|  |  |
| --- | --- |
| **Meeting:** | Security Policy Group (SPG) |
| **Date and Time:** | 14 July 2011 – 14:00-16:00 |
| **Venue:** | Telecon |
| **Agenda:** | <https://www.egi.eu/indico/conferenceDisplay.py?confId=548> |

Participants 2

AGENDA BASHING 3

MINUTES AND ACTIONS FROM JUNE 2011 MEETING 3

ITEMS OF BUSINESS 3

Editorial team: Virtual machines endorsement policy 3

AOB 5

Date for Next Meeting 5

Actions 6

# Participants

|  |  |  |
| --- | --- | --- |
| **Participants** | **Abbr.** | **Organisation** |
| **David Kelsey** | DK | STFC SPG Chair |
| **Damir Marinovic** | DM | EGI.eu Policy Development Officer (Secretary) |
| **David O’Callaghan** | DO | TCD |
| **Peter Solagna** | PS | EGI.eu Operations Officer |
| **Riccardo Brunetti** | RB | INFN |
| **Romain Wartel** | RW | CERN |

AGENDA BASHING

DK presented the agenda points. 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 16 June were approved.

DK checked with other SPG members the action list from the previous SPG meeting. Several actions were closed. See the table at the end of the minutes for details.

Concerning action 03/01 DM suggested adding 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.*

DM will check whether it would be more appropriate to address changes to SPG ToR in a time of mandatory yearly review or for the next SPG meeting together with some other potential changes that will be proposed by Steven Newhouse (***action 04/01).***

# ITEMS OF BUSINESS

## Editorial team: Virtual machines endorsement policy

DK: Discussion of the current internal draft is the main focus of this meeting. Peter, did you have chances to look at the replies to your comments? PS: Yes, I had a chance ad I am happy with them. DK: We don’t have recorded some answers for Ricardo points. RW: We answered them I will record them on wiki. DK: We should record the discussion on the wiki page according to the MS209. I put it on discussion page. DK: Can you move discussion part to the designated discussion page? RW: Yes, I will do it. DK: We uploaded to repository when it is ready for the external draft stage.

DK: We had HEPiX virtualisation group meeting. RW: There was small discussion about the draft, few comments about wording, clarify some definitions, no major comments or issues raised. DK: Whole idea is for this draft to be replacement of HEPiX policy, we don’t want two separate EGI and HEPiX policy, everybody agrees that we need one integral policy; definition of endorser and VM operator were commented. RW: There was request from HEPiX to define them more clearly. DK: Do we expand endorser definition to include team. DO: we define endorser as role, and role can belong to individual and team. DK: One individual should be named and responsible for the team; individual and robot approve robot certificate, responsibility is on individual of a team; either individual or individual representing the team of people with endorser role, we want to name responsible for the team, not to leave that team in general is responsible. DO: I tend to agree, individual has to be responsible DK: We needed a name of the person of responsible, that does not stop team of people behind; the definition needs to include this notion somehow. DK: We would like to use grid certificate, another discussion to have in IGTF. RW: I am worried about privacy and technical implication, but we would like to work in line with IGTF recommendations; the draft policy says digitally signed not signed with your identity. DK: we should discuss with IGTF community. DO: Going back on the clarification of definition, I would suggest role held by individual or team. DK: We still want individual responsible; leader of a team? A role held either by individual or leader of a (small) team? RW: For me it should stay; it should be either individual or individual or a team. DO: Role who is responsible of confirming particular VM image?

DK: Under point 4 for the policy requirements on the endorser, do we have to emphasize it should be single list? Otherwise there is no chance of knowing which one is current one. RW: Still you need to have list of what happened. DK: They must be updated; we should discuss with StratusLab about the model. DO: I am happy to maintain this version for now I think we should have a technical discussion. DK: I think we are not ready to go for external review, we need to give time to HEPiX to make comments and have technical discussion; Roman can you send draft to HEPiX list and SPG list. RW: I can give a deadline for discussion HEPiX need time, I don’t think draft will change much but they need some time. To send draft to HEPiX and SPG mailing list to ask for comments until first week of the August (5th August) ***(action 04/02)***. DK: When shall we discuss this next time. DO: I can involve some major people from StratusLab. RW: To set a date for 3rd of August? DK and DO: It is OK with us. DK: After that we can schedule a SPG meeting for external draft. RW: It should be good to have detailed HEPiX feedback.

PS: I did not find in the draft any sentence about this policy applying to VM visible to infrastructure, site can build virtual network and VM they don’t need to apply this policy; we don’t care about visibility of VM from outside? Does the policy apply to VM that are instantiated from virtual network completely isolated for infrastructure? RW: Doesn’t refer to that all, what are the requirements for operator. DO: If you are running a private virtual infrastructure, do you still need to go to prescribed process in order to comply with the policy? PS: Endorser and operator are at the same site for example the case. DO: Even in that case you may still want to have list of endorsed images. DK: I don’t think it is the case; using images that are not endorsed. PS: I see your point. DK: Use case 1, should we make clear that none of this policy is addressed to them, do we explicitly want to say? DO: Site running virtual machines. DK: Less formal ways, use case 1. PS: Maybe I did not completely understand the first use case. We decided to leave use case 1 in the policy.

RW: I will replace some terms; “Grid” becomes “Infrastructure”. DK: OK, and please also replace “site” with “resource centre”.

## AOB

There were no additional points raised.

## Date for Next Meeting

It was agreed that the next SPG telecon meeting should be held approximately end of the August ***(action 04/03).***

# 

# 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 |
| **01/08** | DK | Harmonise security and operation terminology | CLOSED |
| **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 |
| **02/02** | DK, TF | Have a phone conference with Operations team before the EGI-InSPIRE review about harmonising security and operation terminology (related to action 01/08) | CLOSED |
| **02/03** | TF | TF should send approved Site operations procedure and OLA to SPG mailing list and check whether SPG agrees with them | CLOSED |
| **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 |
| **03/01** | DM | Propose handling of the SPG ToR amendment and actual changes to the document for the next SPG meeting | CLOSED |
| **03/02** | SA | Ask Steven Newhouse about possible mode of collaboration with the PRACE | ONGOING |
| **03/03** | DG/DK | Check what references should be added to the Service Operations Security Policy draft | CLOSED |
| **03/04** | DG | Announce a last call for any final important edit (Service Operations) | CLOSED |
| **03/05** | RW | Have a meeting of editorial team within two weeks and complete internal draft in two weeks’ time | CLOSED |
| **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 |
| **03/08** | DK | Set up Doodle poll for the date of next SPG phone conference meeting in July | CLOSED |
| **04/01** | DM | Check what would be the most appropriate time to address changes to SPG ToR | NEW |
| **04/02** | RW | Send draft to HEPiX and SPG mailing list to ask for comments before 5th August | NEW |
| **04/03** | DK | Schedule next SPG telecon meeting approximately for the end of the August | NEW |

Minutes prepared by Damir Marinovic, 15.07.2011

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.