TAGPMA
The Americas Grid
Policy Management Authority

TAGPMA Update & Building Trust in Attribute Authorities

Derek Simmel dsimmel@psc.edu, TAGPMA Chair

16th Federated Identity Management for Research (FIM4R) Meeting
Denver, Colorado

December 4, 2022

What is TAGPMA?

- The Americas Grid Policy Management Authority (https://www.tagpma.org)
- One of 3 PMAs that constitute the Interoperable Global Trust Federation (www.igtf.net)
  - TAGPMA: North, Central, and South America & the Caribbean
  - EUGridPMA: Europe, Africa, and the Middle East
  - APGridPMA: Asia, Australia, New Zealand, and the Pacific
- Formed to establish common policies and operating standards for Authentication Providers and their Relying Parties
  - PMAs accredit x.509 Certificate Authorities for Research & Education located within their respective regions

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.	Josh Drake	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
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

- **19** Members (**8** APs, **11** 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

- **15** 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(6), InCommon (IGTF Server CA)

  - ~~2 Short Lived Credential Service (SLCS) CAs~~
    - ~~U.S.A.: NCSA SLCS-2013, PSC MyProxy 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 Activities

- TAGPMA SLCS CAs retired August 31, 2022
  - End of U.S. National Science Foundation (NSF) XSEDE project
    - Authentication services (MyProxy, OA4MP) for GSI-based services retired
    - XSEDE MyProxy CA (NCSA) and PSC Myproxy CA retired and removed from IGTF distribution. CRLs available until at least Sept. 12; CRL URL operated until Sept. 30, 2022
  - New NSF ACCESS project operating with federated identities via CILogon
    - https://identity.access-ci.org
    - XSEDE principals retained as ACCESS IDs for continuity and long-term recordkeeping
  - Integrations with NSF ACCESS available via CILogon OIDC interfaces
    - https://www.cilogon.org/oidc

TAGPMA Activities

- New DigiCert Intermediate CAs in IGTF 1.117 distribution

```
Serial Number:
            04:26:83:27:7d:82:d5:31:77:76:d7:e5:75:b1:87:7c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Assured ID Root CA
        Validity
            Not Before: Apr 12 00:00:00 2022 GMT
            Not After : Nov  9 23:59:59 2031 GMT
        Subject: C = US, O = "DigiCert, Inc.", CN = DigiCert Assured ID Grid Client RSA2048 SHA256 2022 CA1

Serial Number:
            0d:2c:a6:07:c8:d7:bb:70:e4:0a:49:41:61:7d:b7:35
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Assured ID Root CA
        Validity
            Not Before: Mar 10 00:00:00 2022 GMT
            Not After : Nov  9 23:59:59 2031 GMT
        Subject: C = US, O = "DigiCert, Inc.", CN = DigiCert Assured ID Grid TLS RSA2048 SHA256 2022 CA1
```

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 Workspace
  - Join **tagpma.slack.com** – Contact Chair (dsimmel@psc.edu) for Slack invitation.

- 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 Meeting ID: 598 670 138 - Passcode provided on request.

- 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

- TAGPMA-related Face-to-Face meetings planned for late 2022;
  - 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/

Building Trust in Attribute Authorities

- IGTF is uniquely positioned to help in building trust in the R&E community
- Trust is earned by sharing common policies and practices, and is sustained by behaving reliably within a community of practitioners, on behalf of relying parties
- Building on what we've learned in establishing standards for accrediting Certificate Authorities and maintaining a repository of CA trust anchors, IGTF is prepared to serve a similar role for Attribute Authorities
- Requirements: What do stakeholders need to make this practical?

Building Trust in Attribute Authorities

- Review: Building Blocks for Building Trust in Certificate Authorities
  - Interoperable Certificate Profile:
    - https://ogf.org/documents/GFD.225.pdf
  - IGTF Profiles of Authentication Assurance:
    - https://www.igtf.net/ap/authn-assurance/
  - IGTF PKI Technology Guidelines
    - https://www.eugridpma.org/guidelines/pkitech/
  - EUGridPMA Guidelines on Private Key Protection
    - https://www.eugridpma.org/guidelines/pkp/
  - Internet X.509 PKI Certificate Policy and Certification Practices Framework
    - https://www.ietf.org/rfc/rfc3647.txt
  - Accreditation activity executed by PMA members
    - Assessment worksheets and Operations validation
    - Interactive review between PMA member reviewers and authentication provider
    - Voting to accredit by PMA members
    - Procedure for secure publication of trust anchors

Building Trust in Attribute Authorities

- IGTF Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities
  - https://www.eugridpma.org/guidelines/aaops/
  - AARC Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities
    - https://aarc-community.org/guidelines/aarc-g071/
  - Assessment worksheet
    - https://www.eugridpma.org/guidelines/aaops/G048-Assessment-Sheet.pdf
    - Google spreadsheet: https://edu.nl/88dwf
- AAOPS Workshop day at EUGridPMA56 (October 2022)
  - Reviewed UK-IRIS and the WLCG proxies

Additional Resources include…

- FIM4R Federated Identity Management for Research Collaborations version 2
  - http://doi.org/10.5281/zenodo.1296031
- REFEDS Assurance Framework and Authentication Profiles
  - https://wiki.refeds.org/display/ASS/Assurance+Home
- Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)
  - https://www.igtf.net/snctfi/
- REFEDS Security Incident Response Trust Framework for Federated Identity version 2 (SIRTFI)
  - https://refeds.org/wp-content/uploads/2022/08/Sirtfi-v2.pdf

A List of Trusted Token Issuers…

(highlights noted by David Groep following EUGridPMA56 discussions)

- Relying parties add a list of trusted token issuers to configurations
- There is value in having a curated source of trusted token issuers
- Useful meta data alongside the list of token issuer end-points
  - e.g., Security Contact
  - metadata should align where possible with the OIDCfed metadata
- OIDC provider trust is necessary for cross-provider access use cases
- There should be a single list (IGTF wide), which can be taken and filtered by RPs based on accepted communities