TAGPMA Update

Derek Simmel dsimmel@psc.edu, TAGPMA Chair

49th EUGridPMA Meeting

Online from Home

May 13, 2020

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 (now OSG ISO)**	**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 (now XSEDE L3 Security Co-Lead)**	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.1.104, 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
    - **NCSA TFCA-2013 retired**
    - **NERSC plans to retire their SLCS 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
  - Now hosted on Google Sites
    - **Migrating to GitHub**
    - Focus of TAGPMA Officers' Meeting March 11-12, 2020
- 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 1:00pm (U.S. EDT, currently UTC -4:00)*
  - Zoom link
    - https://cmu.zoom.us/j/598670138
    - Backup: Vidyo link at https://www.nikhef.nl/grid/video/?m=tagpma
  - *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

- 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.

- 2020 TAGPMA F2F Meeting Planning – *Pending travel capability* – likely online
  - October 5-8: Internet2 Technology Exchange, Atlanta, GA, U.S.A.

- IGTF All-Hands Meeting Planning – *Pending travel capability* – likely online
  - Proposed: NCSA to host in Champaign–Urbana, Illinois before or after U.S. NSF CyberSecurity Summit (Indianapolis, Indiana, Sept 22-24, 2020)

- **Due to current/pending COVID-19 travel restrictions, postponements are likely**

28th TAGPMA F2F Meeting Highlights

- Agenda and presentation slides at https://indico.rnp.br/event/13/

- Assurance for JWT (JSON Web Tokens) [Jim Basney, NCSA]
  - WLCG Common JWT Profiles
  - Adoption by SciTokens (Fed AuthZ tools project) https://scitokens.org
- GridCanada CA redesign discussion
- Peer Review of REFEDS Assurance Adoption
  - Checklists drafted by Jim Basney
    - REFEDS Assurance Framework, Single Factor Authentication, Multifactor Authentication
  - Reviewed checklists completed for XSEDE IdP and Fermilab IdP

REFEDS Assurance Profile Reviews

- XSEDE working on resolving conflicts with profile requirements
  - Removing assertion of IAP/local-enterprise
  - Mitigating use by XSEDE "community accounts" to comply with Unique-1

- LIGO completing work toward compliance with Cappucino

- Work needs to be done to develop a process for certification or accreditation of IdPs…

Sectigo CA consolidation / trustchain

- Sectigo removed the AddTrust External CA Root from the signing chain when it updated the CA certificates for the intermediate CAs that signed the InCommon CA certificates.

- The former Sectigo intermediate CAs now have new certificates with extended expiry dates that make those CAs be their own roots.

- Sectigo-provided info and links to updated CA certificates at https://support.sectigo.com/Com_KnowledgeDetailPageFaq?Id=kA01N000 000rgSZ

- Problems noted with older OpenSSL versions and clients which had not yet updated their trustchains prompted a change to reintroduce the AddTrust External CA Root into the IGTF distribution (expiring May 30 2020)

InCommon IGTF Server CA trustchain

- Before:
  - issuer= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
  - subject= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
    - notBefore=May 30 10:48:38 2000 GMT
    - notAfter=May 30 10:48:38 2020 GMT
  - issuer= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
  - subject= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
    - notBefore=May 30 10:48:38 2000 GMT
    - notAfter=May 30 10:48:38 2020 GMT
  - issuer= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
  - subject= /C=US/O=Internet2/OU=InCommon/CN=InCommon IGTF Server CA
    - notBefore=Jan 1 00:00:00 2014 GMT
    - notAfter=Dec 31 23:59:59 2023 GMT

- After:
  - **issuer= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority**
  - subject= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
    - **notBefore=Jan 19 00:00:00 2010 GMT**
    - **notAfter=Jan 18 23:59:59 2038 GMT**
  - issuer= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
  - subject= /C=US/O=Internet2/OU=InCommon/CN=InCommon IGTF Server CA
    - notBefore=Jan 1 00:00:00 2014 GMT
    - notAfter=Dec 31 23:59:59 2023 GMT

InCommon RSA Server CA (not IGTF accredited)

- Before:

  issuer= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root

  subject= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root

      notBefore=May 30 10:48:38 2000 GMT

      notAfter=May 30 10:48:38 2020 GMT

  issuer= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root

  subject= /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

      notBefore=May 30 10:48:38 2000 GMT

      notAfter=May 30 10:48:38 2020 GMT

  issuer= /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

  subject= /C=US/ST=MI/L=Ann Arbor/O=Internet2/OU=InCommon/CN=InCommon RSA Server CA

      notBefore=Oct 6 00:00:00 2014 GMT

      notAfter=Oct 5 23:59:59 2024 GMT

- After:

  issuer= /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

  subject= /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

      notBefore=Feb 1 00:00:00 2010 GMT

      notAfter=Jan 18 23:59:59 2038 GMT

  issuer= /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

  subject= /C=US/ST=MI/L=Ann Arbor/O=Internet2/OU=InCommon/CN=InCommon RSA Server CA

      notBefore=Oct 6 00:00:00 2014 GMT

      notAfter=Oct 5 23:59:59 2024 GMT