EUGridPMA
Status and Current Trends
and some IGTF topics

March 2017
APGridPMA Spring Meeting

David Groep, Nikhef & EUGridPMA

EUGridPMA Topics

- EUGridPMA (membership) status
  - New CAs: RCauth.eu/AARC CILogon-like TTS; DarkMatter
  - AARC
- IGTF-to-eduGAIN bridge
- Model implementations for video-supported vetting
- Related activities: Sirtfi, Snctfi, REFEDS Assurance WG, and AARC2
- GFD.225 Certificate Profile completed
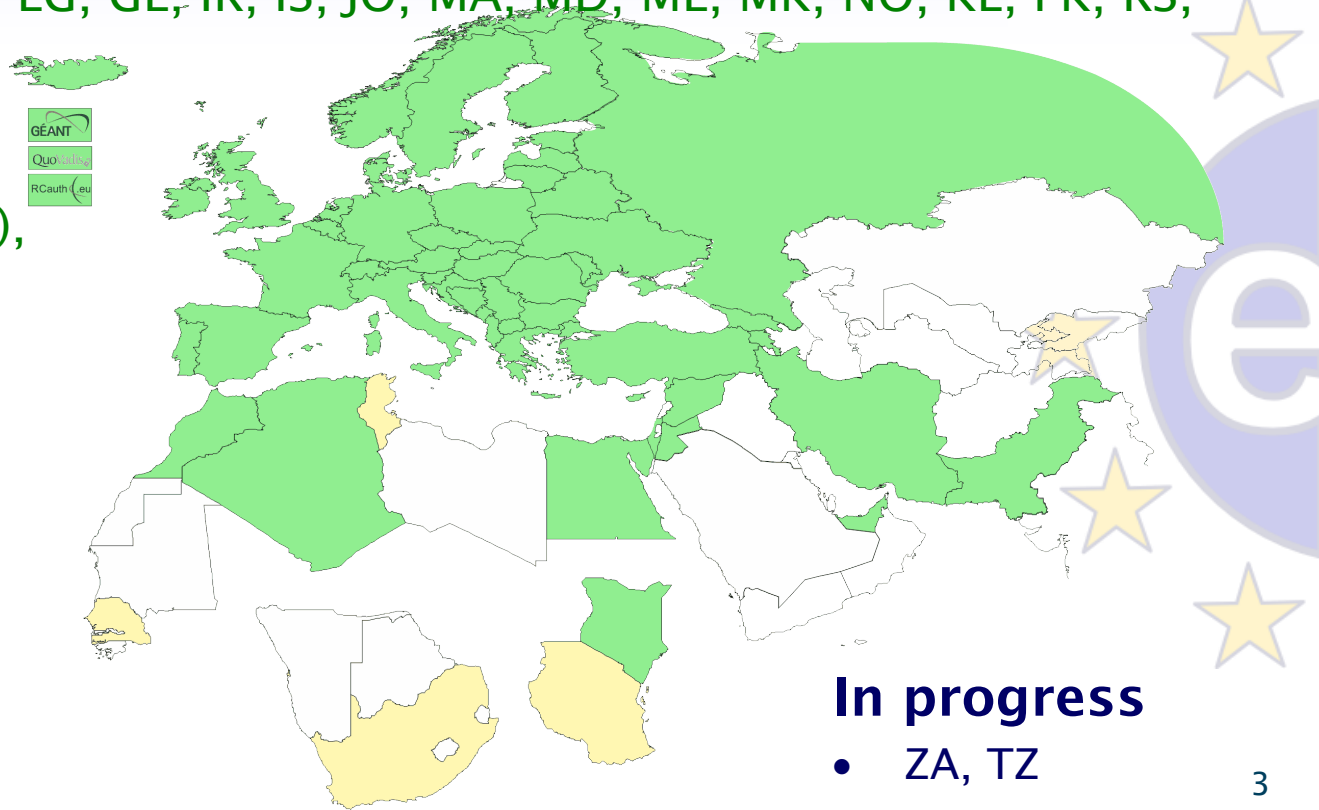- IPv6, SHA-1 collisions, and more

See also the EUGridPMA39 summary:
https://www.eugridpma.org/meetings/2017-01/

Geographical coverage of the EUGridPMA

- 26 of 28 EU member states (all except LU, MT)
- \+ AE, AM, CH, DZ, EG, GE, IR, IS, ~~JO~~, MA, MD, ME, MK, NO, KE, PK, RS, RU, ~~SY~~, TR, UA,
  CERN (int),
  TCS (EU),
  RCauth.eu (EU/NL),
  QV (BM)

47+4

In progress
- ZA, TZ

Membership and other changes

- Responsiveness challenges for some members
  - JUNET CA – removed from membership
  - HIAST CA – suspended for operational reasons

- Identity providers: both reduction and growth
  - New CA for e-Infras: RCauth.eu IOTA CA ("for those who cannot use TCS")
  - New CA for UAE: DarkMatter (phase 1 of 2)
  - Upcoming in UK: adding SLCS
- Self-audit review
  - Cosmin Nistor as review coordinator
  - Self-audits progressing
    on schedule for most CAs

RCauth.eu
white-label CA for the AARC CILogon-like TTS Pilot

- **Ability to serve a large pan-European user base without national restrictions**
  - without having to rely on specific national participation exclusively for this service
  - serving the needs of cross-national user communities that have a large but sparsely distributed user base
- **Use existing resources and e-Infrastructure services**
  - without the needs for security model changes at the resource centre or national level
- **Allow integration of this system in science gateways & portals with minimal effort**
  - only light-weight industry-standard protocols, limit security expertise (and exposure)
- **Permit the use of the VOMS community membership service**
  - attributes for group and role management in attribute certificates
  - also for portals and science gateways access the e-Infrastructure
- **Concentrate service elements that require significant operational expertise**
  - not burden research communities with the need to care for security-sensitive service components
  - keep a secure credential management model
  - coordinate compliance and accreditation – and help meet EU privacy stuff in just one place to ease adoption
- *Optional elements: ability to obtain CLI tokens (via ssh agent or even U/P); implicit AuthZ*

Enrolment and issuance [4.2]

- Users could enroll directly, but are in practice using a Master Portal/Credential Manager
- The credential manager is *explicitly trusted* by the RCauth CA service
  - exchange of OIDC client secret to authenticate
  - 'need to know': (master) portals will hold user credentials, and we need to protect users per the PKP Guidelines
- CA web server checks the incoming assertions from the IdP filter
  - Uses CILogon/OAuth4MP software based on the Shibboleth SAML implementation over server-side TLS
  - Connected for now to the SURFconext WAYF
  - ... and yes, we check the SAML signature ;-)

When moving to wider support of eduGAIN

- WAYF IdP filter check the incoming SAML2Int
  - Use multi-domain WAYF over server-side TLS
  - Based on SimpleSAMLphp implemenation with custom filters
  - ... and yes, also here we'll check the SAML signature
- FIMS IdPs: leverage existing infrastructures
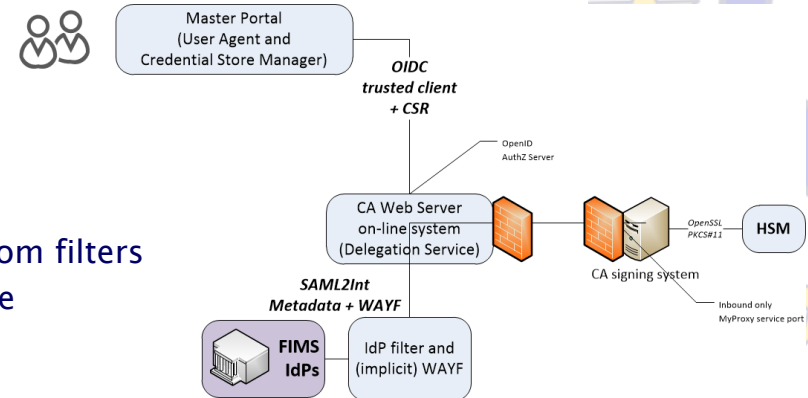
Trusted Credential Stores

- In easing access to e-Infrastructures incrasingly credential management systems appear: UnityIDM, MyProxy hosting, AARC's Master Portals, ...
- Issuing Authorities promoting PKP guidelines (e.g. RCauth.eu) need framework to assess explicitly-connected portals

- Guidance on what constitutes an 'acceptable' credential store
- Guidance for operators on 'community best practice'

↓ Naming
↓ Operational Requirements
    ↓ Protection of stored key material and activation data
    ↓ Life time considerations
    ↓ Network configuration
    ↓ Incident Response
↓ Site security
↓ Publication and Repository responsibilities
↓ Audits
↓ Privacy and confidentiality

https://wiki.eugridpma.org/Main/CredStoreOperationsGuideline

RCauth sustainability

- Somewhat amazingly, many of the e-Infrastructures in Europe all want to 'have a share' in running the service

- Support for now ensured by the Dutch National e-Infrastructure (Nikhef, SURF) – will likely transition to a collaborative entity with own separate PMA and redundant distributed infrastructure - details to be worked

eu gridpma

The Reverse: the IGTF-to-eduGAIN bridge

"the ultimate assured-identity IdP of last resort"

- authenticate with any IGTF accredited client cert
- known to the (SAML2int, R&E) eduGAIN community via GRnet
- with assurance information in ePAss (and 2FA set in ACCR)
- asserts REFEDS R&S and Sirtfi (based on IGTF qualification)

will appear as https://edugain-proxy.igtf.net/

R&S + Sirtfi tags should enable many research SPs to trust you

work by Ioannis Kakavas (GRNET) and Christos Kanellopoulos –
see github for implementation of SimpleSAMLphp module

Developing scalable policy models in light of the Blueprint: Snctfi

✓ allow proxy operators to assert 'trust marks' based on known SP properties

✓ Develop framework recommendations for RIs for **coherent policy sets**
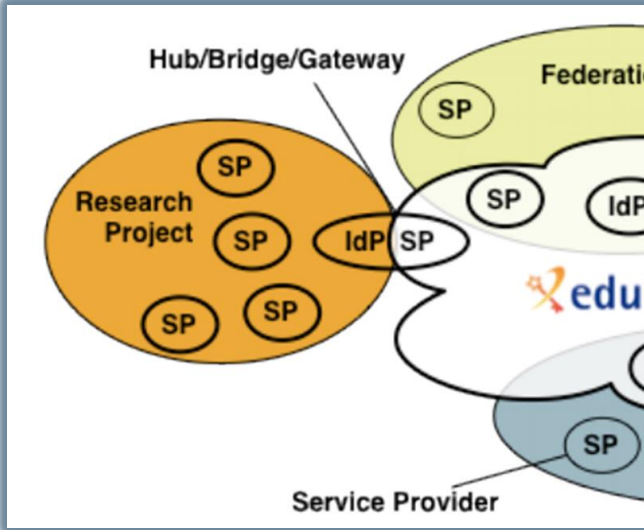
evaluate with the SP-IdP-Proxies in pilots **based on the Blueprint Architecture**

Collaborate in **WISE, IGTF & FIM4R** to get endorsement

Complementary work: Accounting Data Exchange Protection for Infrastructures

Many SPs are alike

Policy frameworks for collective service providers ***Shared use of and collaboration on reputation services, together in FIM4R***

Graphics inset: Ann Harding, SWITCH   *Proxying IdPs to SPs is part of the BPA, with e.g. the RCauth CPS as policy example*

10

More policy harmonisation and development in AARC2

Reflected in updated AARC2 structure

- Operational security capabilities and Incident response in federations – beyond Sirtfi v1

- **Service-centric policies**: traceability & accounting, privacy, gateway operations & proxies

- **e-Researcher-centric policies**: alignment of AUPs and templates, authentication assurance, community attribute management models and provisioning

- Policy Engagement and Coordination: contributes to Community Engagement, provision of policy expertise to the Competence Centre, promotion of best practices globally (WISE, FIM4R, IGTF, REFEDS), easing **end-to-end coordination** across the chain

- Structuring the **exchange of information** amongst SP groups

Video-supported vetting

"[Vetting] should be based on a face-to-face meeting and should be confirmed via photo-identification and/or similar valid official documents." *(BIRCH and CEDAR APs)*

- Many support explicit F2F only, yet designate RAs in different ways
- Video-supported and notary-public postal mail & video: BR, TR
- Government records: some TCS subscribers (universities with access to these databases)
- Kantara LoA 2: some TCS countries (SE) for some of their applicants
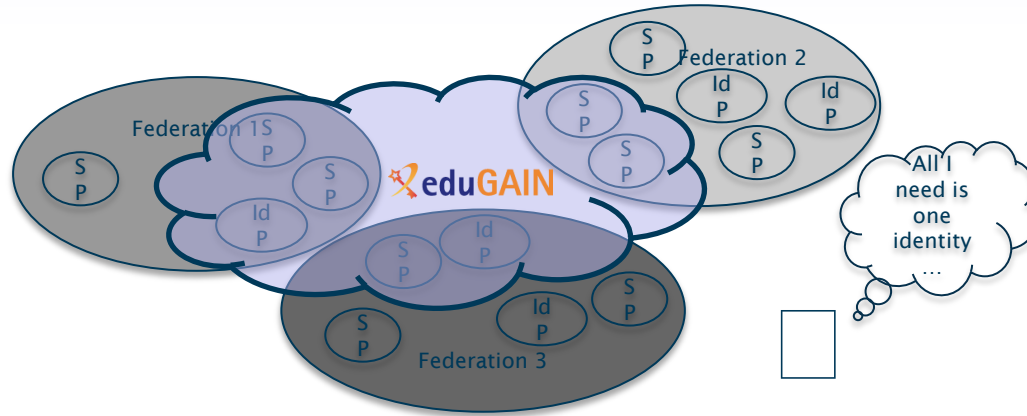
Evolution of guidance

"The aim should be to stay within the 'bandwidth of trust' described in the current text: between the (possibly worthless) notary-public attestations, and the more trusted real in-person hand-shake vetting."

"If appropriate compensatory controls are in place and we can protect same-person continuity (non-reassignment) as well as traceability, it should be viable. Compensatory controls have some 'hard' requirements in the model process described in the Wiki:"

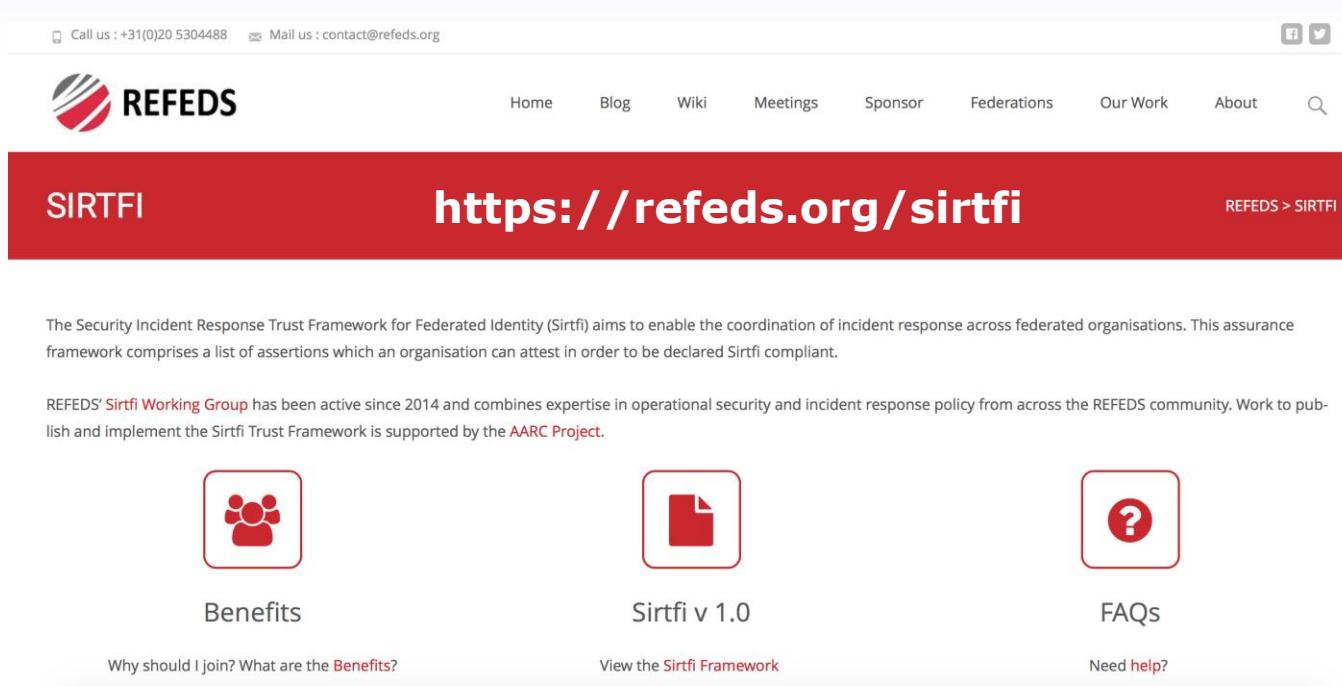**http://wiki.eugridpma.org/Main/VettingModelGuidelines**

It is important that this be described and reviewed in each case, so the proposal is that "The following is also considered to be an acceptable process for implementing method 2 - if so acceptably documented in the CP/CPS and endorsed by the accrediting PMA"

Evaluation leads to mixed results ...

- Realistic test by CESNET (who really wanted to use it) resulted in "unable to decide on validity" over skype
- Test by German bank (using trained verificators and with flashlight on smartphone) was successful
- Really depends on training, knowledge of valid documents, and some specific tests

Photo Credit: Sonnenstaatland

For examples see also e.g.: National Document Fraud Unit, UK Home Office *Guidance_on_examining_identity_documents_v._June_2016*

Sirtfi and R&E federation assurance

Clearly an inviting vector of attack… luckily, this was noticed several years ago!

Find out more on Sirtfi

https://refeds.org/sirtfi

Call us : +31(0)20 5304488   Mail us : contact@refeds.org

REFEDS

Home   Blog   Wiki   Meetings   Sponsor   Federations   Our Work   About

SIRTFI   REFEDS > SIRTFI

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant.

REFEDS' Sirtfi Working Group has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC Project.

Benefits

Why should I join? What are the Benefits?

Sirtfi v 1.0

View the Sirtfi Framework

FAQs

Need help?

More R&E developments on assurance

- REFEDS Assurance WG
  - Baseline comes out of Mikael's AARC work **https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLl3UJbaOX5o9eLtsyBI**
  - beyond the baseline: "Cappucino" (BIRCH), "Espresso" (EIDAS substantial, KI LoA 3)
- EGI ad-hoc assurance evolution
  - Use cases identified for several levels – needs alignment
  - There is a noted difference between 'open guest IdPs' and controlled university IdPs, but these cannot be identified now
  - UKAMS publishes UnitedID to edugain: 'edugain' is not enough
  - But hardly any need for >>BIRCH LoA (only some biomed cases)

GFD.225

- Now done – Jens also picked the last nits:

Interoperable Certificate Profile

Status of This Document

This document provides **recommendations** to the OGF community.

Obsoletes

This document supersedes GFD.125 [1].

- published now: http://www.ogf.org/documents/GFD.225.pdf
- Also there the reviews should probably check compliance
- Ursula Epting re-wrote the auditing spreadsheets
  see www.eugridpma.org/agenda/39/
- How to progress with future updates?

IPv6 status

- New continuous v6 CRL monitor
  http://cvmfs-6.ndgf.org/ipv6/overview.php

- 41 CAs offer working v6 CRL (down from 43 in Oct 2016 ☹)
  - but: also 1-2 CAs that give AAAA record but the GET fails …
  - Still 52 broken endpoints support only legacy IP
  - the ClouldFlare cache solution is trivial, so please either …
  - dl.igtf.net *can* act as v6 source-of-last-resort for RPs that need it

And really: get rid of SHA-1 – it's broken!

The first collision for full SHA-1

Marc Stevens[1], Elie Bursztein[2], Pierre Karpman[1], Ange Albertini[2], Yarik Markov[2]

[1] CWI Amsterdam
[2] Google Research
info@shattered.io
https://shattered.io

Do we *still* have SHA-1 EECs??

- FNAL KCA
- REUNA?
- …?

Abstract. SHA-1 is a widely used 1995 NIST cryptographic hash function standard that was officially deprecated by NIST in 2011 due to fundamental security weaknesses demonstrated in various analyses and theoretical attacks.
Despite its deprecation, SHA-1 remains widely used in 2017 for document and TLS certificate signatures, and also in many software such as the GIT versioning system for integrity and

https://shattered.io/static/shattered.pdf

For more details,
see https://www.eugridpma.org/meetings/,
but meanwhile:

UPCOMING MEETINGS

Upcoming events

EUGridPMA 40, Ljubljana　　**May 22 – 24**

I2 Global Summit　　April 23 - 26
TNC2017, Linz, AT　　May 29 – June 2 (REFEDS: Monday!)

EUGridPMA41　　September 2017