

22nd EU Grid PMA 11-May-2011.

13⁰⁰ Attendance: Vladimir, Hroch, Jelis, San-Francisco, Milan, Havel, Nuno, Edgars, Emir, Reimer, PA, Daniel, Sunny, Zoro, Bozidar.
 Remote: Christof, Feyza, Yung.
 Minutes: Nilly, Jelis, Emir.

Dinner: 19³⁰.

Agenda: SAC PMA : Milan → early in the period (so 14-15 daily)

~~14⁰⁰ Sunny - APGrid PMA status.~~

14⁰⁰ - Introduction

RBT check IWD recommendation of EPEL to ensure fetch-only is used not automatic in EL4/EL5.

MIBST: last version (Feyza)
 Feyza: should be ready to go soon.
 Need more to test.

SANren: sent SANren to Feyza. the CP/CPS.
 Support is working.

Sanit: provide feedback before Hanakub!
 Reviewers: PK + Feyza.

coming: Tunisia! Egypt is delayed to end of the month.

Self-Whirl status

Baltic Grid - had staff issues but is getting better with EPT.
 New CP/CPS before August 1.

WCC: Israel is unresponsive. → tomorrow more updates.

UKCSC: Suno should send staff. New cert should be accomp. by CP/CPS.

phlBrs: ask Diego.

AEJIS: no updated version sent! ask Dusan!

OFN: own CP/CPS still to do.

MREN: no news. Nilly has to do some work on it.
 Subject DR matching has been patched.

EUGmaPMA Prague May 11-13 2011.

Josef Brezina: reviewer → also Sen
will send new CP/CD.

14³⁵ Jimmy - APGmaPMA.
see presentation

14⁴⁵ Dinner: meet at: [Bilhouc 5.] Batekha restaurant @ 19³⁰
[tea time] Plüsterh @ 19⁰⁰ +420 602 593 047.
Helen mobile

15⁰⁰ Jules - PRICE
<see online presentation>

for thank you local institutions in a country a having RA like
in UK would be helpful.

15¹⁵ TCS issues are being collected and then followed up. Issues are mostly
new issues.

16⁰⁰ Auth2-operations (Dovek).
see wiki

Thursday 12

09³⁵ Christoph. AAI-NG ENI.
disc. start at slide 10* Issues: #21.

10¹⁰ GEMmas - Grant3. - Diego L.

AS (validation) policies joined to producers.
Based on OpenSAML.
EMD profile iteration in the next few months
See TNC for the GEMmas cook book. (incl. STS).

Team: role of DNSsec in STS message structure?

initially role of DNSsec will be discovery of STS service instances.

STS discussion

→ scaling of STS? Geant would like a single one.
Trustworthy enough?

esp. Diego 2013 case: 1 per country / federation.
@diego

Milan: more than one type of connection, so one per
connection and community structure.

Christoph: STS are per federation worthwhile for EUGridPMO.

→ mostly generation STS Ltd

What about PS, i.e. stand validation.

outsourcing validation? then 'accrediting' the RP
side.

} "UMIA" group in web-2.0 space.
describes this use case.

↳ info disclosure policies.
Wantara.

Eligible LPA requirement for non grid?

↳ Geant has valuable resources, but
how far access to it has/will be accessible through
federations / STS is unclear.

TRACE: list of staff coming from institutions.
CLADIN.

Diego → Collaborate w/ commercial world, i.e. cloud. SCIM.

LDAP → SPANL

Is STS always short-lived? Diego: yes. Christoph: "should not matter".
mainly: short.

SLCS: need for revocation! also for STS!

STS has to handle it. AS could do,
but then has to know origin!

* revocation also comes back in SAML meta-data in eduGAIN.

> concentrate on 24 hr + renewal.

> start with SACS.

* the data will be long lived (EduGAIN).

↳ so name should be long-lived, but signing is a problem due to key management.

the key persistence and escrow has to be solved.

> extend SACS single STS - collect more than subject IDs.
 ⇒ - can take input tokens from multiple sources.

↳ and spit out a single combined token.

→ needs a way to express source of each element

"enriched SACS".

↳ this cannot currently be done, only the STS will sign.

↳ or put all the stuff in a blob and let the auth 2 side figure it out.

> targets

↳ look at Shinto (Dover Channel).

barrier with Auth 2 Ops WG: should only deal with ops, not the LOP or trust issues!

Balthead is in SACS and should be in STS.

> timespan 10-20 mo.

> STS profile:

- generalised SACS for non X-509 output.

- non-subject-entity attributes.

- combined assertions from multiple sources into single assertion.

"extract from X509 those trust elements that would also be needed for the other technologies and get them into the SACS as it is being developed.

- limit to target RPs.

(ACT) → extract ESPE's as PIA RPs

measnet: distributed transaction trust (c.f. PGP).

[12:00 Lunch]

[13:00 [MCO may drop, in order to complete at least the DAOps.]]

Dave U - DAOps see wiki

"Attr. Management" section deliberately short. In "STS" profile would elaborate on this.

[15:00 - 15:30 Tea]

15:35 Bozidar - MARGI S/A.

Reviewers: Emir, David G.

new CP/CPS forth coming - new cur.

16:01 TCS update. (Stevan).

validation for personal etc not going to change yet.

17:00 AAOPS

[Dinner Spirků] Hotel Dora. reservation @ 19:30 }
Kožná 12.

CPB Survey: - release conditions
-> members may look at aggregated data in presentation (and request new aggregated views)
-> in public presentations by members only totals (no spreads) or lists should be used.

18:00 BEgrid - now actually offline, so OK for now. Will change later again to new CP
Life time of CA cur => usage of time of private key.

10:34 Bgr Acad S/A.

- add checks on key material: - no Debian keys
- good (>253) exponent.
- keypair not used prior
- no known-weak exp.

Reviewers Edgars, Boris

22nd PMD Prague meeting

11:40 AOB

Tenn: on cert life time: when STP-1 is trouble?
only the request in case of real compromise.
most CP's can issue, but it will break all software.
NIST hopes STP-3 is ready before STP-1 is broken.
we advised jund2012.

Diego: last subsc. OK

Ales: Training facility, certs?
we use national training CP's, otherwise use communities
training CP's.

Reiner: Tidy up the registered participants pages? Old stuff?
out of search engines?
↳ move to intranet.

12:10 AAOs →

13:00 Closure.