOCDB registry they are hosted by ROC sites that closed operation couple years ago. Therefore, in some of the fundamental services are operated by external partners. Is that acceptable scenario and what are the boundaries? DK: Good point, we need to have a look at the current policies. TF: If VOMS services are compromised, what are the implication for EGI? DK: VO registration policy is stating that they are bound to our policies. This is something that we need to thoroughly review. DK: We should continue discussion on this issue come on the SPG meeting next week. It is important point and also a general one. It is general issue and it needs to be discussed in SCI where we are talking with our collaborating partners.

## Date for Next Meeting(s)

DK will create doodle pool for the next SPG meeting (to be held before the Technical Forum in Lyon) that will discuss [Service Operations Security Policy](https://wiki.egi.eu/wiki/SPG:Drafts:Operations_Policy) ***(action 05/04).*** We need to address the feedback and go for actual approval and follow PDP. Short face-to-face SPG meeting will also be held at Technical Forum in Lyon on 20th September.

# Actions

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Resp.** | **Description** | **Status** |
| **01/02** | DK | Invite all EGI.eu Council participants to nominate a voting member of SPG | ONGOING |
| **01/04** | SA | License statement, to make more compact and explain how external partners should mention it | ONGOING |
| **01/05** | DG | Provide English translation for Dutch data protection law, art. 35(?) | ONGOING |
|  |  |  |  |
| **01/07** | DG&DK | Go through digital agenda items related to trust and security | ONGOING |
|  |  |  |  |
| **01/09** | DK | Get rid of “site registration security policy” at the same time as the updated site operations policy is approved | ONGOING |
| **01/12** | DK | Ask TERENA if they have policies in the area of cloud to be considered as base for new top level security policy | ONGOING |
| **02/01** | DK | Ask members to check whether their entry in the membership list is correct | ONGOING |
| **02/07** | DK | Investigate whether the document Security for Collaborating Infrastructures (SCI) overlaps with existing CSIRT agreements | ONGOING |
| **02/08** | DK, SA | Investigate possibility of involvement of Balboni during SPG work on drafting the Data protection policy and what we could offer to him | ONGOING |
|  |  |  |  |
| **03/02** | SA | Ask Steven Newhouse about possible mode of collaboration with the PRACE | ONGOING |
|  |  |  |  |
| **03/06** | DK | Have a look at potential terms and definitions conflicts that are currently present in the common glossary draft | ONGOING |
| **03/07** | DK and PDT | Define terms and definitions that should be included in the Common Glossary after the Service Operations Security Policy is finalised | ONGOING |
| **04/01** | DM | Check what would be the most appropriate time to address changes to SPG ToR | CLOSED |
| **04/02** | RW | Send draft to HEPiX and SPG mailing list to ask for comments before 5th August | CLOSED |
| **04/03** | DK | Schedule next SPG telecon meeting approximately for the end of the August | CLOSED |
|  |  |  |  |
| **05/01** | DM | Send ToR with draft amendments to SPG mailing list | NEW |
| **05/02** | DK | Define General statement in introduction part for every policy | NEW |
| **05/03** | DK | Create MS Word format of the VM endorsement and operations policy draft and store it to EGI document repository | NEW |
| **05/04** | DK | Create doodle pool for the next week SPG meeting | NEW |

Minutes prepared by Damir Marinovic, 01.09.2011

Minutes Approved SPG Chair David Kelsey

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

COPYRIGHT NOTICE

Copyright © EGI.eu. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

The work must be attributed by attaching the following reference to the copied elements: “Copyright © EGI.eu (www.egi.eu). Using this document in a way and/or for purposes not foreseen in the license, requires the prior written permission of the copyright holders. The information contained in this document represents the views of the copyright holders as of the date such views are published.