Security Coordination Group (SCG)

Meeting:	Phone call
Date and Time:	Wed 10th February 2011 at 12
Venue:	
Agenda:	https://www.egi.eu/indico/conferenceDisplay.py?confId=312

Participants

Name and Surname	Abbr.	Representing	Membership[1]
Steven Newhouse	SN	EGI.eu Director and CTO	Member
David Kelsey	DK	EGI SPG Chair	Member
Linda Cornwall	LC	EGI SVG Chair	Member
David Groep	DG	EGI Representative in EUGridPMA	Member
John White	JW	EMI Representative	Member
Michel Drescher	MD	EGI.eu Technical Manager	Observer
Tiziana Ferrari	TF	EGI.eu Chief Operations Officer	Observer
Damir Marinovic	DM	EGI.eu Policy Development Officer	In attendance

[1] Member, Observer, in Attendance

MINUTES OF THE PREVIOUS MEETING

The minutes of the last meeting held on 10th December 2010 were reviewed. No other additions/corrections were reported. The minutes were approved as a correct record of the proceedings.

AGENDA BASHING

No changes

ACTION REVIEWS

ID	Resp.	Description	Status[2]
01/01	DK	Add in the SPG F2F agenda an item related to policy for VMs	CLOSED
01/02	LC	To prepare a poster for the User Forum explaining the responsibilities for the various security policy groups within EGI	OPEN

ITEMS OF BUSINESS

SPG Report

DK presented his latest activities as a SPG chair. SP mentioned his participation in the EUGridPMA meeting (24-26 January 2011 Utrecht). SP led the session working on new policy standards for general Attribute Authorities, thereby expanding the work of IGTF beyond pure identity management to the management of attributes in general, e.g. for Authorisation of access to Grid services. The plan is to have a good draft profile for wider discussion at the IGTF All Hands meeting in Taipei. SP added that together with Romain Wartel (WLCG Security Officer) he had produced a first draft of a Security Policy Standard for interoperating infrastructures on Security Operations, Traceability and Incident Handling. DK said that he plans setting up a phone meeting with WLCG security people (OSG, FNAL, CERN etc. including EGI SPG interested people) to discuss this. He mentioned that if IPG is planning to meet in Taipei, this would be a good topic on which he could give a short presentation. SN mentioned that is a request for an IPG workshop and most like it will be approved. SN will find out whether it is possible to have IPG meeting in Tapei, Taiwan **(action 02/01)**

TZ asked when site security policy drafting coordinated by DG will start. DG answered that the next week he will be setting up editorial teams and making sure that the team starts working before the next face-to-face meeting at the User Forum. TZ said that OMB is reviewing site certification procedure and it would be a good opportunity to work in parallel on the site policy in

[2] NEW, OPEN, CLOSED, REJECTED

order to avoid duplication. She stated he would like to converge quickly procedure to have it approved in March. DG confirmed that that he will put it at the top of the list.

SN asked if there was an issue that EMI was examining an eduGAIN model for federated identity and TERENA which some NGIs may use for issuing certificates was using eduPERSON. DG said that in his opinion it is not something else, it is different complementary technologies, they are not incompatible. JW said that eduGAIN is just eduGAIN person. JM said that he will circulate to the SCG list EMI faults on common security libraries **(action 02/02)**

SVG Report

LC said that Bart suggested the idea of a European Assessment Centre, partly funded by industry; possibly try to get some core funding to get it started. She posed the question: is there a way we could start looking at this? SN said that it is very intriguing subject. If we manage to connect it with the magic word “cloud” it is possible to get funding. LC said it is not sure whether we should apply for funding SN said that whenever is the next round of calls, to have a look at it. Call opens in July this year and there is no direct info what the topics are. DK said that there is potential for the homeland security funding also.

LC asked when poster template will be available. SN said that it is ongoing action on our designer hopefully something in the next few weeks. LC would like to see the template as soon as possible in order to start drafting the content and getting the quality feedback.

AOB

JW said that he is interested in resurrecting the middleware security group so he sent an email to the list. However, there is no much interest. EMI is not willing to commit itself to this activity. Nor was there any interest from developers outside Europe. He asked about possible next steps. He said that focus should be more on security and middleware not so much on security. SN said it is hard to get anything in Vilnius. Next logical opportunity would be Technical Forum. It will be good opportunity to include IGE and people from USA and the focus should be much more on technology than on deployment. **(action 02/03)**

Actions

ID	Resp.	Description	Status[3]
01/02	LC	To prepare a poster for the User Forum explaining the responsibilities for the various security policy groups within EGI	OPEN
02/01	SN	Find out whether it is possible to have IPG meeting in Tapei, Taiwan	NEW
02/02	JW	Circulate to the SCG list EMI faults on common security libraries	NEW
02/03	SN	Establish link with other software providers for the middleware security group	NEW

Date for Next Meeting

There being no further business, the meeting concluded at 12:45

[3] NEW, OPEN, CLOSED, REJECTED



Minutes prepared by Damir Marinovic 14.02.2011.

Minutes Approved Group Chair Steven Newhouse

Report from SPG (since 1st Jan 2011)

1. Terms of Reference approved by EGI.eu Executivce Board

2. First formal Face to face meeting held at Nikhef on 12-13 January 2011.

Agenda and minutes at https://wiki.egi.eu/wiki/SPG:Meetings

The group (approximately 25 members were able to attend) discussed many important topics with the main aim of understanding which new security policies are needed and which of the current policies are most in need of revision. A work plan for 2011 was agreed including the creation of several editorial teams.

3. The agreed SPG work plan for 2011 includes work on the following policy areas:

- Full revision of the old top-level Security Policy document.
- Policy related to Data privacy.
  - Phase 1: expand the job-level accounting policy to include storage accounting.
  - Phase 2: even more general data privacy policy and its relationship with the EU Digital Agenda.
- Revision of the Grid Site Operations Policy.
  - To include general service operation security policy (real and virtual services).
  - Include Resource Providers, Virtual Machine managers, etc.
  - This will now exclude operational (non-security) items to be considered by SA1 and OMB.
- Generalise the HEPiX Security Policy on the Endorsement of Virtual Machine Images to include other types of trustworthy Virtual Machines.
- SPG Glossary (as a contribution to the more general EGI Glossary).

4. SPG input to MS214 (Security Activity within EGI)

Some personal security policy work for me as chair, included:

1. Participation in the EUGridPMA meeting on 24-26 January 2011 (Utrecht). I led the session working on new policy standards for general Attribute Authorities, thereby expanding the work of IGTF beyond pure identity management to the management of attributes in general, e.g. for Authorisation of access to Grid services. The plan is to have a good draft profile for wider discussion at the IGTF All Hands meeting in Taipei.

2. Romain Wartel (WLCG Security Officer) and I have produced a first draft of a Security Policy Standard for interoperating infrastructures on Security Operations, Traceability and Incident Handling. I will now set up a phone meeting with WLCG security people (OSG, FNAL, CERN etc including EGI SPG interested people) to discuss this. If IPG is planning to meet in Taipei, this would be a good topic on which I could give a short presentation.

Report from SVG

Four new vulnerabilities reported. 2 not Grid middleware (handled operationally), 1 (Globus) not in a version used in EGI, and another awaiting TD (Low risk).

The only vulnerability reported in EGI that has reached TD has just had the new version released. (VOMS admin) vulnerabilities found as a result of the vulnerability assessment. We have been asked to hold off releasing the advisory as the patches are not available for OSG yet.

F2F meeting with Barton Miller (University of Wisconsin) and Elisa Heymann (University of Barcelona). Discussed the Vulnerability Assessment plan, which is completed from our side, a small re-arrangement of the order of assessments due to an imminent CREAM re-write to comply with EMI-ES (Execution Service) specification. A tutorial on secure java programming will be available soon.

Bart suggested the idea of a European Assessment centre, partly funded by industry, possibly try to get some core funding to get it started. Is there any way we could look at starting this?

Plans:

- Continue issue handling process.
- Improve use of RT to automate more, e.g. send reminders, produce info that allows us to extract information for use in templates and reporting.
- Start having SVG meetings (EVO?) as stated in TOR - up to now most communication by e-mail.
- Complete going over 'OLD' issues from pre-EGI.

CSIRT related and other activities that I have done:

I have put together for CSIRT a Critical Security Handling procedure, which was discussed at the NOC mangers meeting. It was (almost) approved, one change that needed making was that CSIRT should suspend sites for security reasons (NOT COD) and I need to check a couple of small points when Mingchao is back. Probably only 5 minutes work needed for completion.

A more detailed critical vulnerability handling procedure has also been written (joint SVG/CSIRT doc), this needs updating to fit with the new Critical security handling procedure.

Also, will start on UF poster draft in a couple of weeks.

Report from David Groep

The main technical bit is the first release through EGI channels of the trust anchor distribution. 1.38 is now available and announced. It showed a couple of issues that are now (to be) resolved:

- monitoring nagios tests needed to be updated fomr new repository url and format
- the EGI-broadcast tool cannot handle special characters
- the old lcg-CA repo needs to be repointed and forward to the EGI repo.

And there was of course the EUGridPMA meeting last month. Summary from the last EUGridPMA meeting:

The minutes of the meeting, kindly provided by Jules Wolfrat and Nuno Dias, are now available at https://www.eugridpma.org/meetings/2011-01/

A few highlights:

- Developments in the Secure Token Services (STS) and the embedding of automated 'translation' services for identity and other attributes has picked up momentum all over Europe. The presentation from SURFnet shows several options, EMI is scheduled to develop STS services linked to short-lived X.509 generators, and there are other related developments such as www.pistoiaalliance.org. The exploration of options in this direction will be continued in the Prague meeting
- the EUMedGridSupport II project is actively encouraging identity management around the Mediterranean basin, and besides the CAs that have already come forward more are expected.
- With respect to the Classic guidelines on maximum EE certificate life time and key length, it was agreed that
  - 1 year plus 1 months is considered equivalent to 395 days
  - it should be seriously considered to increase minimum RSA key length to 2048 bits for EECs, following current best practice
- Self-audits and updates were presented and reviewed in this meeting, see the page at https://www.eugridpma.org/review/selfaudit-review for details and status
- HIAST and DZ-eScience both presented their CA in person and the accreditation can continue via the list. Both prospective members should converge on an accreditable CP/CPS with their reviewers and a final call will be issued on the mailing list.

See the minutes for additional statements

HIAST reviewers: Onur and Roberto; DZ-eScience reviewers: Eygene and Pawel

The Guidelines on Private Key Proteciton for End-entity credentials should be reviewers with regard to text and meaning, but with the text as it stands and with rough consensus, the following has been decided:

- the proposal by Jim Basney can proceed as it is within the current form of the PKP Guidelines
- Guidelines should be clarified with respect to actions by 'third parties'
- any specific implementation of a system by an authority will anyway be reviewed by the accrediting PMA, which should be satisfied with the over-all integrity of the system
- strong emphasis should be put on auditability of any system
- a new test draft should be put on the Taipei all-hands agenda
- a down time notification system for relying parties has been set up by ChristosT. See https://igtf-devel.grid.auth.gr/downtimes and the corresponding RSS feed at http://igtf-devel.grid.auth.gr/downtimes.rss RPs and VOs can import this into their dashboards.

Authorities SHOULD use this system for:

- any length of scheduled down time
- publishing unexpected issues as soon as practical
- register at least one authority manager before the end of February!

- the text-edited MICS profile (version 1.2) has been accepted by the EUGridPMA. See http://tagpma.es.net/wiki/bin/view/Main/TagMICS for the full version history, and the EUGridPMA Guidelines section for the accepted version.
- The PMA will experiment with the use of videoconferences for the tracking of self-audit review progress. This should speed up the reviews and keep peers focussed. When this experiment is successful, changing the lengths of the plenary meeting may be considered. The frequency (3 times per year) will remain as-is regardless -- as this will facilitate meeting the attendance requirements of at least one meeting per year.

Next meetings:

- IGTF All-Hands in Taipei, 21-22 March, followed by ISCG & OGF31
- Prague: Wednesday May 11 13.30 until Friday 13th (either noon or end-of-day, depending on VC experiment and agenda)

FOLLOWED by REFEDs and TNC2011

The September meeting, on invitation by the EUMedGridSupport II project and with the kind flexibility of SiGNET, is now scheduled to be held in Marrakesh, MA, from September 12-14 (Mon morning - Wed lunchtime), graciously hosted by CNRST and MA-Grid.

The January 2012 meeting will take place in Ljubljana, Slovenia, and is kindly hosted by the Josef Stefan Institute.