



TAGPMA
The Americas Grid
Policy Management Authority

TAGPMA Update

Derek Simmel dsimmel@psc.edu, TAGPMA Chair

43rd EUGridPMA Meeting

Karlsruhe, Germany

May 23, 2018



TAGPMA Update

- The Americas Grid Policy Management Authority (TAGPMA)
 - Leadership
 - Members
 - Communications
 - Conference Calls
 - Face-to-Face Meetings
 - Current Work and Activities



TAGPMA Leadership

- Chairs: Derek Simmel dsimmel@psc.edu (PSC, U.S.A.)
Paula Venosa pvenosa@info.unlp.edu.ar (UNLP,
Argentina)
- Vice-chair: Ale Stolk alestolk@gmail.com (ULAGrid, Venezuela)
- Secretary: Jeff Porter (retired April 30)
- Web Master: Scott Sakai ssakai@sdsc.edu (SDSC, U.S.A.)



TAGPMA Members

Organization	Country	Representative	Member Type
FNAL	U.S.A.	Jeny Teheran	Relying Party
OGF	U.S.A.	Alan Sill	Relying Party
REBCA	U.S.A.	Scott Rea	Relying Party
SDSC	U.S.A.	Scott Sakai	Relying Party
UFF	Brazil	Vinod Rebello	Relying Party
ULAGrid	Venezuela	Ale Stolk	Relying Party
UNIANDES	Colombia	Andres Holguin	Relying Party
WLCG	Switzerland	David Kelsey	Relying Party
XSEDE	U.S.A.	Jim Marsteller	Relying Party
DigiCert	U.S.A.	Clint Wilson	Authentication Provider
GridCanada	Canada	Lixin Liu	Authentication Provider
IBDS ANSP	Brazil	Angelo de Souza Santos	Authentication Provider
InCommon	U.S.A.	Jim Basney	Authentication Provider
OSG	U.S.A.	Susan Sons	Authentication Provider
NCSA	U.S.A.	Jim Basney	Authentication Provider
NERSC	U.S.A.	Jeff Porter	Authentication Provider
PSC	U.S.A.	Derek Simmel	Authentication Provider
REUNA	Chile	Alejandro Lara	Authentication Provider
UNAM	Mexico	Jhonatan Lopez	Authentication Provider
UNLP	Argentina	Paula Venosa	Authentication Provider



TAGPMA Members

- 20 Members (11 APs, 9 RPs) from the North, Central and South American countries + Switzerland
 - Including Argentina, Brazil, Canada, Chile, Colombia, Mexico, U.S.A and Venezuela, + WLCG (RP) in Switzerland
- 20 IGTF-Accredited CAs (as of distribution v.1.91)
 - 14 Classic CAs
 - Argentina: UNLPGrid
 - Brazil: ANSPGrid
 - Canada: GridCanada
 - Chile: REUNA
 - Mexico: UNAM (2)
 - U.S.A.: DigiCert(6), InCommon (IGTF Server CA), CILogon-OSG
 - 4 Short Lived Credential Service (SLCS) CAs
 - U.S.A.: NCSA (SLCS-2013, TFCA-2013), NERSC, PSC
 - 1 Member-Integrated Credential Service (MICS) CA
 - U.S.A.: NCSA (CILogon-Silver)
 - 1 Identifier-Only Trust Assurance (IOTA) CA
 - U.S.A.: NCSA (CILogon-Basic)



TAGPMA Communications

- TAGPMA Website: <http://www.tagpma.org>
 - Public information and documents
 - Now hosted on Google Sites
- TAGPMA twiki [http\(s\)://tagpma.es.net/wiki](http(s)://tagpma.es.net/wiki)
 - Legacy documents, meeting agendas, notes
 - Working to retire this ASAP and move current docs to Google Sites
- Mailing lists:
 - tagpma-general – subscribe by joining the tagpma-general Google Group
 - tagpma-private – members-only mailing list currently maintained at PSC
- E-mail any suggestions or issues directly to the Chair (dsimmel@psc.edu)



TAGPMA Conference Calls

- Monthly conference calls:
 - Currently scheduled on the 2nd Thursday of every Month*
 - Spanish language call begins at 10:30am EDT (UTC -4:00)*
 - English language call begins at 11:00am EDT (UTC -4:00)*
 - Vidyo link at <https://www.nikhef.nl/grid/video/?m=tagpma>
 - Next call will be on June 14, 2018
- *times and dates change periodically to maximize member availability
- All IGTF members and prospective TAGPMA members are welcome to attend and participate in TAGPMA meetings!
 - Contact the Chair (dsimmel@psc.edu) for current call times and coordinates



TAGPMA Face-to-Face Meetings

- 26th TAGPMA Face-to-Face Meeting @ Internet2 Global Summit
 - May 10, 2018 – Marriot San Diego
 - Agenda and presentations at <http://indico.rnp.br/conferenceTimeTable.py?confId=254#20180510>
- Co-location with Internet2 meetings
 - Global Summit (2017, 2018, ...) have gone well
 - Considering Internet2 TechEx (Orlando, FL October 15-18 2018)
- Attempts to have a meeting in Latin America have been unsuccessful recently
 - Upcoming RedCLARA-affiliated events?
 - TICAL2018/eScience – <http://tical2018.redclara.net/index.php/en/>
 - September 3-5, 2018, Cartagena de Indias, Colombia
 - Call for papers due June 11, 2018 – Travel paid for one author
 - LACNIC30/LACNOG - <http://www.lacnog.org/en/>
 - September 24-28, 2018, Rosario, Argentina
 - Call for papers forthcoming... - Travel paid for one author



TAGPMA Current Work and Activities

- OpenID Connect (OIDC) Federation working group
- Certificate Transparency – scope and needs for IGTF-accredited CAs
- Open Science Grid (OSG) CA retirement
- IBDS ANSP Grid CA (Brazil) updating CP/CPS to expand scope of operations to cover all of Brazil
- Working Group initiated to examine development of a new assurance level (Elm?) and an associated IGTF profile for host certificates issued with Domain Control Validation (DCV) + additional controls
 - Dave Kelsey (WLCG), Jim Marsteller (XSEDE), Jim Basney (NCSA), Brian Brockelman (OSG, Univ. of Nebraska), OSG stakeholders



Open Science Grid CA retirement

- Short version:
 - History: ESN Net CA, then DigiCert IGTF CA, then CILogon OSG CA
 - A funding shortfall requires the shutdown of the OSG Information Management (OIM) System and CA front-end (RA) at Indiana University
 - The back-end, operated by NCSA with the CILogon infrastructure remains OK
 - The OSG CA RA will cease operations on May 31, 2018
 - Security monitoring, certificate revocation, and CRL issuance will continue through June 2019
 - User certificates are available for most OSG-related users via CILogon or other IGTF-accredited CAs
 - Biggest challenge is what to do about obtaining host / service certificates



OSG CA retirement / U.S. DoE Lab needs

- Fermilab gets ~1300 host/service certificates from OSG CA
 - Fermilab operates the largest (and only U.S.) Tier-1 site for the CMS experiment
- All US-CMS Tier-2 and Tier-3 sites get their host/service certs from OSG CA
- Brookhaven National Laboratory (BNL) gets ~100 host/service certificates from OSG CA
 - BNL is the sole Tier-1 computing facility for the ATLAS experiment in the U.S.
- Fermilab and BNL currently require IGTF-accredited Cas
 - Alternatives limited to InCommon IGTF Server CA, DigiCert Grid CA
 - U.S. DoE labs are not currently eligible to subscribe to InCommon Certificate Service
 - Small Tier-3 sites cannot afford to subscribe to the InCommon Certificate Service
 - DigiCert host/service certificates cost ~\$175 each
- Investigating LetsEncrypt CA as an alternative...



LetsEnCrypt CA?

- Global CA in CABForum offering Domain Validation (DV) certificates
- Provides 90-day host certificates
- Relies on an FQDN's authoritative DNS records to identify host owners
- OSG interested in using this in combination with OSG knowledge of authorized hostcert applicants
- What would suffice for IGTF to include LetsEncrypt CA in the distribution?
 - Invite LetsEncrypt to apply for accreditation – under what profile(s)?
 - As an unaccredited CA, as Fermi KCA was in the past?
 - What additional security controls would be sufficient for a minimum acceptable LoA?
 - Can we develop a sufficient LoA & Profile for accreditation?
 - What existing / additional One Statement Certificate Policies would be needed?



OSG CA retirement / related links

- OSG CA Transition Plans
 - Brian Brockelman @ TAGPMA 26, May 10, 2018
 - <http://indico.rnp.br/getFile.py/access?contribId=19&resId=0&materialId=slides&confId=254>
- OSG CA Fermilab Status Update
 - Jeny Teheran, Mine Altunay @ TAGPMA 26, May 10, 2018
 - <http://indico.rnp.br/getFile.py/access?contribId=20&resId=0&materialId=slides&confId=254>
- CILogon Update
 - Jim Basney @ TAGPMA 26, May 10, 2018
 - <http://indico.rnp.br/getFile.py/access?contribId=14&resId=0&materialId=slides&confId=254>
- Open Science Grid ISO Position Paper on LetsEncrypt CA for Host Certificate Signing
 - Susan Sons, OSG Information Security Officer, document dated April 11, 2018
 - <https://opensciencegrid.org/security/OSGISOppLetsEncrypt.pdf>
- IETF RFC 6844: DNS Certification Authority Authorization (CAA) Resource Record
 - <https://tools.ietf.org/html/rfc6844>
- IETF Draft: Automatic Certificate Management Environment (ACME)
 - <https://ietf-wg-acme.github.io/acme/draft-ietf-acme-acme.txt>