



TAGPMA
The Americas Grid
Policy Management Authority

TAGPMA Update

Derek Simmel dsimmel@psc.edu, TAGPMA Chair

27th APGridPMA Meeting
ISGC2021, Taipei, Taiwan

March 23, 2021



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: Jeny Teheran, jteheran@fnal.gov (Fermilab, U.S.A.)
- 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
OSG	U.S.A.	Mike Stanfield	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.	Derek Simmel	Relying Party
DigiCert	U.S.A.	Tomofumi Okubo	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
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 (10 APs, 10 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
- **18** IGTF-Accredited CAs (as of distribution v.1.109, January 2020)
 - 13 Classic CAs
 - Argentina: UNLPGrid
 - Brazil: ANSPGrid
 - Canada: GridCanada
 - Chile: REUNA
 - Mexico: UNAM (2)
 - U.S.A.: DigiCert(6), InCommon (IGTF Server CA)
 - **3** Short Lived Credential Service (SLCS) CAs
 - U.S.A.: NCSA SLCS-2013, PSC MyProxy CA
 - **NERSC (plans to retire their SLCS CA – still up as of today).**
 - 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 Activities

- Review of CILogon CA CP/CPS updates for infrastructure migration
 - CILogon web front-end to be moved from NCSA to AWS US East (Ohio)
 - Higher availability of web services (SAML, OIDC, OAuth, SciTokens)
 - CA back-end and HSMs remain at NCSA machine room at uiuc.edu
 - Amazon CloudHSM remains prohibitively expensive at over \$1K/month
 - Communications between front- and back-ends to be secured via TLS with mutual authentication
 - Updated CP/CPS documents at:
 - <https://ca.cilogon.org/policy/silver> (v.14)
 - <https://ca.cilogon.org/policy/basic> (v.6)
 - Contact: Jim Basney - jbasney@illinois.edu
 - Presentation and discussion scheduled for April 13 13:00 EDT TAGPMA meeting



TAGPMA Communications

- TAGPMA Website: <http://www.tagpma.org>
 - Public information and documents
 - Still hosted on Google Sites – migration to GitHub stalled
- Mailing lists:
 - tagpma-general – subscribe by joining the tagpma-general Google Group
 - tagpma-private – members-only mailing list currently maintained at PSC
- TAGPMA Slack Channel
 - Join group tagpma.slack.com
- E-mail any suggestions or issues directly to the Chair (dsimmel@psc.edu)



TAGPMA Conference Calls

- Monthly conference calls:
 - Currently scheduled on the 2nd Tuesday of every Month*
 - Spanish language call TBD*
 - English language call begins at 13:00 (U.S. Eastern, currently UTC -4:00)
 - Zoom link
 - <https://cmu.zoom.us/j/598670138> **Send e-mail to Chair for passcode**
- 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

- 28th TAGPMA F2F Meeting @ Internet2 Technology Exchange
 - December 13, 2019, New Orleans, Louisiana, U.S.A.
- TAGPMA Officers Meeting – Focus on TAGPMA website
 - March 11-12, 2020, San Diego, CA, U.S.A.
- No TAGPMA F2F meetings planned until after COVID-19
 - All meetings and workshops online via Zoom until further notice.
- IGTF All-Hands Meeting – no plans yet



Workshop on Token-Based Authentication and Authorization (WoTBAN&AZ 2020)

- November 30 – December 1, 2020
- Agenda, slides and video available at <https://indico.rnp.br/event/33/>
- Sessions:
 - Token Based Authorisation for WLCG
 - Globus Auth: expanding the services ecosystem for protected data
 - LIGO's use of SciTokens
 - XSEDE's Perspective on Token Assurance for Authentication and Authorization
 - Fermilab's experience transitioning to token-based AAI technologies
 - Final Panel: What Have We Learned? What Do We Need? What Should We Do?



Workshop on Token-Based Authentication and Authorization (WoTBAN&AZ 2020)

- Observations:
 - Each project investing in token-based A&A infrastructure is building it to provide new functionality while maintaining continuity with established local A&A infrastructure
 - Each project is engaged independently in developing its own implementation that addresses the needs of its local/project constituency
 - Interoperability between implementations is desirable
 - Globus is working on JSON Web Token interfaces – expected this year (2021)
 - The weight of trust now lies with the token issuers
 - We need policies and standards for secure operation of token service infrastructure
 - IGTF should develop an accreditation framework for token issuers
 - Services relying on token-based A&A must enforce their policy expectations (e.g., MFA)



Workshop on Token-Based Authentication and Authorization (WoTBAN&AZ 2020)

- Needs:
 - Use cases to drive development of interoperable solutions
 - Consuming multiple tokens from different issuers
 - Common Identity attributes
 - VOs of different scale
 - Common best practices for token handling
 - for issuers, developers, service operators and users
 - Addressing Security concerns, e.g.:
 - Hybrid/concurrent implementations during transition from GSI to token-based AuthN & AuthZ
 - Trust in token issuers (independence? authority? auditing?...)
 - Responsibility for vetting Identity Providers
 - Revocation of authorization
 - Refresh token security
 - Incident prevention, and preparation for incident handling and recovery



Workshop on Token-Based Authentication and Authorization (WoTBAN&AZ Spring*2021)

- Planning for the next workshop:
 - Use cases development / exercises
 - Building blocks for a token-issuer accreditation process
 - Token lifecycle management
 - Best practices
 - Security roles, policies, procedures and tools
 - Other ideas?
- Logistics
 - April/May 2021 time frame (*Spring in the Northern Hemisphere)
 - Two half-days 9:00am-12:00noon EDT (UTC -4:00)
 - Online via Zoom