TAGPMA
The Americas Grid
Policy Management Authority

TAGPMA Update

Derek Simmel dsimmel@psc.edu, TAGPMA Chair

30th APGridPMA Meeting
Academia Sinica, Taipei, Taiwan

March 21, 2023

TAGPMA Leadership

- Chairs: Derek Simmel dsimmel@psc.edu (PSC, U.S.A.)
  Paula Venosa pvenosa@info.unlp.edu.ar (UNLP, Argentina)

- Secretary: Jeny Teheran, jteheran@fnal.gov (Fermilab, U.S.A.)*

- Web Master: Scott Sakai ssakai@sdsc.edu (SDSC, U.S.A.)

Jeny is retiring from TAGPMA after many years of service as Fermilab's representative and as TAGPMA secretary – TAGPMA sincerely appreciates Jeny for her participation and many contributions! We look forward to Jeny's continued work in advancing trust and security in HPC!* ***Thanks Jeny!*

TAGPMA Members

Organization	Country	Representative	Member Type
FNAL	U.S.A.	Jeny Teheran → Mine Altunay	Relying Party
OGF	U.S.A.	Alan Sill	Relying Party
OSG	U.S.A.	Mike Stanfield	Relying Party
REBCA	U.S.A.	Scott Rea	**Retired – no participation in > 3yrs**
SDSC	U.S.A.	Scott Sakai	Relying Party
UFF	Brazil	Vinod Rebello	Relying Party
ULAGrid	Venezuela	Ale Stolk	Relying Party
UNIANDES	Colombia	Andres Holguin	**Retired – no participation in > 3yrs**
WLCG	Switzerland	David Kelsey	Relying Party
ACCESS	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
PSC	U.S.A.	Derek Simmel	Relying Party
REUNA	Chile	Alejandro Lara	Authentication Provider
UNAM	Mexico	Jhonatan Lopez	Authentication Provider
UNLP	Argentina	Paula Venosa	Authentication Provider

TAGPMA Members

- **17** Members (**8** APs, **9** RPs) from the North, Central and South American countries + Switzerland
  - Including Argentina, Brazil, Canada, Chile, Mexico, U.S.A and Venezuela, + WLCG (RP) in Switzerland

- **15** IGTF-Accredited CAs (as of distribution v.1.119, March 2023)
  - 13 Classic CAs
    - Argentina: UNLPGrid
    - Brazil: ANSPGrid
    - Canada: GridCanada
    - Chile: REUNA
    - Mexico: UNAM (2)
    - U.S.A.: DigiCert(**6**), InCommon (IGTF Server CA)
  - 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
  - Operating on “new” Google Sites
- 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*
  - 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 dsimmel@psc.edu 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 Activities – Retiring SHA-1 certs

- TAGPMA CAs have all been advised to check for and replace SHA-1-signed CA certificates with SHA-2-signed CA certificates
  - Updates made in IGTF distribution 118 for GridCanada and CILogon CAs

  - When will DigiCert update SHA-1 signed CA certificates to SHA-2?

  The following CA certificates in the IGTF distribution are signed with sha1WithRSAEncryption:
    - ca_DigiCertAssuredIDRootCA-Root-1.117/DigiCertAssuredIDRootCA-Root.pem*
      - Updating may be complicated as this CA cert is currently in the CABForum public distribution, which requires a more formal procedure to replace it with a SHA-2-signed certificate.
      - **This root CA signs the new DigiCert 2022 Grid Client and Grid TLS CA certificates.**
    - ca_DigiCertGridRootCA-Root-1.117/DigiCertGridRootCA-Root.pem
    - ca_DigiCertGridCA-1-Classic-1.117/DigiCertGridCA-1-Classic.pem **(retired from IGTF distribution)**
    - ca_DigiCertGridTrustCA-Classic-1.117/DigiCertGridTrustCA-Classic.pem **(retired from IGTF distribution)**

  - DigiCert representative Tomofumi Okubo is looking into these issues (as of March 14, 2023).

TAGPMA Activities – DigiCert + Quo Vadis

- https://www.quovadisglobal.com/tls-ssl/

- QuoVadis Certificates: “TLS/SSL certificates issued by one of Europe’s leading Certificate Authority and backed globally by DigiCert.”
- No word yet from DigiCert about assuming responsibility for IGTF-accredited QuoVadis CAs in TAGPMA
- QuoVadis Root CA 2 certificate is SHA-1 signed – updating to SHA-2 may be complicated as this CA certificate is also in the CABForum public distribution, which requires a more formal update procedure to replace it.

- What is the correct transfer-of-membership process between PMAs?

TAGPMA Activities – Google CA?

- New prospective TAGPMA member & Classic CA accreditation applicant
- Certificate issuance in support of CERN/ATLAS project + Google Cloud
- A CPS from "Google Trust Services, LLC", (https://pki.goog/) was provided
  - https://static.googleusercontent.com/media/pki.goog/en//repo/cps/4.11/GTS-CPS.pdf
  - Initial review initiated, to identify areas that would need to be modified for IGTF accreditation in the Classic Profile.
- Working with Ross Thomson and Dustin Sell at Google
  - Derek met with Ross at Google Pittsburgh on February 1, 2023, to introduce him to IGTF, TAGPMA, and the CA accreditation process.
  - Current Google CA services only support Domain Validation for their public API…
  - Ross attended the March 14, 2023 TAGPMA meeting to describe their needs for service certificates acceptable to CERN/ATLAS project
  - We are investigating whether these can be obtained from InCommon – maybe with ACME?

TAGPMA Activities – InCommon

- InCommon is replacing their currently-accredited “IGTF Server CA” with a new “InCommon RSA IGTF Server CA 2”
  - The CA certificate for this new CA has been added to the IGTF distribution 1.119 in the *Experimental (Not Yet Accredited)* category until the CPS document has been updated, reviewed and accepted by TAGPMA
  - A first review of the updated CPS has been completed and returned to Paul Caskey at InCommon for corrections and to resolve comments.

- InCommon relying parties (notably Fermilab) are eager to have a functional ACME service available from InCommon…
  - Paul Caskey has promised to re-emphasize the urgency to get this working, which would help Fermilab and may help CERN/ATLAS + Google Cloud

TAGPMA Face-to-Face Meetings

- Recent TAGPMA-related Face-to-Face meetings:
  - Workshop on Token-Based Authentication and Authorization (WoTBAn&Az 2022) at U.S. NSF CyberSecurity Summit, Bloomington, Indiana
    - 09:00-13:00 EDT (UTC -4:00) October 18, 2022
    - https://sciauth.org/workshop/2022/
  - Internet2 Technical Exchange (Dec. 5-8, 2022, Denver, Colorado)
    - 16th FIM4R Workshop & TAGPMA
      - Sunday December 4, 2022 10:00-17:30 UTC -7:00
      - https://indico.cern.ch/event/1202335/
    - Panel session: Migrating to Token-Based AuthN and AuthZ
      - Tuesday December 6, 2022 13:40-14:30 UTC -7:00
      - https://internet2.edu/2022-technology-exchange/2022-program/iam-sessions/
      - Slides available at https://sciauth.org/2022/12/06/TechEx.html

Token-Based Authentication and Authorization

- Research computing infrastructures worldwide are working to migrate their legacy and X.509-based user authentication and authorization infrastructures to use OpenID Connect (OIDC, https://openid.net/connect/)
- OIDC is a protocol built on OAuth2 specifications that delivers identity and authentication information using JSON Web Tokens, (JWT, RFC 7519)
- OIDC is in widespread use in commercial web applications and services
- However, many research computing infrastructures have a significant investment in IAM protocols and services that are not (yet?) web-centric

Workshop Series 2020..2022

- WoTBAn&Az 2020: https://indico.rnp.br/event/33/
  - Token-based authorisation in WLCG, Globus Auth, LIGO's use of SciTokens, XSEDE's perspective on Token Assurance, Fermilab's transition to Token-based AAI
- WoTBAn&Az 2021: https://sciauth.org/workshop/2021/
  - Tokens in WLCG, Tokens in the TAPIS API Platform, Using CILogon OIDC Service for user authentication in Kubernetes, SciTokens at LIGO, HTCondor and OSG Token transition
- WoTBAn&Az 2022: https://sciauth.org/workshop/2022/
  - SSH with Federated Identities using OIDC, Token-based access to HPC resources in IRIS, Globus integration with NIH's Research Authentication Service and Common Fund Data Ecosystem, Adoption of SciTokens and WLCG Tokens by LIGO and Fermilab using CILogon

Token-Based AuthN & AuthZ @ TechEx

- *Moving to Tokens: IRIS & WLCG*, Tom Dack STFC
  - https://sciauth.org/20221206-2-tdack-tokens.pdf
- *CILogon and SciTokens*, Jim Basney, NCSA, Univ. of Illinois
  - https://sciauth.org/20221206-3-jbasney-tokens.pdf
- *Token-based AAI at Fermilab*, Jeny Teheran, Fermi Laboratory
  - https://sciauth.org/20221206-4-jteheran-tokens.pdf

SciAuth

- SciAuth is a U.S. National Science Foundation-funded project (2114989) that seeks to "improve the usability and interoperability of the security credentials that scientists use to access NSF cyberinfrastructure"
- https://sciauth.org/
- Co-sponsor of WoTBAn&Az workshops together with TAGPMA

- PEARC22 Paper: Brian Aydemir, Jim Basney, Brian Bockelman, Jeff Gaynor, Derek Weitzel (2022). *SciAuth: A Lightweight End-to-End Capability-Based Authorization Environment for Scientific Computing*
  - describes a containerized end-to-end environment for learning about SciTokens
  - https://dl.acm.org/doi/pdf/10.1145/3491418.3535160
  - Jupyter Notebook-based SciTokens demo: https://sciauth.org/notebook-demo

SSH Integration Examples

- pam-ssh-oidc + motley-cue, oidc-agent + ssh clients
  - as presented by Diana Gudu, Marcus Hardt, Gabriel Zachmann Karlsruhe Institute of Technlogy
  - https://github.com/EOSC-synergy/ssh-oidc

- STFC PAM module
  - as presented by Jens Jensen et al, UKRI
  - https://github.com/stfc/pam_oauth2_device

- These and other approaches presented at 17th FIM4R (Feb. 16, 2023)
  - as presented by Marcus Hardt and others
  - https://indico.cern.ch/event/1224755/#32-federated-shell-access-job