2020-01 Prague security

21 January 2020 15:29

PMA Notes.

https://indico.nikhef.nl/event/2146/

Wednesday 22/01/2020

Self-audit review & status of suspended authorities 15'

Speaker: Cosmin Nistor (ROSA)

Status as noted in wiki table.

https://wiki.eugridpma.org/Members/SelfAuditStatus

Discussion of suspension of RDIG under review process since 2016. Move to full suspension with appropriate notices to relying parties.

SR: need better defined process/milestones for suspension. And clear expectations - cut off date

----

RAT-CC communications challenge report and SCCC-JWG 30'

Speaker: David Groep (Nikhef)

https://wiki.geant.org/display/WISE/SCCC-JWG

Review of spreadsheet of results of RAT-SCC of CAs sent 2019-10-07

RK: What's the plan for non-responders?

DC: following up by various PMA chairs.

SR:do we need maybe annual re-attestation of requirements on CAs?

Test the failers?

DK:retest them all again after 4m, not too onerous replying to one email

SR:transparency appropriate instrument of trust

DG:happy to challenge those that fail

HS:put results behind secure website?

DG:grouped unnamed results should be ok at tlp:g

All:TI CSIRT reaction test, 4/yr.

DG:ACTION:will challenge those that did not respond.

HS:SCCC-JWG will discuss at ???/ and also TIIME

14:00 - 14:30 APGridPMA: developments in the Asia Pacific region

Speaker: Eisaku Sakane (NII)

As per slides with no questions. Some (4) will go to APGridPMA meeting at ISGC.

15:30 - 16:20CA update I: GEANT TCS service updates && new back-end issuance provider 50'

Speaker: David Groep (Nikhef)

Discussion about which API is offered by vendor: Retail API

JC:Is there access to testing API?
DG: GEANT implementing training material (send email)
SR:What about the certificate profiles, OIDs etc. and how to reference back through CPS.
DG:will be in TCS CPS
DG: Actions on SR and ?RK to review SECTIGO (@5.1.6)
RK asks for red-line version from TCS doc changes. sectigo.com/legal

----

17:00 - 17:30 TAGPMA - developments from the Americas 30'
Speaker: Derek Simmel (PSC)

Given by DG.

Content as per slides by DG with no question.
DS: checklist was interesting exercise - should be formalised as a process to, maybe, badge of compliance etc.
JJ: has been useful to have InCommon Silver supported. Is there mechanism in US for InCommon Basic?
DS: not afaik but does come along with Silver.

Thursday

09:00 - 09:45 Enabling Communities with T&I – the workplan for 2020
Speakers: Maarten Kremers (SURFnet), David Groep (Nikhef)

SCI -
US: evolution of SCI assessment sheet - as shown for EGI@Karlsruhe meeting. Participation via WISE.
DK: WISE: ongoing developing baseline guidance (PDK) together with SCI assessment sheet: By Dec20 some document describing the guidance/policy framework.
MK: ideally available/hosted outside of project repos etc. By WISE/REFEDS.....

SCCC -
DG: on WISE wiki but not on WISE website (no access). PY2 continue to contribute, identify Infras, calendar .... As per slides p8.
InCommon did succeed in executing challenges. Needs work (DG:~1200hrs) and contacts.
DG: some (SURF,DFN) just need to register what they do already.

Assurance Profiles -
JZ: improve guidance, want logos/identifiers for profiles. Contacted IANA and 4 (SFA,MFA, RAFs) profiles successfully registered.
MK: Y2 contributions?
JZ: Polling for need for entity categories for each profile. Show in metadata which IdPs offer required profile. Allow filtering at user auth time rather than fail/reject at runtime.
US: should we develop guidance for achieving desired assurance level?
DG: InCommon have examples.

SIRTFI
DG: started Incident Response handbook. But too large/complex. EduGain security team now developing guidance/procedure..
SG: SG+US participating - 2 phone conf - with eduGain. Initially based on experience with Grid which is not like eduGain. Now removing grid-specific items with aim of 1-2 page guidance/helpsheet for operators etc.

US: some IdPs
SG: plan SCC using generic contact point - may provide security contact which is ?usually missing.

AA Ops guidelines
DG: not much progress. Hannah to report of check against CERN AAI.
MK: discussion about complaints that guidelines disallow using Amazon - "largely theoretical" - can request (?pay for) more secure/HSM environments.
DG+DK: could almost be merged with SCI work?

FIM4R
DK: review FIM4R Community blog entries of meetings (made by HS) https://fim4r.org/ Case studies with problems adopting Federated Infras. Reported USA moving away from relying on IdPs publishing necessary attributes. More discussion in Vienna at point in time for standing back and reflecting - FIM4R paper on hold pending redirection.

OIDC Fed
DG: slides as per Friday Agenda

Outreach and Communities -
DG+DK: poster at ISGC?

11:00 - 12:30 Assurance FAQ and best practices 1h30'
Speaker: Jule Ziegler (LRZ)

JZ: use this time to develop content for paper at ISGC. Look at abstract for paper.
DK: do we aim at linking to existing documents or writing a new guidance document.
DG: perhaps take example of IdP and statements of why particular assertion is arrived at.
DK: attractive to base on UseCase studies.
DK+US: what use cases BBMRI, Grid/WLCG
IN: AARC milestone on High requirements?
US: target service providers, not to ask for more than really required.
DK: how to describe/diagram/graphically? Stories from the blog ....
JZ: one slide with basic bullet points
.... Discussion ......

14:00 - 14:30RCauth service: distributed operations and trust evolution
Speakers: Mischa Salle (Nikhef), Jens Jensen (STFC RAL), David Groep (Nikhef)

JJ: Reported roadmap to EOSC-hub. Rather stuck at secret material exchange, depends on GRNET purchase of HSM. Other step is database synchronisation + virtual private circuit.
Tasks 5.17 (in roadmap to finish Q2-2020) & 5.18 (finished by Q3)
Added self-audit certification @Autumn PMA
Broadly the plan but would also like to look at usability.
MS: key exchange planned as presented to PMA
JJ: in the spirit but not quite to the letter.
MS: practically need to sort out software pieces - not sure about doing by Q1
JJ: all non-secret information has been exchanged last year. Need means of easy comms between the operators
MS: keybase - doesn't use Slack browser based
JJ: nice to have a truly distributed CA (MS: cilogon?)

MS: RCAuth instance upgraded to latest SimpleSAML.php
Nicholas: distribution of WAYF? Would add complexity.
MS: should be second line/doable compared to offline CAs

14:30 - 15:00 Applying AAOPS to the WLCG Token Profile and Kubernetes deployments
Speaker: Hannah Short (CERN)

DG: running within a Kubernetes environment (only) with other security services implies appropriate administrative/administrator controls will be in place. Uplifts security. Not a problem with Kubernetes per-se but more risky with public (website) and AA services hosted together. Should be adequate controls plus well managed (separated hypervisors) cluster.
HS: Lifetime of refresh token, is this seen as equivalent to an access token? - but it is revocable.
DG+DK: Not conceived that would apply to refresh tokens.
DK: should update the wording regarding the ops reqs for virtual environments
: discussion about signed assertions and OIDC signing key (6 month) lifetimes
DG: OIDC federation would add layer for key validation against local trust anchor. Ultimate trust is in well known endpoint (TLS)
DK: use EV certificate etc. for wellknown

16:00 - 17:20 SCIv2 assessment infrastructure comparison
Speakers: Dave Kelsey (STFC RAL), Uros Stevanovic (KIT)

DK: what is the motivation for infra to complete the assessment?
US: there is no 'certification' body as with a PMA. Exchange or peer information - bodies not in WISE - what about AEGIS?
DK: will call meeting of SCI-WG
US: coordination with TrustedCI (BobC) - started but not progressed.
Sirtfi group suggested help with incident response.

09:45 - 10:30 AARC Policy Development evolution: review of (too short) top-level security policy
Speaker: David Kelsey (STFC RAL)

Display and discussion analysis of EGI,EOSC-hub and PDK Top-Level policies.

Friday

09:15 - 10:15 Targeted policy implementation recommendations for (EGI) communities: outstanding requests 1h0'
Speaker: Dave Kelsey (STFC RAL)

Review of notes.

10:15 - 10:45 trust distribution for OAuth (both signing and TLS connection certs) 30'
Speaker: Hannah Short (CERN)

Research Infras issuing Oauth Tokens. Various certificates involved in key signing but not much

governance around them.
US: Would largely be solved by OIDC Federation but also movement in ?APINT (G052)? to have a trust layer at the proxy level where a service requests the necessary key from its proxy which does necessary negotiation.
RK: is the suggestion that IGTF would sign some collection of CA certificates
GD: or organisational meta-data.
HS: need to be quite quick in putting some policy/practice in place as people are deploying this now. Envisage a handful of providers.
MS: one per VO. OIDC Fed could have one layer above that.
DK: statement by somebody/we/IGTF as to what is OK
MS: people used to push-model of distribution trust anchors.
DG: something like a script which RPs use to pull and install keys from known url. Envision O(100) OPs O(n*1000) RPs
HS: same question for RPs
DG: e.g. LetsEncrypt would be OK provided the URL is assured. What is the source of the proper URL for the endpoint.
MS: fundamentally different: hanging of TLS, rather than an out of bound distribution.
RK: if you can't trust DNS then it doesn't matter which certificate you use. Need to check the signature on the metadata.
US: present OIDC Fed practice only distributes URL but probably should distribute key hash.
DG: may be that Infra may accepted the risk of DNS spoofing.
SR+RK: need some governance over root of trust - EV OID etc.
HS: maybe some wont' be happy but wlcg probably open to putting in place something similar to what we have at the moment.
DG+SR: maybe an OR of all the trust anchors.

10:45 - 10:50 easing use of the IGTF eduGAIN bridge: policy and assurance encoding (coherent policy OIDs) 5'
Speaker: David Groep (Nikhef)

10:50 - 11:00OIDC fed for the IGTF
Speaker: David Groep (Nikhef)

11:30 - 12:30 Jens' Soap Box
Speaker: Jens Jensen (STFC RAL)