| | |
|---|---|
| **Meeting:** | Security Policy Group (SPG) – Face to Face |
| **Date and Time:** | 12-13 January 2011 |
| **Venue:** | Amsterdam, the Netherlands |
| **Agenda:** | https://www.egi.eu/indico/event/263 |




## Participants

| Participants | Abbr. | Organisation |
|---|---|---|
| **David Kelsey** | DK | STFC SPG Chair |
| **Steven Newhouse**[1] | SN | EGI.eu Director |
| **Christoph Witzig (day 1)** | CW | Switch |
| **Sergio Andreozzi** | SA | EGI.eu Policy Development Manager |
| **Damir Marinovic** | DM | EGI.eu Policy Development Officer |
| **Tiziana Ferrari (day 1)** | TF | EGI.eu COO |
| **Peter Solagna** | PS | EGI.eu Operations Officer |
| **Jules Wolfrat** | JW | SARA |
| **Michel Drescher** | MD | EGI.eu Technical Manager |
| **Dorine Fouossong** | DF | IN2P3 |
| **David Durvaux** | DD | Belnet |
| **David O'Callaghan** | DO | TCD |
| **Christos Kanellopoulos** | CK | University of Thessaloniki |
| **David Groep** | DG | Nikhef SPG Deputy Chair |
| **Sven Gabriel** | SG | Nikhef |
| **Mingchao Ma*** | MM | STFC |
| **Reimer Karlsen-Masur*** | RK | DFN |
| **Nuno Dias*** | ND | LIP |
| **Riccardo Brunetti*** | RB | INFN |
| **Carlos Fuentes Bermejo*** | CF | RedIRIS |
| **Oxana Smirnova*** | OS | NDGF |
| **Vincent Ribaillier* (day 2)** | VR | IDRIS |
| **Romain Wartel* (day 1)** | RW | CERN |
| **Linda Cornwall* (day1)** | LC | STFC |

Apologies: Keith Chadwick (FNAL), David Jackson (STFC), Stefan Lueders (CERN), Frederic Schaer (CEA)

[1] Present at the opening and during the virtualization session

* Remotely connected

# AGENDA BASHING

- SA reminded that contributions from SPG will be needed for "MS214: Security Activity within EGI"; table of content to be drafted by 17 January 2011, SA will send to the list request for contribution
- TF requested that naming/numbering scheme for policy/procedure documents to easy reference to them; important to distinguish them

# ITEMS OF BUSINESS

## SPG Terms of Reference, Procedures and Membership

- DK recalled that the ToR was finally approved; discussion about rewording of NGIs/EIROs to (associated) participants;
- DK showed the list of members, to be updated (***action 01/01***); CW asked if all NGI participants were invited since some of them seemed not to know about the group; (***Action 01/02***)
- TF raised the issue of how infrastructure providers signing MoUs with EGI.eu are represented in SPG (***action 01/03***)
- TF raised the issue of how virtual research communities (VRC) signing MoUs with EGI.eu are represented in SPG (***action 01/03***)

## Work plan for 2011

- DK presented the work plan (see slides); DK mentioned that there should be conventions on usage of terms (e.g., Grid vs. grid., Site vs. site vs. *site*) and could be useful EGI-wide;
- TF observed that in the security policy documents, sentences like "the grid can do this" are present, TF wondered if they should be more EGI-specific or they are meant to be general; DK answered that the goal is to have them general in order to let other infrastructures to reuse them (e.g., DEISA/PRACE); JW who contributed to the earlier policy document definition would like to have a shorter copyright statement to report on the documents that are based on EGI policies (***action 01/04***); DO mentioned that StratusLab is also aiming to reuse EGI policies
- DK mentioned that IPG (including stakeholders EGI, OSG, Japanese Grid, Canada, DEISA, PRACE among others) is a good place to define a policy framework and define interoperability about policy

## EU Digital Agenda, Data Privacy and implications for EGI security policy

DM presented items for discussions related to the Digital Agenda (see presentation); CW recalled that the use digital certificates with embedded user name creates the issue of consent in granting the access to the EGI infrastructure; DG observed that EGI.eu, as a Dutch foundation, observes the Dutch law; in NL, if people use computer and these computers collect data from them, users should be informed; nevertheless the Dutch data protection law provides exceptions in case of access control to auditing/security of ICT systems (***action 01/05, 01/06, 01/07***)

- JW wondered how far the digital agenda can address issues which cross EU borders; for instance France cannot import some identity information from Switzerland (so they behave differently if the person is from EU or not); DK observed that we may reopen issue of using certificate with names; DG wondered if EGI.eu should register with the appropriate Data Protection Officer;
- DK observed that for 2011, there is the need to revisit the accounting policy to be extended to storage
- DF asked if SPG should define indicators to measure if policies are well applied; DK answered that it is an interesting matter, nevertheless effort to address this may not be available

## Virtualisation Policy

- SN explained the vision on the evolution of the infrastructure towards virtualization using two slides; SN set out the context of Digital Agenda in the wider scope of EU and explained that several user communities do not have use cases fulfilled by gLite/ARC software stack, therefore EGI needs to be open to adapt to them; illustrated the vision of extending EGI with virtualization as also presented in the DCI Collaborative Roadmap (https://documents.egi.eu/document/207); in this vision, authorized individuals should be able to deploy VMs as edge services in the various sites; existing AAA components should be reused (e.g., VOMS, X.509); cross-site provisioning should also be possible (e.g., there are two data-sets in two different sites, deploy VMs in both); StratusLab and Venus-C are exploring solutions at different levels; help to support the exploration of; by aligning to Digital Agenda, EGI will be in a good position for future funding in FP8; after further discussion, it was also agreed that only some big site should be enabled for these functionalities otherwise small sites not being able to manage properly WNs may have corrupted VMs propagating issues to other on big sites
- DG wondered why the ability to deploy VMs should be restricted to a kind of super-users; BigGrid is going to provide a completely isolated area to deploy VMs; SN observed that this is a necessary step in order to build trust; moving the deployment of the software stack to the users give them all the flexibility but also the problems; DO stated that StratusLab is not working on tools to let the end-user deploy VMs, but rather for a restricted set of users;
- DG stated that assigning public and routable IP addresses to VMs bring extra responsibilities to the owners; MM then introduced the issue of maintaining usage traceability and accountability; SN clarified that traceability should be available for VMs deployment and content, not for who is using it; a system for reporting who is using the VMs to the VOs using a common messaging backplane should be available
- DK introduced the need for a service policy to be adopted by sites offering VM capabilities
- DK presented the HEPIX Virtualisation working group policy document “Policy on the Endorsement of Virtual Machine Images” (https://edms.cern.ch/document/1080777/) and asked if it can be a good starting point for a policy on endorsing VMs; common agreement on yes; SN suggested to pay attention on policy vs procedure; rephrase better as policy

- DF observed that the endorsement is a kind of certification; therefore the person who does that should be different than the one who created the machine; agreement that it should be a different person;
- SG asked if VMs are going to be read-only or read/write; DO said that StratusLab is working on possibility of installing packages in VM and then write-once; may need to be re-endorsed;
- DK presented the second document on virtualization from Polish NGI (see document on the agenda page)

## Current set of policies

- TF showed her slides "Feedback on Site Operations Policy and Site Registration Security Policy"; EGI-InSPIRE SA1 worked on reorganized and collected operations policy that where not well organised during EGEE; DK clarified that the policy document named "Grid Site Operations Policy" got the name from an EGEE deliverable and was a kind of a precursor of OLA; it contains both security and operations related aspects and probably no Site ever signed it; agreement on the need to split the two areas and move the operations part to OMB; TF suggested that a policy could set as a requirement that sites need to sign an OLA in order to achieve certification;
- SPG has its own glossary of terms and Operations as well; the need for a joint glossary was discussed (***action 01/08***)
    - SPG Glossary: https://documents.egi.eu/document/71
    - Operations Terminology introduced here: https://documents.egi.eu/document/218
- Further discussion on the items issues raised by TF in the presentation led to the following decisions
    - DECISION: to get rid of "site registration security policy" at the same time as the updated site operations policy is approved (***action 01/09***)
    - DECISION: rewrite site operations policy joined with service policy (from virtualization discussion)
- DF explained that France has a site in GOCDB and that is not in EGI but is in LCG; so wondered about the applicability of policies (e.g., site suspension); it was observed that the scenario in EGI is more complex than before; TF clarified that in the architecture document, there is mention of resource providers and not about NGIs; moreover site suspension, certification and OLA are in the pipeline and involvement of both operations and security people would be useful
- DF asked what EGI would do in case of a site with a known vulnerability but with no patch/solution available; DG observed that it is not possible to force NGI to suspend them; it is a site decision; DK asked if CSIRT feels it is wrong to let sites decide; SG said no

*The first day of the meeting concluded at 17.00. The second day of the meeting started at 9:30.*

## Day 2: Security Policy for collaborating DCIs (DEISA, PRACE, OSG, WLCG, …)

DK recalled that in the past, the JSPG spent time in defining more general policy for other infrastructures, in a collaborative way; DK was invited by JW to participate in a DEISA/PRACE security workshop in Helsinki; the conclusion of that was that it is desirable to collaborate where possible through the participation of individuals in SPG;

JW says that the focus is not totally overlapping, e.g., registration of sites by DEISA was never an issue probably because of different background; in the past the JSPG AUP was accepted by DEISA; in Helsinki the current EGI AUP was discussed noting that many of the recent changes had been as a result of feedback from DEISA; another area of collaboration is security incidents; in May DEISA will end, PRACE will be the only left, and the security forum team of PRACE agreed to collaborate; a document to state the responsibilities of the security team and the collaboration areas was written, nevertheless it was no yet put forward to the management;

WLCG was a primary stakeholder in JSPG, now WLCG is a primary user community but does not play as important a role in EGI SPG; in a meeting at FermiLab with RW and OSG, the new SPG was described and OSG did not see an important role to be played in it; nevertheless two OSG persons are present into the mailing list; it is desirable that SPG and WLCG policies remain aligned; collaboration with OSG can be achieved via a high-level security policy framework; this work can be taken forward under the auspices of IPG, e.g. at its meeting next March;

DK showed a document Policy Framework (http://www.jspg.org/wiki/Policy_Framework) from JSPG activity; DK showed also a spreadsheet with an attempt to extract Security Incident Response top level aims in a similar way to RFC PKI CPS (http://www.ietf.org/rfc/rfc2527.txt); the work is not strictly SPG but a collaboration of EU+US individuals who will bring the proposal to IPG (***action 01/10***); DF wished to be informed about this activity (***action 01/11***); MM asked why the activity will start mainly with WLCG, but there are other stakeholders; DK said it is just a mechanism to get started and others are welcome to join.

## Revision of top-level Grid Security Policy

- DK showed the PDP document and read the definition of Policy vs. Procedure (see document on agenda page)
- DK showed the top-level Grid Security Policy document; (see document on agenda page)
- the term “Grid” refers to EGI when the policy is adopted by EGI; Policy definition needs to be aligned with PDP definition; The word “Grid” may need to be changed; DCI or e-Infrastructure are ok; the problem with the latter is that in the US, they use cyber-infrastructure instead of e-infrastructure. “DCI” seems to be the preferred word.
- discussion around the need to change the term VO; JW said in DEISA have concept of Principal Investigator who is responsible for applying for usage access;
- Agreement that the document needs revision already in the definitions area;

- Section 2.0 may have repetition in sub documents; in future revision, this should be avoided; many statements should be in sub-documents;
- DO asked about the propagation chain of responsibility; a site is responsible to the related NGI and its Security Officer; what is the chain up to EGI? DK said this should be considered in the new revision, maybe the EGI policy should be that NGIs should have their own NGI security policy, while each NGI instantiates it in specific way
- DK asked if the top-level security policy document is still needed; JW stated that it is needed for describing roles and responsibilities, scope of the activity; DO mentioned that it is like having a constitution, where you can fall back on; AGREEMENT IT IS NEEDED
- DK asked about the scope; should it be Grid-specific or more general? AGREE: it should be general enough to encompass Grid & Cloud & external infrastructures joining via MoU
    - DD mentioned that some NREN are involved in cloud and maybe they have some policy already; ask to TERENA (***action 01/12***)
- DF brought back the discussion to suspending sites which are WLCG but not EGI; DK observed that potentially sites can register with multiple grids and whoever they register with should be responsible for any required suspension; DK also recalled that sites register with NGIs, NGIs are part of EGI; VOs can connect to NGIs or to EGI; layers of authorities are more complex; there should be a top-level document which is general enough to encompass this complexity; we need to deal, for example, with virtual services run by a registered VO on resources which are not registered with NGIs/EGI.
- DK proposed to remove the definitions from top-level document to the Glossary. AGREEMENT TO REMOVE
- SA observed that there are many glossaries in EGI and outside; SA proposed to have a unified glossary for EGI merging at least security and operations terminology; maybe a team composed by representatives from TCB, OMB, UCB, SPG and the Policy Team could work on the merge; connection to ESFRI and e-IRG glossaries should also be considered;

## Plans for the future

Agreed workplan for 2011

**Table 1 Work plan for 2011**

| # | Document | Draft by | Team |
|---|---|---|---|
| ***1*** | Rewrite top-level security policy | *External: 31/10/2011 (draft to be presented at TF)* | *DK* DD DG RW PDT* |
| ***2*** | Data privacy:<br>- Phase 1: expand job-level accounting to storage<br>- Phase 2: think also about more general data privacy and relationship with Digital Agenda<br>(external consultation with Tilburg Univ.) | *External: 31/10/2011* | *DG DK DO DF* |
| ***3*** | Rewrite site operations policy as a general services security policy<br>a. Include service operation security policy (real and virtual)<br>b. Resource, providers, VM managers, etc<br>c. Exclude operations items to be considered by OMB | *Internal: 31/05/2011*<br>*External: 30/06/2011* | *DG* CK DO DF SG EGI Operations* |
| ***4*** | Generalise HEPiX VM Endorsement to include other types of trustworthy VMs | *External: 14/07/2011* | *RW* DO Ric DK HEPiK WG* |
| ***5*** | SPG Glossary | *Major revision in step with new top-level document* | *Full SPG* |

** leader*

- All discussion about documents will take place in the SPG-discuss mailing list
- The work on the Security Policy Framework with other infrastructures will be done outside SPG among a number of individuals and to be presented to IPG; work plan to be communicated to SPG list

## AOB

None

## Actions

| ID | Resp. | Description | Status |
|---|---|---|---|
| **01/01** | DK/DM | Update the list of members in the wiki | NEW |
| **01/02** | DK | Invite all EGI.eu Council participants to nominate a voting member of SPG | NEW |
| **01/03** | SA | Define how external infrastructure providers and virtual research communities can be represented/engaged in SPG (Steve/Gergely) | NEW |
| **01/04** | SA | License statement, to make more compact and explain how external partners should mention it | NEW |
| **01/05** | DG | To provide English translation for Dutch data protection law, art. 35(?) | NEW |
| **01/06** | SA | Ask Steven Newhouse if we can we have legal advice through EGI.eu about compliance of accounting with law?<br>*No dedicated budget, we can pay expert to travel here; anyway the topic will come up with the digital agenda* | NEW |
| **01/07** | DG&DK | Go through digital agenda items related to trust and security | NEW |
| **01/08** | DK | Harmonize security and operation terminology | NEW |
| **01/09** | DK | get rid of "site registration security policy" at the same time as the updated site operations policy is approved | NEW |
| **01/10** | DK,RW | Discuss Security Incident Response proposal for IPG | NEW |
| **01/11** | DK | Send dates for meeting collaboration on Security Incident Response to SPG list to gather contributors | NEW |
| **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 | NEW |

## Date for Next Meeting

It was agreed that the full SPG will aim to meet quarterly primarily to receive reports on the activity of the editorial teams, but also to carry-out any other routine business. It would be useful if this coincided with the production of the EGI-InSPIRE quarterly report. Additional meetings will be called as necessary to discuss drafts of policy documents.

At least two of the annual meetings will be held face to face. It was agreed that holding these at the User Forum and Technical Forum meetings made sense (if we can find time on the busy agenda!). The next F2F meeting will be held during the EGI User Forum (11-15 April 2011, Vilnius).

There being no further business, the meeting concluded at 15:30




e-infrastructure


Minutes prepared by Sergio Andreozzi, 17.01.2011

Minutes Approved SPG Chair David Kelsey

_____