



TAGPMA Update

Derek Simmel dsimmel@psc.edu, TAGPMA Chair

57th EUGridPMA Meeting
CERN, Geneva, Switzerland

February 13, 2022



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.)



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	Retired – no participation in > 2yrs
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

- **18** Members (**8** APs, **10** 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
- **17** IGTF-Accredited CAs (as of distribution v.1.117, August 2022)
 - 13 Classic CAs
 - Argentina: UNLPGrid
 - Brazil: ANSPGrid
 - Canada: GridCanada
 - Chile: REUNA
 - Mexico: UNAM (2)
 - U.S.A.: DigiCert(**8**), 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

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

- Chasing DigiCert to 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 (**ICA, obsolete?**)
 - ca_DigiCertGridTrustCA-Classic-1.117/DigiCertGridTrustCA-Classic.pem (**ICA, obsolete?**)
- DigiCert representatives Martin Sullivan and Tomofumi Okubo e-mailed directly Jan. 30, and again Feb. 13, 2023, asking that these be updated to SHA-2 signed certificates – no response yet received



TAGPMA Activities

- DigiCert + QuoVadis
 - <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.
 - Who will represent Google in TAGPMA remains to be determined...



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>