

Developments in the IGTF and EUGridPMA – an update

David Groep
davidg@nikhef.nl



*enabling an interoperable
global trust federation*

part of the work programme of EOSC-Hub and GEANT 4-3

*the work has received co-funding from the
Horizon 2020 programme of the European Union*



*co-supported by Nikhef and the Dutch
National e-Infrastructure coordinated by SURF*



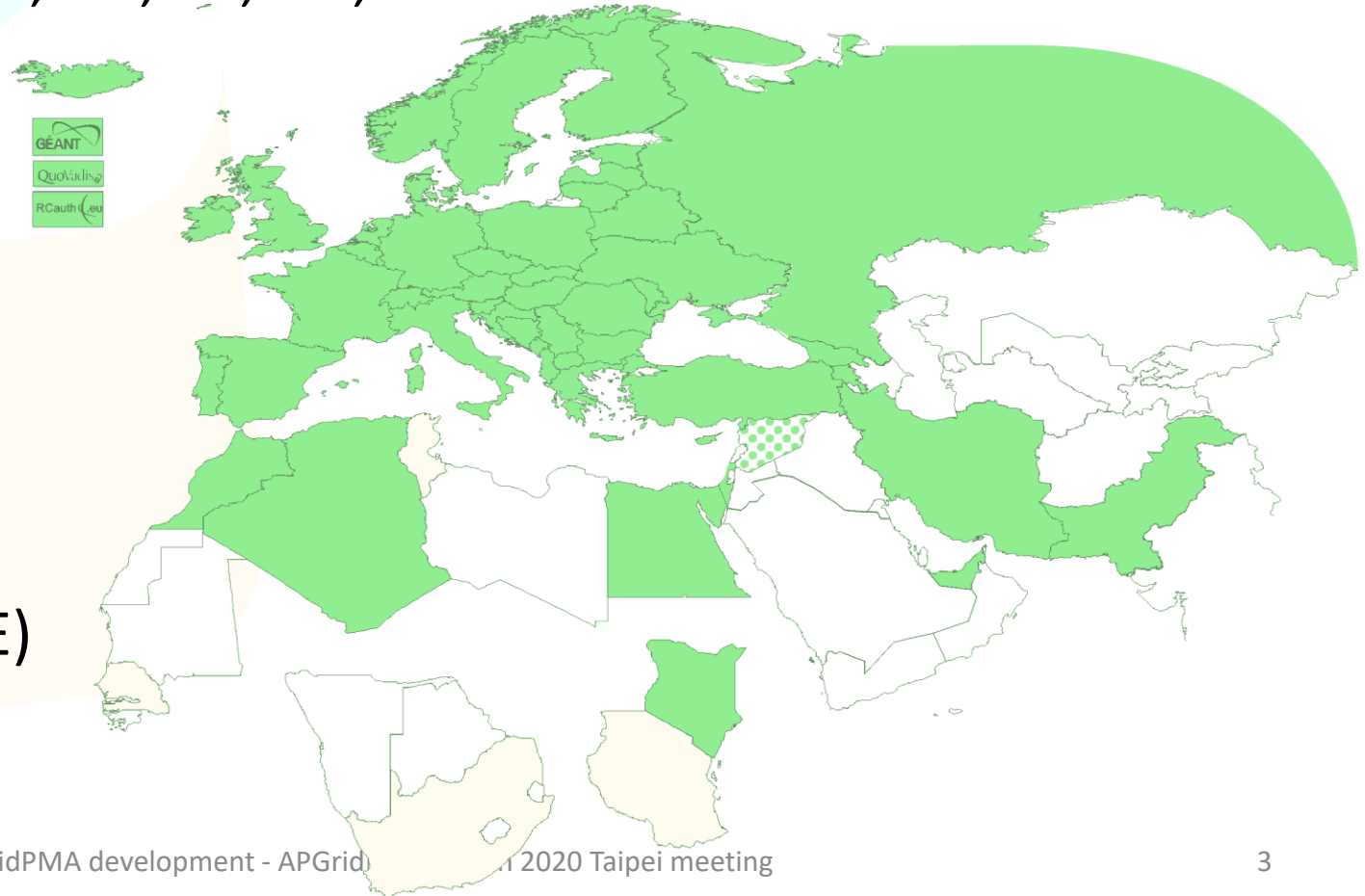
For today ...

- EUGridPMA membership and updates
- IGTF Relying Parties in OIDC and OIDCfed
- GEANT TCS Generation 4 implementation
- Assurance Profiles
- Attribute Authority operations AARC G048
- Communications Challenges: RATCC4 and the SCCC-JWG



EUGridPMA – membership and evolution

- Europe: CZ, DE, DK, ES, FI, FR, GR, HR, HU, IT, NL, PL, PT, RO, SE, SI, SK; AM, GE, IS, MD, ME, MK, NO, RS, RU, TR, UA, UK and the GEANT TCS
- Middle East: AE, IR, PK
- Africa: DZ, EG, KE, MA
- CERN, RCauth.eu, QuoVadis (BM), DigitalTrust (AE)



Membership and other changes

- Responsiveness challenges for some members
 - PLEASE take care to renew your trust anchors in time, as well as your CRLs
 - EG-EUN now temporarily withdrawn for availability reasons*
- Identity providers: both reduction and growth
 - RCauth.eu distributed operations (GRNET, STFC, Nikhef) *using a shared key (and some smart border-guard-proof distribution)*
 - AustrianGrid discontinued, INFN CA by 2021
- Self-audit review
 - Cosmin Nistor as review coordinator
 - Self-audits on schedule for most CAs

		Specific Policies and Practices			
TR-Grid CA (Turkey) <i>(Authority member)</i> (TACAR OK)	Feyza Eryol	CA TRGrid (accredited:classic): CERT CRL concerns: ca@grid.org.tr A2:31:9E:C8:90:AF:D9:6D:F4:4A:59:31:F2:E6:D2:D5:39:EC:1D:F0 Generic CP and CPS statements	2005-09-29	2016-01-20	2016-01-20 (0.2yr)
Trans-European Research and Educational Networking Association (TERENA) <i>(Relying Party member)</i>	Licia Florio (277707CC)	CP and CPS are not relevant About TERENA: http://www.terena.org/	2004-04-01	2015-09-09	
UK e-Science CAs <i>(Authority member)</i> (TACAR OK)	Jens Jensen (9210F006) David Kelsey	CA UKeScienceRoot-2007 (accredited:classic): CRL concerns: support@grid-support.ac.uk A1:39:B0:F3:04:6C:0B:F9:F5:0A:1B:33:00:06:4F:83:6B:7D:4F:3E CA UKeScienceCA-2A (accredited:classic): CRL concerns: support@grid-support.ac.uk 41:C7:C4:A0:31:F7:07:02:81:C7:61:D5:7E:92:48:01:DF:87:C9:06 CA UKeScienceCA-2B (accredited:classic): CRL concerns: support@grid-support.ac.uk DB:D9:5A:B4:E9:AD:74:26:E0:33:68:AA:B1:77:CC:5B:64:B2:CB:0E Generic CP and CPS statements	2000-12-04	2016-01-20	2014-01-14 (2.2yr)
Ukrainian Grid CA <i>(Authority member)</i> (TACAR FAILURE)	Sergii Stirenko Oleg Allenin	CA UGRID (accredited:classic): CERT CRL concerns: ca@ugrid.org 21:E7:0D:EE:D7:57:B6:47:A6:F5:04:29:76:81:FE:CD:E8:48:DD:9A Generic CP and CPS statements	2008-02-14	2013-09-11	2013-09-11 (2.5yr)







OIDC Federation

SUPPORTING RELYING PARTIES IN OIDC

OpenID Connect: registering clients does not scale...

Show OpenID Connect Client

Name	hekel.nikhef.nl
Description	Hekel using mod_auth_openidc
Client id.	_f6bfe81892e680e4ecfc3b41ecf1a15d141c0d106b 
Client secret	_____ 
Auth. source	saml2
Redirect URI	https://hekel.nikhef.nl/rp/redirect_uri
Scopes	openid profile email assurance
← Return ↻ Reset secret	

configuration of a (test) client on the Nikhef institutional OP sso.nikhef.nl



OIDC Federation use cases for communities

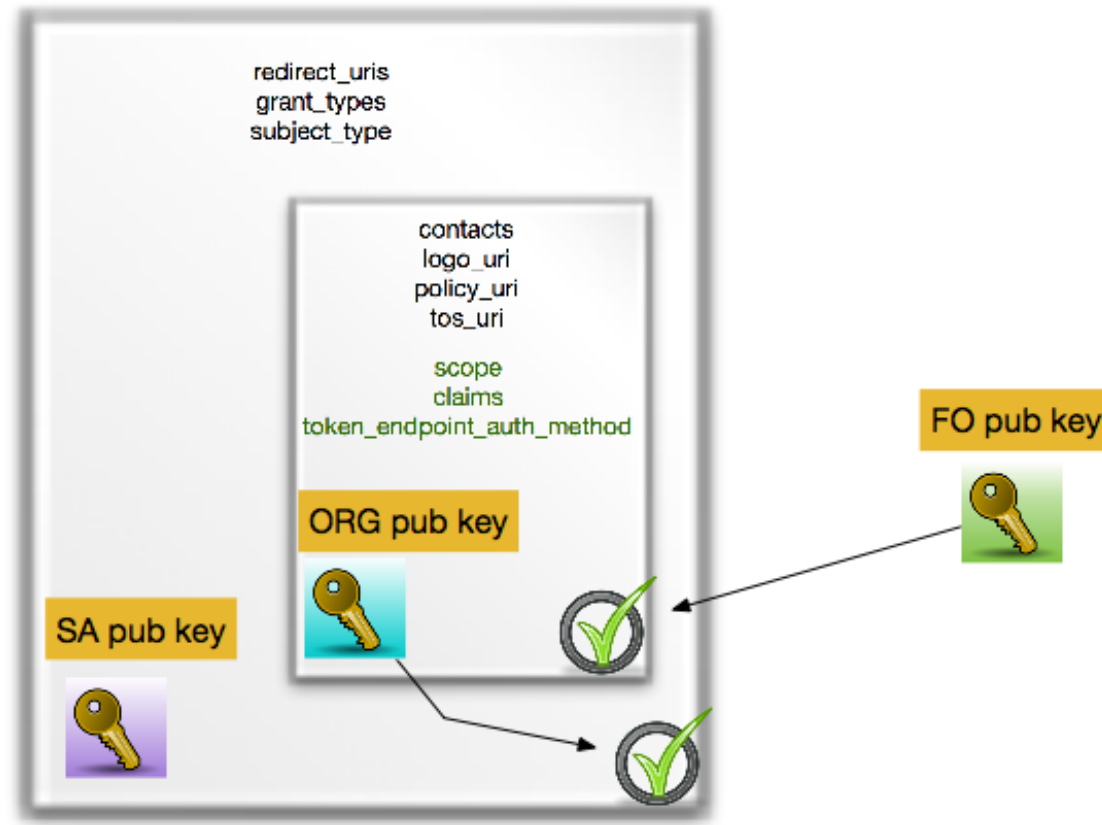
Why did we embark on OIDC Fed for global e-Science?

- EOSC-HUB registration of clients
goal for EGI and EUDAT is a scalable and trusted form of OIDC usage.
Today $< O(50)$ clients; next year maybe $O(100-1000)$?
cloud-based services (containers, microservices) could push that to millions
- CILogon (and XSEDE) use cases see need for a set of policies and practices that support a 'trust anchor distribution'-like service targeting OIDC OPs and RPs and where RPs that are 'in the community' can be identified as such
- ELIXIR (and the Life Sciences) AAI expect growth in # OIDC RPs as AAI extends beyond just ELIXIR and into other biomedical RIs – potentially dynamically created
- All of these need a policy framework, on both the (infrastructure) OPs and on the RPs
- This is the community that traditionally also relied on the IGTF trust anchor distribution

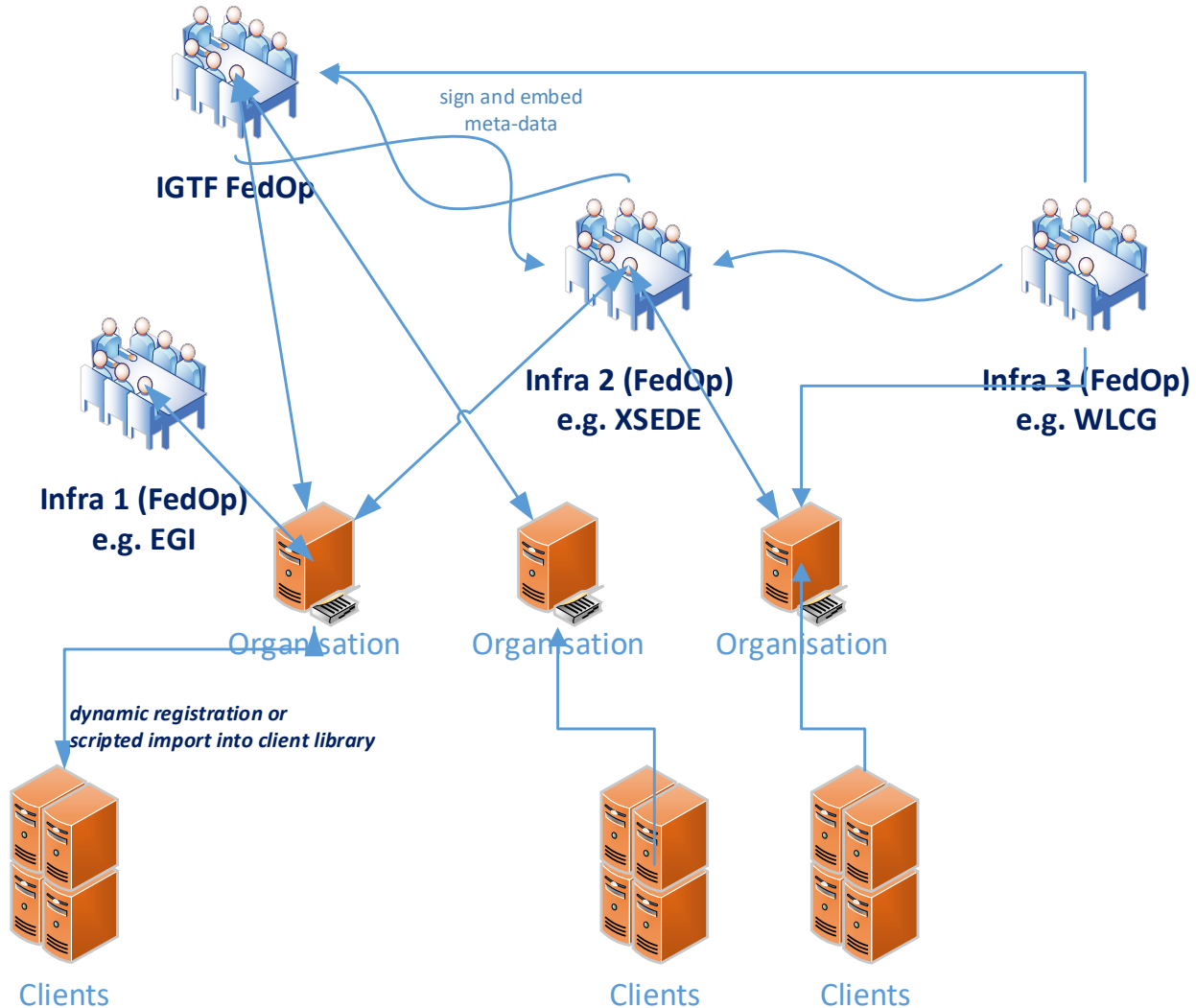


OIDCfed is basically signing a tree of entities with extensions

we kind-of know building trees and meshed of signed entities work – is this ‘just recast it JSON’ ?



Or can we do without a single one to rule them all?



- today the RIs and EIs trust the IGTF trust anchors and *may (but do rarely)* add their own
- Can the 'federation' be the community and import a commonly trusted set?
- Can the IGTF allow devolved registration *provided* that the trusted organisations implement the same policy controls *Snctfi* and the proper *Assurance Profiles*?

and this works now: oidcfed.igt.f.net

```
dauidg@x13dauidg ~  
$ curl -s http://oidcfed.igt.f.net/.well-known/openid-federation  
eyJrawQioiJOawtoZwYvSudURiBUZXNOiIiwYXNlIjoiRVM1MTIifQ.eyJpc3MiOiJodHRwczovL29pZGNmZWQuawd0Zi5uZXQvcn9vdCIsInN1YiI6Imh0dHBzOi8vb2lkyZzI7ZC5pZ3RmLm51dC9yb290IiwiaWF0IjoxNTc1OTkwNDMxLCJleHAiOjE1NzU5OTQwMzEsImp3a3MiOnsia2V5cyI6W3sia3R5IjoirUMiLCJrawQioiJOawtoZwYvSudURiBUZXNOiIiwidXNlIjoic2lnIiwiYXNlIjoiRVM1MTIiLCJ4IjoivQvknXFxdndnV216aTNYOGZIM2R1U1JCSmZTlM3SxpLV1hbQ2tKRwEdV5aEFxZjVEcWxb1ZwYm5udXRjvXlFM3ZXZxVAVzV0F4WUtoMDVjc0N0qWndkLlSInkioiJBWFFVf5Y185QW7obDBEMj1kN1dULTFEB3hrZn15duJBM2oxNGS50DB2N1JqeC1WRXcyd21YSE5XY2M5EXmbHBhTDlMLVA5ekFCZ2htRwYjRCckNtIiwY3J2IjoUC01Mjeifv19LcJtZXRhZGFoYSI6eyJmZWRlcmF0aw9uX2VudG10eSI6eyJmZWRlcmF0aw9uX2FwaV9lbmRwb2ludCmImh0dHBzOi8vb2lkyZzI7ZC5pZ3RmLm51dC9yb290NDMvY2l1bm1uZy1zZXJ2aWNlIn19fQ.ABZ-XA707Ia5JdGOWBMthooidjE8tT5mMoWofkGcyA2vV9BtAbacZTStChLEtD44T8ttDjeuZInfzLLgShBRF7APfexXQOZSp1dJCdxq1qwMyWdOPk16W7Kz16F1k7qhDXfmq3HXJ_A0KXCNYytLOJWBj0yqzRidSeG5Joc13e  
dauidg@x13dauidg ~  
$ echo "eyJrawQioiJOawtoZwYvSudURiBUZXNOiIiwYXNlIjoiRVM1MTIifQ" | base64 -di 2>/dev/null  
{ "kid": "Nikhef/IGTF Test", "alg": "ES512" }  
dauidg@x13dauidg ~  
$ echo "eyJpc3MiOiJodHRwczovL29pZGNmZWQuawd0Zi5uZXQvcn9vdCIsInN1YiI6Imh0dHBzOi8vb2lkyZzI7ZC5pZ3RmLm51dC9yb290IiwiaWF0IjoxNTc1OTkwNDMxLCJleHAiOjE1NzU5OTQwMzEsImp3a3MiOnsia2V5cyI6W3sia3R5IjoirUMiLCJrawQioiJOawtoZwYvSudURiBUZXNOiIiwidXNlIjoic2lnIiwiYXNlIjoiRVM1MTIiLCJ4IjoivQvknXFxdndnV216aTNYOGZIM2R1U1JCSmZTlM3SxpLV1hbQ2tKRwEdV5aEFxZjVEcWxb1ZwYm5udXRjvXlFM3ZXZxVAVzV0F4WUtoMDVjc0N0qWndkLlSInkioiJBWFFVf5Y185QW7obDBEMj1kN1dULTFEB3hrZn15duJBM2oxNGS50DB2N1JqeC1WRXcyd21YSE5XY2M5EXmbHBhTDlMLVA5ekFCZ2htRwYjRCckNtIiwY3J2IjoUC01Mjeifv19LcJtZXRhZGFoYSI6eyJmZWRlcmF0aw9uX2VudG10eSI6eyJmZWRlcmF0aw9uX2FwaV9lbmRwb2ludCmImh0dHBzOi8vb2lkyZzI7ZC5pZ3RmLm51dC9yb290NDMvY2l1bm1uZy1zZXJ2aWNlIn19fQ" | base64 -di 2>/dev/null  
{ "iss": "https://oidcfed.igt.f.net/root", "sub": "https://oidcfed.igt.f.net/root", "iat": 1568975528, "exp": 1568979128, "jwks": { "keys": [ { "kty": "RSA", "use": "sig", "alg": "RS512", "n": "mXnlu604kEPtMeNQNn-q1Mey4FzXRxzJb4WVfZ4t0E2T5l6fzQm0WizK1NgcACFwtQ3Wd1LkzsF03GgYntsuM7X4CxrEYV08-d0vc5IIMv1HmF8Sv4vTRn8TMiWSscNPNRu0Tz4nl7 XvwmlIVPFh75sSF7nt", "crv": "P-521" } ] }, "metadata": { "federation_entity": { "federation_api_endpoint": "https://oidcfed.igt.f.net:443/signing-service" } } }
```

Ask Jouke for all details

```
{ "iss": "http://[redacted]/federations",  
  "sub": "http://[redacted]/federations",  
  "iat": 1568975528,  
  "exp": 1568979128,  
  "jwks": {  
    "keys": [  
      {  
        "kty": "RSA",  
        "use": "sig",  
        "alg": "RS512",  
        "n": "mXnlu604kEPtMeNQNn-q1Mey4FzXRxzJb4WVfZ4t0E2T5l6fzQm0WizK1NgcACFwtQ3Wd1LkzsF03GgYntsuM7X4CxrEYV08-d0vc5IIMv1HmF8Sv4vTRn8TMiWSscNPNRu0Tz4nl7 XvwmlIVPFh75sSF7nt",  
        "crv": "P-521" } ]  
    }  
  },  
  "metadata": {  
    "federation_entity": {  
      "federation_api_endpoint": "http://uvm-[redacted]-signing-service"  
    }  
  }  
}
```



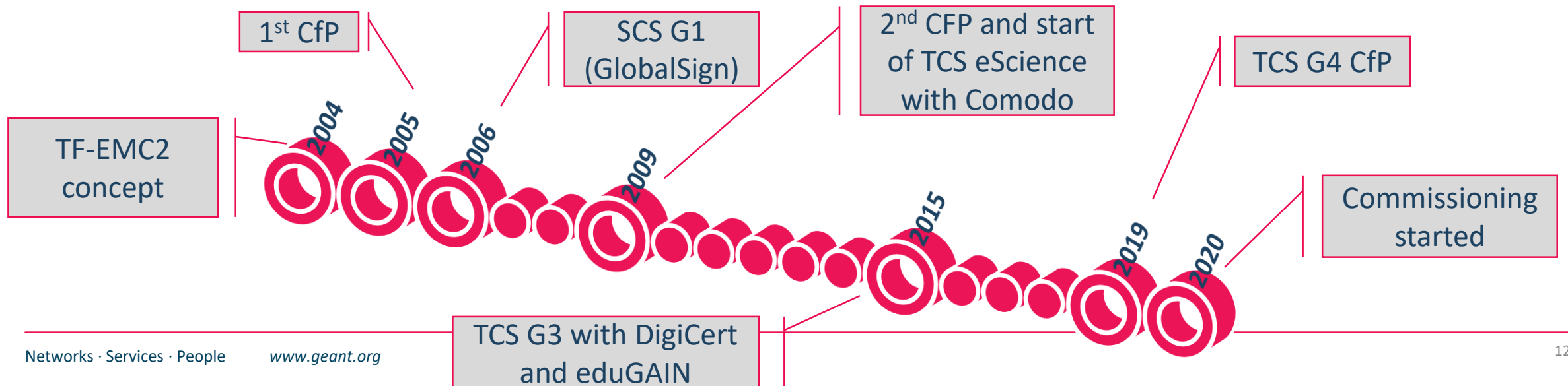


Generation 4 Trusted Certificate Service – issuing provider update

GEANT TCS SERVICE UPDATE

15 years of TCS service

- based on a concept by Jan Meijer back in 2004
- driven primarily by the NREN constituency, but with the eScience use cases very much in mind
- NREN (GEANT constituency) requirements on public trust, today esp. EV, but also eIDAS
- in a way that scales to 45 countries and ~100k active certificates today, increasing steadily
- and also ~10000 organisations, most of which cannot deal with certificates ... or with much change
- now going to its 4th iteration: GlobalSign, Comodo, DigiCert, ... and now Sectigo again



- service is ultimately driven by the GEANT members: 45 national R&E network organisations
- wide range of inputs: some countries adore Qualified Certificated and eIDAS, others don't care
- some countries really need a native-language interface (like .fr, .es, ...), others don't care (.nl, .se)
- stakeholders regard EV as mandatory, and many stakeholders pushed for ultimate stability – since the subscribers have actually no knowledge of PKI, nor of validation, and certainly not about chaining
- eScience use cases are important for many, but certainly *not* the only driving factor in the game

Result of the formal 3-round consultation sessions with the NRENs (22 / 40 participated, April 2019)

- one set of knock-out minimum requirements (which then cannot be materially changed any more)
- a long list of 'quality' criteria, with a strong focus on compliance (CABF), public trust continuity, all manner of interfaces to the service, and personnel & contract management

Certificate profiles



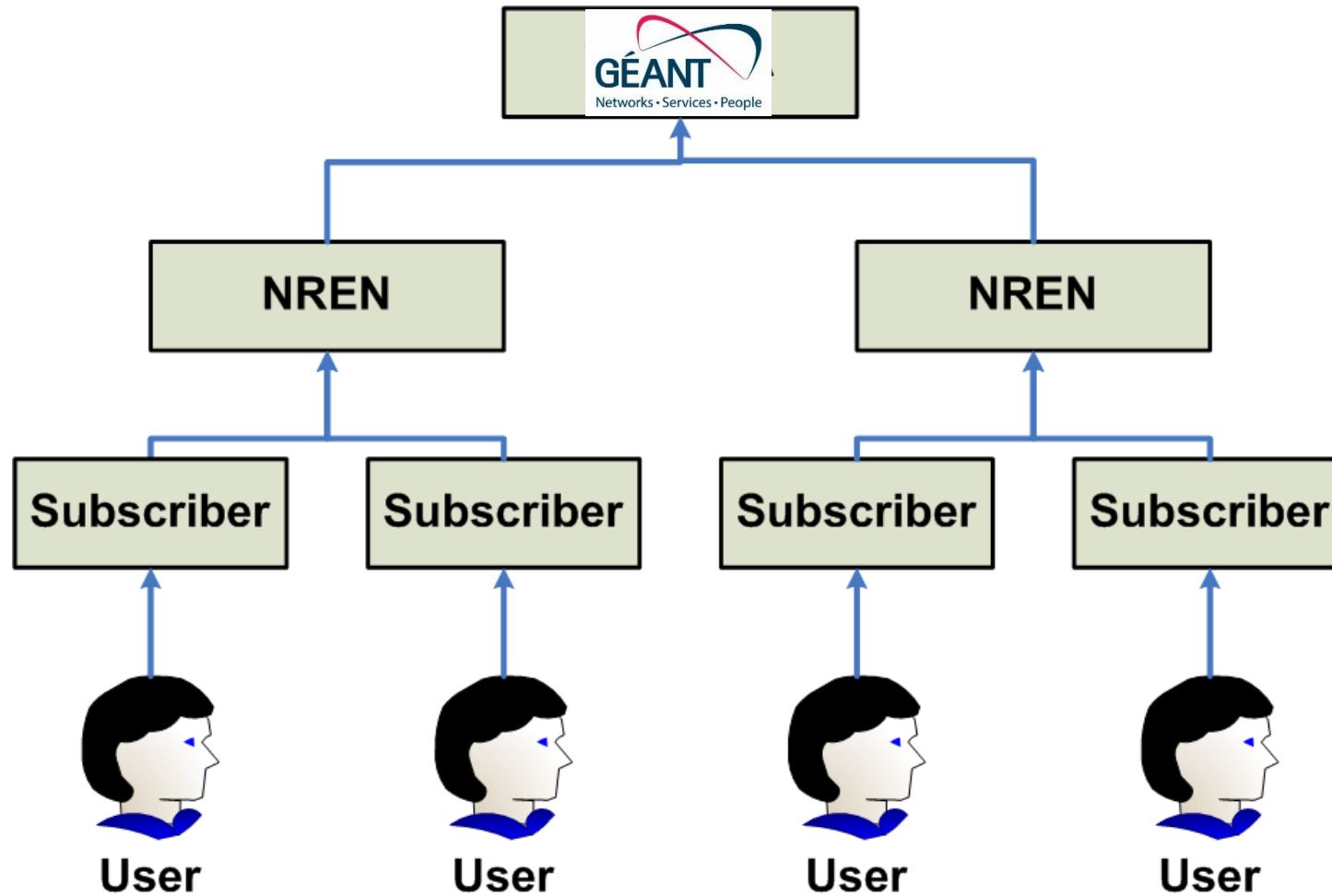
OV TLS Server	BR OV validated multi-domain with mixed SANs
OV TLS wild	BR OV validated multi-domain with mixed SANs combining both wildcard and non-wildcard domain names
EV TLS	BR EV validated multi-domain with mixed SANs
Personal webClientAuth and S/MIME	End-user personal certificate recognised by the major MUAs suitable for identifying the users real name
Personal webClientAuth IGTF and S/MIME	End-user personal certificate adhering to IGTF profile (using IA5String representation of the name with unique prefix /DC=org/DC=terena/DC=tcs/...), suitable both for authentication, and also including validated name and email address
Personal Robot webClientAuth IGTF and S/MIME	End-user personal software agent certificate adhering to IGTF profile (like above) and Robot Profile, suitable both for authentication, and also including validated name and email address
Robot Email webClientAuth IGTF and S/MIME	E-mail validated software agent certificate adhering to IGTF profile (like above) and Robot Profile, suitable both for authentication, and also including validated email address
IGTF OV TLS Server	BR OV validated multi-domain with mixed SANs including unique prefix "/DC=org/DC=terena/DC=tcs/..."
Document Signing	Adobe AATL compliant signing certificate
Code Signing	Conventional code signing certificate recognised by Oracle, MSFT, &c
EV Code Signing	BR EV Code Signing certificate recognised by MSFT &c

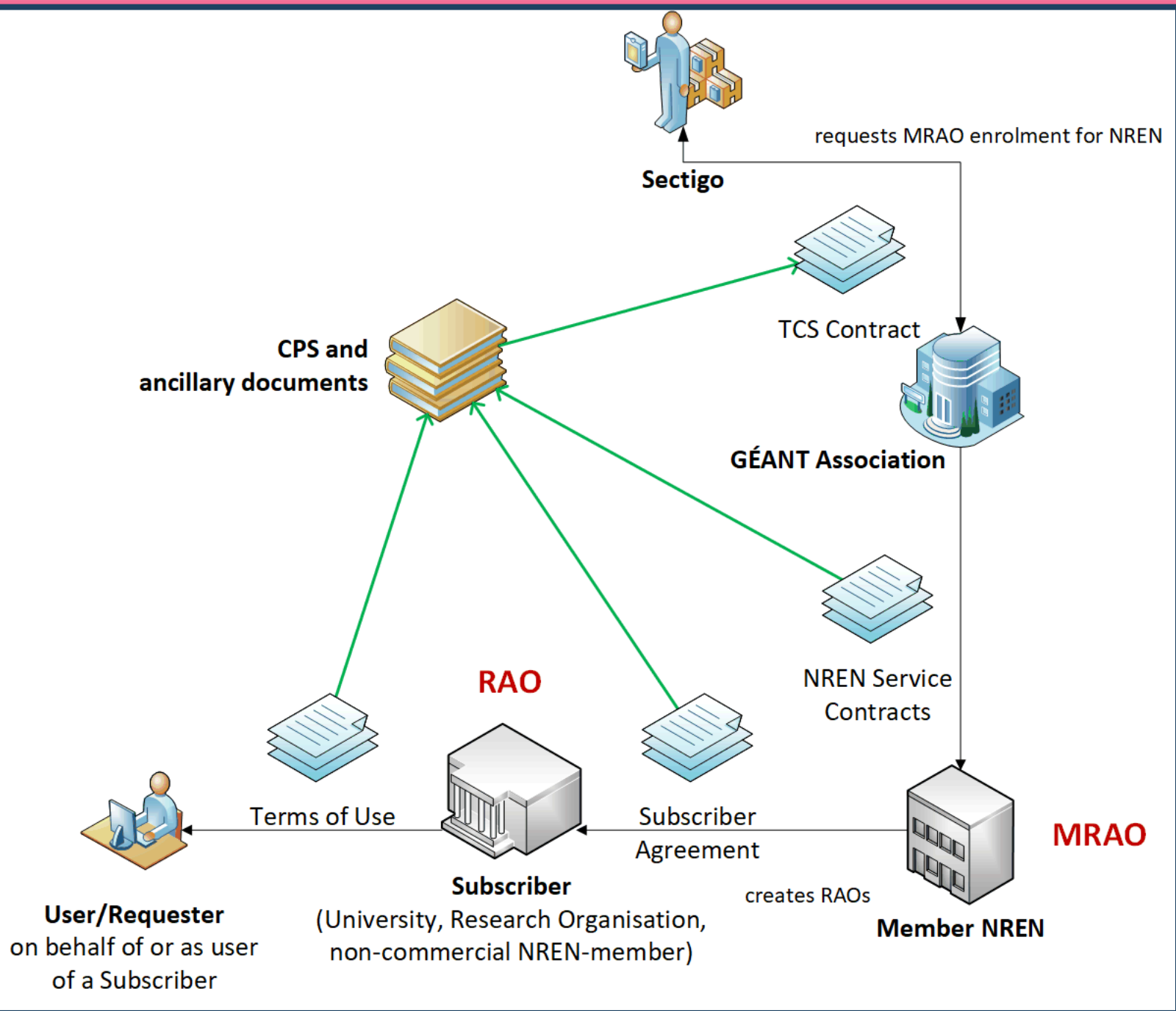
TCS is a GEANT service – with the TCS PMA defining the profiles and policy



- TCS PMA drawn from the wider GEANT community (NRENs as well as individual orgs)
- Current PMA members ... some of whom you will have seen
 - Teun Nijssen (SURF, NL)
 - Dominique Launay (Renater, FR)
 - Kurt Bauer (ACONET, AT)
 - Kent Engström (SUNET, SE)
 - David Groep (Nikhef, NL)
 - Nicole Harris (GEANT)
 - Sigita Jurkynaite (GEANT)
- GEANT service manager is nowadays Sigita Jurkynaite

The basic structure remains the same ... again!





Assurance levels

Host certs all meet CABF OV requirements, which actually exceed 'IGTF Classic' a bit

- OV validation requires DCV, which is stronger than the RA checks minimally required
- the IGTF+public trust combination is getting more important for S3/cloud like deployments

User and personal robot certs

- SAML process, and the eligibility checking by the subscribers (organisations), remains the same *urn:mace:[terena.org](https://www.terena.org):tcs:personal-user* in attribute *eduPersonEntitlement*
- real name of the person – by the subscriber agreement and CP/CPS this goes beyond R&S assurance
- manual side-process may remain just like today, based on data entry by the 'RAO/DRAO' in SCM as per <https://wiki.geant.org/display/TCSNT/Documentation> 'non-SAML issuance model process'
- the CP/CPS requirements though the Subscriber Agreement meet IGTF BIRCH
- *and this time we will put the right OIDs in the policy extension ...*

All stuff audited already for CABF/WebTrust things (SSL certs) and similarly for the 'S/MIME' use cases



And the CPS says ...



The CA or an RA confirms that the following are consistent with the application and sufficient to identify a unique individual:

(a) the name on the government-issued photo-ID

DigiCert or an RA may confirm an address by issuing credentials in a manner that confirms the address of record or by verifying knowledge of recent account activity associated with the

refer

(b)

(c)

15

1. I

pro

ent

aut

form

2. T

pho

per

be t

the

tele

gov

suc

ID

(e.g

utili

an

thro

with

databases.

For the invite-based, direct (classic) process

1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent (or entity certified by a state, federal, or national entity as authorized to confirm identities) with presentment of a reliable form of current government-issued photo ID.

For the Subscriber expresses that an identity has been properly validated by setting a specific value in the App ***eduPersonEntitlement*** attribute of the Requester's identity in the Subscriber's IdP

was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo-ID, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret.



Naming and real names

- › Name uniqueness method is TCS specific:
 - › Responsibility is placed on the Subscriber and its IdP
 - › The unique identifier is scoped to the Organisation anyway

*"The Subject Distinguished Name of a TERENA eScience
Pe by including an **Identifier** that uniquely and persistently
by represents the Requester in the IdP of its Subscriber*

*rep
Su
af
TE*

*Almost universally we will use ePPN for this
But some federations/subscribers may use ePTID or so*

*The Identifier must be traceable to a Requester for at least
as long as the certificate issued to the Requester is valid. If
the traceability from Identifier to Requester is lost, the
Subscriber will ensure the Identifier will not be reused."*

- › Rest is inherited from the upstream CPS again

Slide 33

We have been there before ... but not quite

The TCS G2 had essentially the same back-end provider (then called Comodo)

- which we accredited in 2010 (hosts) and 2012 (personal)
- but where personal certs were issued off a central TERENA-managed service ('Confusa')

This now all moves to the selected provider

- of course we are slightly different from the InCommon use case
... *which only does server certs via SAML* and not personal or S/MIME
- we require the personal issuance based on SAML to be hosted at the provider as well
- maybe one-per-NREN, and not a single global instance for all of TCS, but still this requires multi-lateral federation
- Sectigo now working on an implementation (fall-back scenarios are under study, though ...)

Phasing is tight

- contract final as of the last days in December 2019
- Jan 6th 2020 started early-commissioning phase
 - challenges in this phase include both the new web-management interface, but also getting the enrolment and provisioning flow right
 - there are *a lot of orgs and domains* to go through, with some interesting DBA vs. legal names
 - certificate profile definition (e.g. making sure Robots work even if they are not in the InCommon scheme)
- subsequent phases in February & March
 - multi-lateral eduGAIN SAML meta-data parsing (done for SCM-managed login)
client cert portal based on SAML attributes, auto-provisioning security (pending ...)
 - confirmation of exact profiles and all relevant controls re-implemented in new system + API
 - **all dedicated intermediates for the (small number of) chains available for distribution (awaiting EEC profiles)**
 - translation of interfaces and messages to all relevant languages
- End of March: commissioning complete and ready for large-scale roll-out
- End of April: all subscribers on-boarded, trained, and ready is issue
- End of September 2023: last TCS G3 certificates will expire (for IGTF: end of July 2021)

Main relevant items for the IGTF trust

- subscriber validation for host/server certs as well as the model for personal/robot **remains the same**
- the contractual obligations and **adherence to the TCS CP/CPS remains** the same
and the TCS CP/CPS is already today written as an incremental one, so need not change except for the same of the new upstream provider:
 - “No further stipulations beyond those set forth by the CA Operator.”
- now on top of Sectigo’s CP/CPS 5.1.5 (<https://sectigo.com/uploads/files/Sectigo-CPS-v5.1.5.pdf>)
see also <https://sectigo.com/uploads/files/Certificate-Subscriber-Agreement-v2.2-click.pdf>
- **it is a new hierarchy**, but it shares some of the HLCAs with the InCommon IGTF Server CA
- we will aim to **keep the current prefix** /DC=org/DC=terena/DC=tcs the same
- **issuer names will change** (since these show visibly in the UX), and without É (E-acute) in there
- will need to distribute the new chains in March
updates to the CP/CPS under review by Reimer and Scott in EUGridPMA

1.2 Document Name and Identification

This document is the TCS Server & CS CAs CPS version 2.0, which was approved for publication on February 2015 by the TCS Policy Management Authority. This document is identified by the following unique registered object identifier: **1.3.6.1.4.1.25178.2.1.2.0**.

The CPS is a public statement of the practices of the TCS Server & CS CAs and the conditions of issuance, revocation and renewal of a certificate issued under the TCS Server & CS CAs PKI hierarchy. Revisions to this document have been made as follows:

Revision	Version	Date
Changed copyright notice	1.1	11 June 2010
Corrected PMA contact e-mail	1.2	16 December 2011
Added DCV and reflected OV G2 validation	1.7	February 2013
Added G2 SHA-2 hierarchy	1.8	18 October 2014
Align with DigiCert CA Operator operations	2.0	February 2015

Revisions not denoted “significant” are those deemed by the CA’s Policy Management Authority to have minimal or no impact on Subscribers and Relying Parties using certificates, using the CRLs or using the OCSP responses of the issuing CAs. Insignificant revisions may be made without changing the version number of this CPS.

1.3 PKI Participants

1.3.1 Certification Authorities

3.2.3 Authentication of Individual Identity

The identity of a Applicant in a Subscriber's IdP will be validated by the Subscriber in accordance with the requirements set forth by the CA Operator for the certificate product requested.

For eScience Server certificates, the validation process shall comply with the requirements for OV SSL Server Certificates.

There are no further stipulations beyond those set forth by the CA Operator.

3.2.4 Non-Verified Subscriber Information

No further stipulations beyond those set forth by the CA Operator.

3.2.5 Validation of Authority

An Applicant is authorised to request and/or obtain a certificate with the TCS Server & CS CAs either by having enrolled as a User on behalf of the Subscriber, or by explicit invitation of the Subscriber via means provided by the CA Operator.

The Subscriber shall, on an ongoing basis, control and be responsible for the data that its Applicants supplied to TCS. The Subscriber must promptly notify TCS of any misrepresentations and omissions made by a Applicant.

Copy of TCS Generation 4 Certificate Authority Naming

File Edit View Insert Format Tools Add-ons Help Last edit was seconds ago

100% Normal text Arial 12 B I U A [tools]

RSA requirements = for 4096-bit RSA
 ECC requirements = NIST P-256

Type	Current TCS (DigiCert)	Proposed <u>Sectigo</u> Naming
GÉANT OV RSA GÉANT OV ECC	/C=NL/ST=Noord-Holland/L=Ams terdam/O=TERENA/CN=TEREN A Server CA 3	/C=NL/O=GEANT/OU=TCS/CN=G EANT OV RSA CA 4 /C=NL/O=GEANT/OU=TCS/CN=G EANT OV ECC CA 4
GÉANT eScience Server	/C=NL/ST=Noord-Holland/L=Ams terdam/O=TERENA/CN=TEREN A eScience SSL CA 3	/C=NL/O=GEANT/OU=TCS/CN=G EANT eScience SSL CA 4 which is an RSA intermediate /C=NL/O=GEANT/OU=TCS/CN=G EANT eScience SSL ECC CA 4
		/C=NL/O=GEANT/OU=TCS/CN=G EANT EV RSA CA 4 /C=NL/O=GEANT/OU=TCS/CN=G EANT EV ECC CA 4
	land, TERENA, Signing CA 3	/C=NL/O=GEANT/OU=TCS/CN=G EANT Code Signing CA 4 which is an RSA intermediate /C=NL/O=GEANT/OU=TCS/CN=G EANT Code Signing ECC CA 4

```

*****
*** GEANTeSciencePersonalCA4_test.crt
*****
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      aa:32:72:ee:da:1b:19:a6:37:f6:f2:56:2a:f4:ee:f1
    Signature Algorithm: sha384withRSAEncryption
    Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA
    Validity
      Not Before: Feb 18 00:00:00 2020 GMT
      Not After : May 1 23:59:59 2033 GMT
    Subject: C=NL, O=GEANT Vereniging, CN=GEANT eScience Personal CA 4
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-key: (4096 bit)
      Modulus:
        00:95:a2:49:3d:b9:1d:54:00:94:5c:36:0d:4d:4d:
  
```



REFEDS RAF, SFA and MFA


Peer-reviewed assessment process

AUTHENTICATION ASSURANCE PROFILES

Assurance – standard profiles and ‘untangling spaghetti’

- REFEDS RAF profiles (feasible assurance from all over R&E federations – as far as we can!)
- inter-infrastructure profiles and relying-party oriented profiles (IGTF BIRCH, DOGWOOD)
- how to express social media assurance, for citizen science and in support of account linking

AARC-G041
Expression of REFEDS RAF assurance components for identities derived from social media accounts



3. RAF component recommendations

The above-listed consideration lead to the following guidance on asserting assurance component values:

The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam DO NOT assert any REFEDS RAF component values
The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through	Assert profile AARC-Assam ALSO assert https://refeds.org/assurance/ID/unique

5. Profiles.....	5
5.1. REFEDS RAF Profiles	5
5.2. Supplementary IGTF profiles for Infrastructures.....	6
5.3. Supplementary specific profiles for Infrastructures	7
5.4. Attribute freshness assurance component	AARC-G021 8
5.5. Implementation notes.....	inter-infrastructure adoption. 8

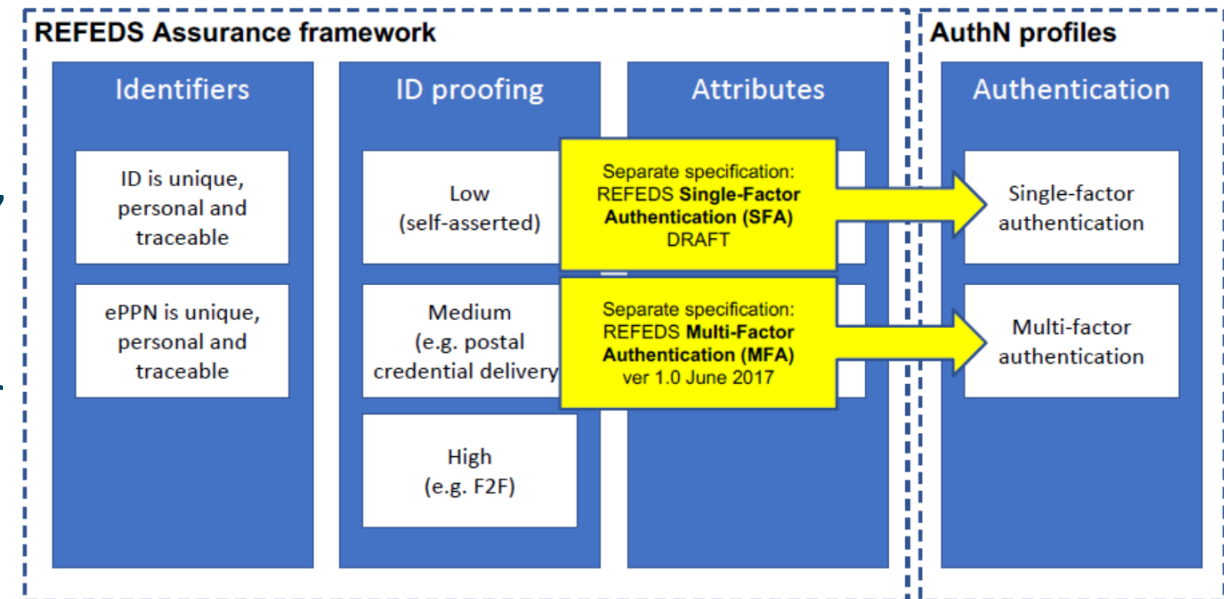
skolfederation.se/loa/2fa	skolfederation.se-2fa	[https://www.skolfederation.se/policy/assurance/al1]
sunet.se/policy/assurance/al1	SWAMID-AL1	[https://www.sunet.se/swamid/se/policy/assurance/al2]
sunet.se/policy/assurance/al2	SWAMID-AL2	[https://www.sunet.se/swamid/se/policy/assurance/al2]
refeds.org/sirtfi	Sirtfi	[https://refeds.org/sirtfi]
igtf.net/ap/authn-assurance/aspens	IGTF-ASPEN	[https://www.igtf.net/ap/authn-assurance/aspens]
igtf.net/ap/authn-assurance/birch	IGTF-BIRCH	[https://www.igtf.net/ap/authn-assurance/birch]
igtf.net/ap/authn-assurance/cedar	IGTF-CEDAR	[https://www.igtf.net/ap/authn-assurance/cedar]
igtf.net/ap/authn-assurance/dogwood	IGTF-DOGWOOD	[https://www.igtf.net/ap/authn-assurance/dogwood]

Differentiated Assurance Profile – in eduGAIN and REFEDS

Specific definitive guidance to IdPs and federations

- **Uniqueness:** at least ePUIID or NameID
- **ID proofing:** ‘low’ (good for local use), ‘medium’ (Kantara LoA2, IGTF BIRCH, eIDAS low), or ‘high’ (Kantara LoA3, eIDAS substantial)
- **Authenticator:** in REFEDS separate profiles, single (SFA) and multi-factor (MFA) authenticator
- **Freshness:** better than 1 month

Logical grouping and profiles for the Infrastructures



All assurance profiles assume organizational-level authority, also used *by the IdP* for ‘real work’, good security practices

e-Infra & Research Infra: high-assurance use cases – does it stand the test?

Two representative use cases from the AARC Pilots

Sensitive data – assurance must stand up to scrutiny, and seen in conjunction with other standards

- Retrieval of data from medical data repository
BBMRI-ERIC Colorectal Cancer Cohort study data
- Processing personal data on secure computing infrastructures
BioBankCloud, TSD Trusted Sensitive Data, MOSLER platform

COLORECTAL CANCER COHORT - ADOPT BBMRI-ERIC

The colorectal cancer cohort (CRC-Cohort) is developed within the EU-funded project ADOPT BBMRI-ERIC (H2020) as a use case for piloting access to European biobanks.

The CRC-Cohort is developed by BBMRI-ERIC, its National Nodes and BBMRI-ERIC partner biobanks, and it will become a permanent asset of the BBMRI-ERIC infrastructure after the end of the ADOPT project. The CRC-Cohort collection is a joint long-term European endeavor, which enables existing, well-established biobanks to connect with BBMRI-ERIC and obtain increased recognition and visibility along with new users and data.

The CRC-Cohort is expected to enable high-quality research and innovation to improve colorectal cancer treatment. The cohort should enable a large spectrum of different types of research and is therefore not restricted to any specific research question. The procedures and IT tools developed within the CRC-Cohort are expected to be reusable for similar future efforts on different use entities implemented using BBMRI-ERIC as an infrastructure.

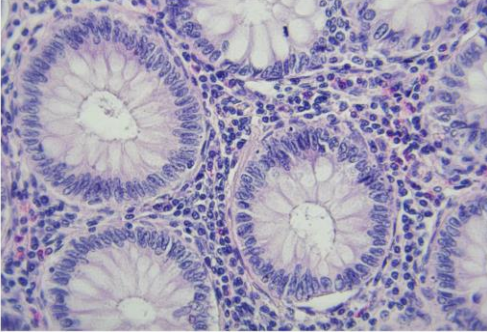


Table 8: Minimum requirements for basic data types. Non-personal data is used to denote data that does not contain any traces of privacy-sensitive data (e.g., data about operation of the biobank storage systems).

	raw (non-deidentified)	pseudonymous	practically anonymous	non-personal
<i>Authentication and authorization</i>				
Identity verification	LoA ≥ 2	LoA ≥ 2	LoA ≥ 0	op
Authentication instance	LoA ≥ 3	LoA ≥ 2	LoA ≥ 0	op
Assessing project & informed consent compliance	not available for research	MANDATORY	RECOMMENDED	
Restricted access	high security	high security	medium-low security	op
DTA/MTA	REQUIRED	REQUIRED	RECOMMENDED	op
<i>Authentication and authorization</i>				
Access log archive since last access	≥ 10 years	≥ 10 years	≥ 3 years	
<i>Data transfers and storage</i>				
Encrypted storage	REQUIRED	REQUIRED		
Encrypted transfers	REQUIRED	REQUIRED		

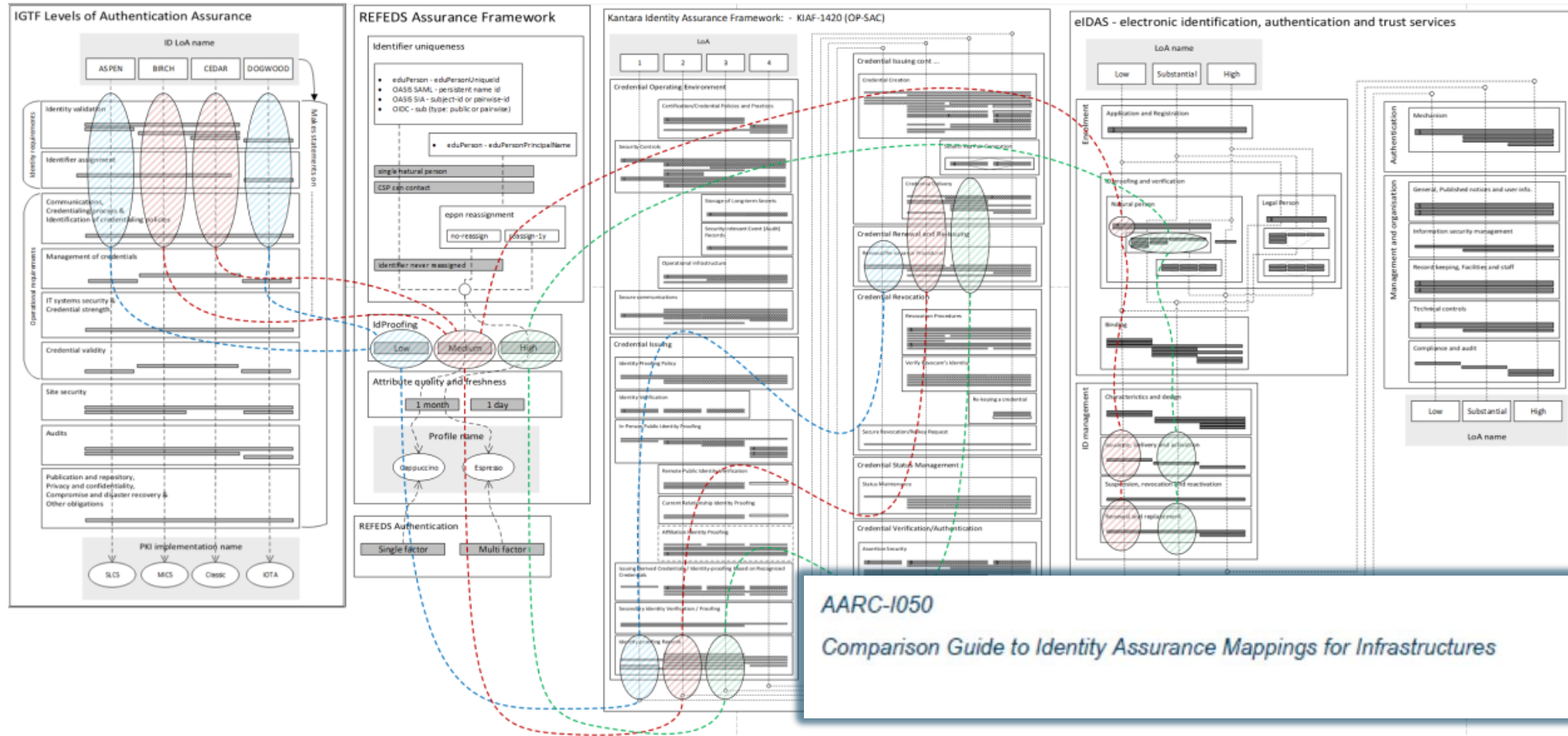
raw (non-deidentified)	pseudonymous
<i>Authentication and authorization</i>	
LoA ≥ 2	LoA ≥ 2
LoA ≥ 3	LoA ≥ 2

REFEDS RAF Assurance in relation to Kantara, eIDAS, and IGTF profiles

Value	Description
\$PREFIX\$/IAP/low	<p>Identity proofing and credential issuance, renewal, and replacement qualify to any of</p> <ul style="list-style-type: none"> • sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance level 1 [Kantara SAC] • IGTF level DOGWOOD [IGTF] • IGTF level ASPEN [IGTF] <p>Example: self-asserted identity together with verified e-mail address, following sections sections 5.1.2-5.1.2.9 and section 5.1.3 of [Kantara SAC].</p>
\$PREFIX\$/IAP/medium	<p>Identity proofing and credential issuance, renewal, and replacement qualify to any of</p> <ul style="list-style-type: none"> • sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3 of Kantara assurance level 2 [Kantara SAC] • IGTF level BIRCH [IGTF] • IGTF level CEDAR [IGTF] • section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low [eIDAS LoA] <p>Example: the person has sent a copy of their government issued photo-ID to the CSP and the CSP has had a remote live video conversation with them, as defined by [IGTF].</p>
\$PREFIX\$/IAP/high	<p>Identity proofing and credential issuance, renewal, and replacement qualifies to any of</p> <ul style="list-style-type: none"> • section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3 [Kantara SAC] • section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial [eIDAS LoA] <p>Example: the person has presented an identity document that is checked to be genuine and represent the claimed identity and steps have been taken to minimise the risk of a lost, stolen, suspended, revoked or expired document, following sections 2.1.2, 2.2.2 and 2.2.4 of eIDAS assurance level substantial [eIDAS LoA].</p>

raw (non-deidentified)	pseudonymous
<i>Authentication and authorization</i>	
LoA \geq 2	LoA \geq 2
LoA \geq 3	LoA \geq 2

Untangling Assurance Spaghetti: Comparison Guide to Identity Assurance Mappings for Infrastructures



Interpreting the graphs

- on context and missing 'breadcrumbs'
- components vs. profiles
- implicit trust vs. completeness

IGTF Levels of Authentication Assurance

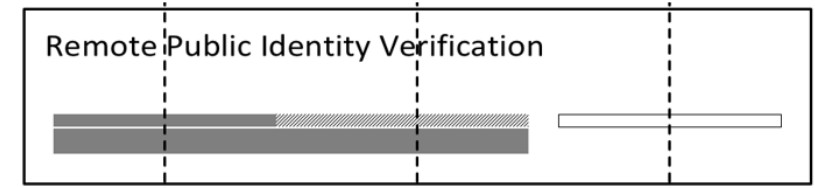
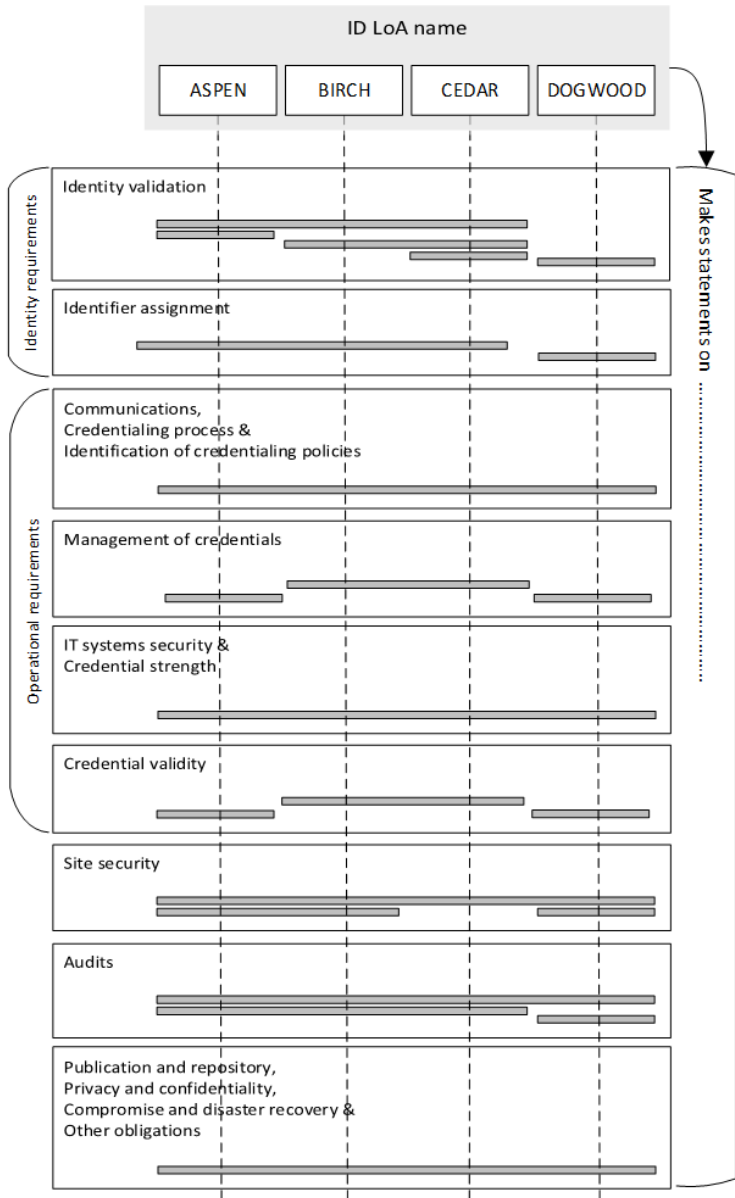


Figure 4.3: Variations of requirement representation

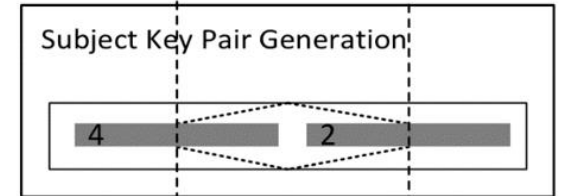
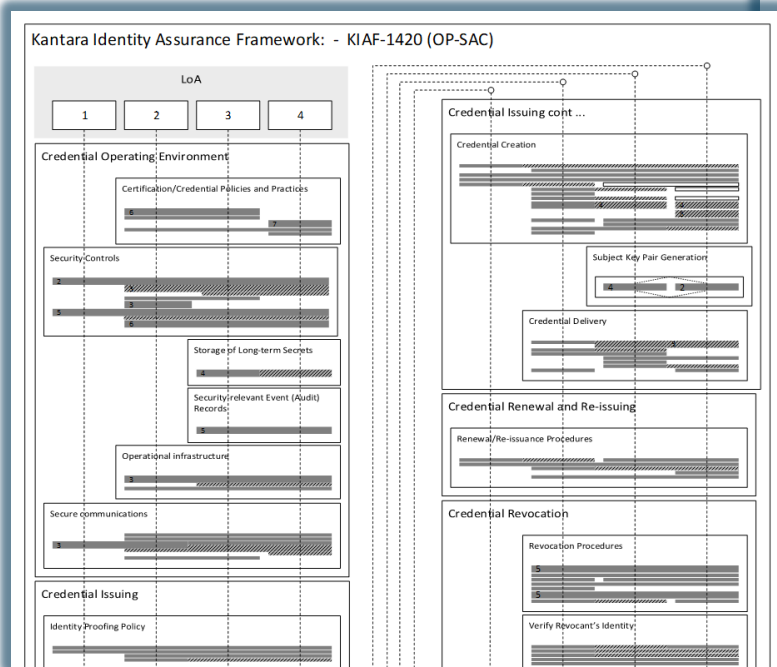


Figure 4.4: Alternate requirement choices



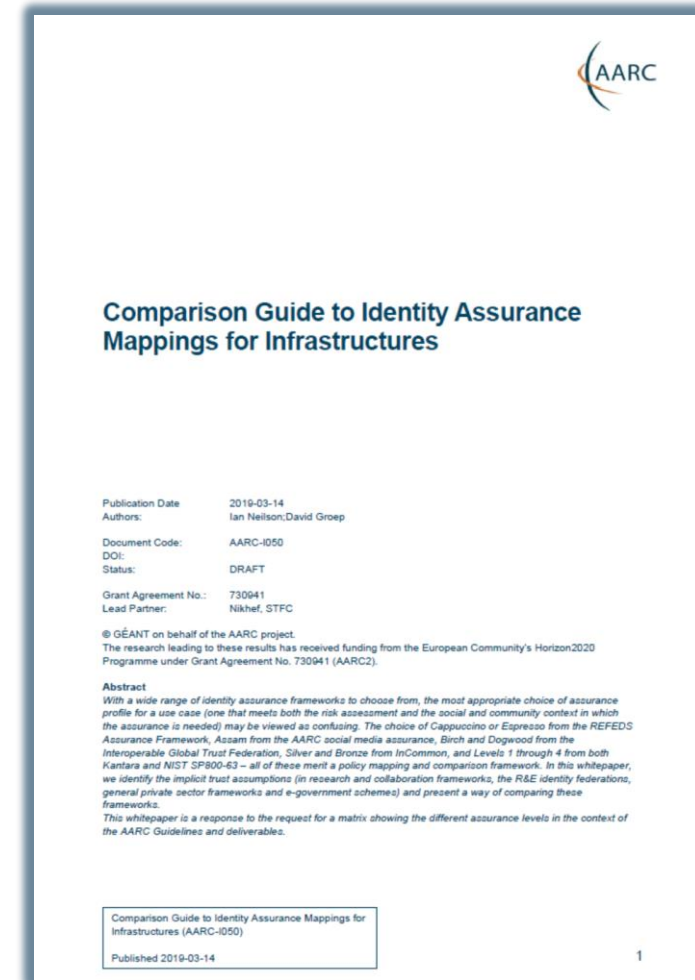
About the mapping exercise – the AARC-I050 white paper

Answering the questions

- why are there so many Assurance Frameworks
- why are the academic and research ones different
- why is there more than one for each
- how do they compare? what are the unique features

We attempted to answer your request ... at TIIME and in **AARC-I050!**

- addressing different audiences:
IdP feasibility vs SP minimal requirements
- orthogonality vs component-suite approach (profiles)
- completeness vs community-focused:
leveraging common understanding,
... and forgetting the grains of rice on how we got there



Conveying Assurance and Profiles in practice – at the IGTF: XSEDE & FNAL

Questions to ask yourself when defining this policy:

- Which identity providers are acceptable for your infrastructure? SAML Identity Federation IdPs? Social providers such as Google, Facebook etc?
- How much certainty does your community require of the identity? Review each of the elements (personal accounts, uniqueness, freshness, vetting quality, and authentication strength). How will you validate this for each source of (federated) identity?
- How can you ensure that each user is covered by a security incident response capability at their home organisation?
- Do your services, or a subset, require step-up (multi-factor) authentication?

The following chart can be used to help determine an appropriate assurance profile for you. Refer also to [AARC Guideline 21](#):

Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	

AARC Assam
 IGTF Dogwood
 RAF Cappuccino
 IGTF Birch
 RAF Espresso

REFEDS Assurance Framework Checklist: XSEDE

REFEDS Assurance Framework Checklist
 REFEDS Assurance Framework ver 1.0
 Checklist ver 1.0 (Nov 26 2019)
<https://refeds.org/assurance>

Identity Provider Name: Extreme Science and Engineering Discovery Environment (XSEDE)
 entityID: https://idp.xsede.org/idp/shibboleth
 Contact: XSEDE Help Desk <help@xsede.org>
 Date(s): Drafted by Jim Basney on Nov 26 2019, Reviewed by TAGPMA on Dec 13 2019

Assertion	Description	Required for Cappuccino	Required for Espresso	Meets Requirement?	Comments by Jim Basney on Nov 26 2019
https://refeds.org/assurance	1. The Identity Provider is operated with organizational-level authority.	Yes	Yes	<input checked="" type="checkbox"/>	Accepted by XSEDE Operations on May 1 2017. See: https://software.xsede.org/display/xs30 XSEDE's IdP is trusted for issuance of X.509 certificates for access to XSEDE systems. XSEDE conducted a security review of the IdP before beginning operations. XSEDE's metadata includes all 4 contacts plus logo, error URL, and privacy statement.
	2. The Identity Provider is trusted enough that it is (or it could be) used to access the organization's own systems.				
	3. Generally-accepted security practices are applied to the Identity Provider.				
	4. Federation metadata is accurate, complete, and includes at least one of the following: support, technical, admin, or security contacts.				
https://refeds.org/assurance/D/unique	(Unique-1) The user identifier represents a single natural person.	Yes	Yes	<input type="checkbox"/>	CURRENT: The XSEDE IdP asserts this for every account, but that fails to meet the requirement. TODO: The XSEDE IdP only asserts this for individual users who are associated with an active XSEDE allocation and thus have been "vetted" by the XSEDE allocations process (peer review or delegated review) to represent a single natural person. XSEDE enforces a policy against account sharing (https://www.xsede.org/us-age-policies). The XSEDE IdP explicitly does not assert this for so-called "Community User" accounts used by Science Gateways (https://ind.handle.net/2142/48925).
	(Unique-2) The CSP can contact the person to whom the identifier is issued.				
	(Unique-3) The user identifier is never re-assigned.				

REFEDS MFA Checklist

REFEDS MFA Profile v1.0
 Checklist ver 1.0 (Nov 26 2019)
<https://refeds.org/profile/mfa>

Identity Provider Name: Extreme Science and Engineering Discovery Environment (XSEDE)
 entityID: https://idp.xsede.org/idp/shibboleth
 Contact: XSEDE Help Desk <help@xsede.org>
 Date(s): Drafted by Jim Basney on Nov 26 2019, Reviewed by TAGPMA on Dec 13 2019

Description	Meets Requirement?	Comments by Jim Basney on Nov 26 2019
The authentication of the user's current session used a combination of at least two of the four distinct types of factors defined in ITU-T X.1254: Entity authentication assurance framework, section 3.1.3, authentication factor (something you know, something you have, something you are, something you do) The factors used are independent, in that access to one factor does not by itself grant access to other factors.	<input checked="" type="checkbox"/>	The XSEDE IdP uses Kerberos passwords (something you know) and Duo MFA (something you have) for authentication.
The combination of the factors mitigates single-factor only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor.	<input checked="" type="checkbox"/>	XSEDE Kerberos passwords are independent from Duo MFA. XSEDE Kerberos KDCs are operated by XSEDE. Duo is a cloud service operated by Cisco. Users establish their Kerberos passwords and Duo credentials separately at account sign-up time.
	<input checked="" type="checkbox"/>	Duo credentials (push, OTP, SMS) are one-time use and time-limited to mitigate non-real-time attacks.





Guidelines for running a secure membership and group management service

ATTRIBUTE AUTHORITY OPERATIONS

Operational guideline landscape for - proxy or source - AAI components

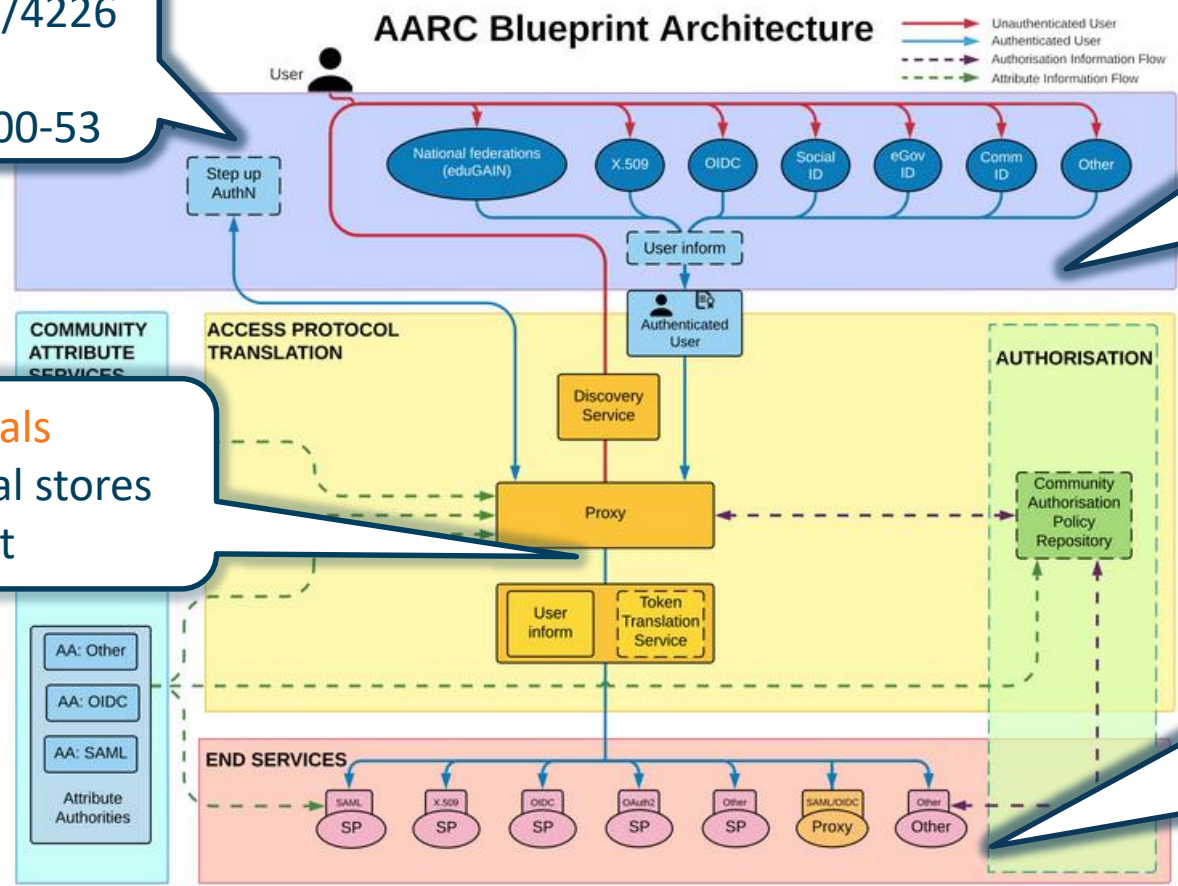
MFA
 RFC6238/4226
 FIPS140
 NISTSP800-53

Authentication/identity sources
 Sirtfi
 (eduGAIN) baselining
 IGTF AP Profiles
 NIST SP800-63
 eduGAIN sec. team workflow

Ephemeral credentials

- trusted credential stores
- protection at rest

Service provider operations
 ISO27k
 Sirtfi
 Infrastructure response plans



COMMUNITY ATTRIBUTE SERVICES

ACCESS PROTOCOL TRANSLATION

AUTHORISATION

END SERVICES

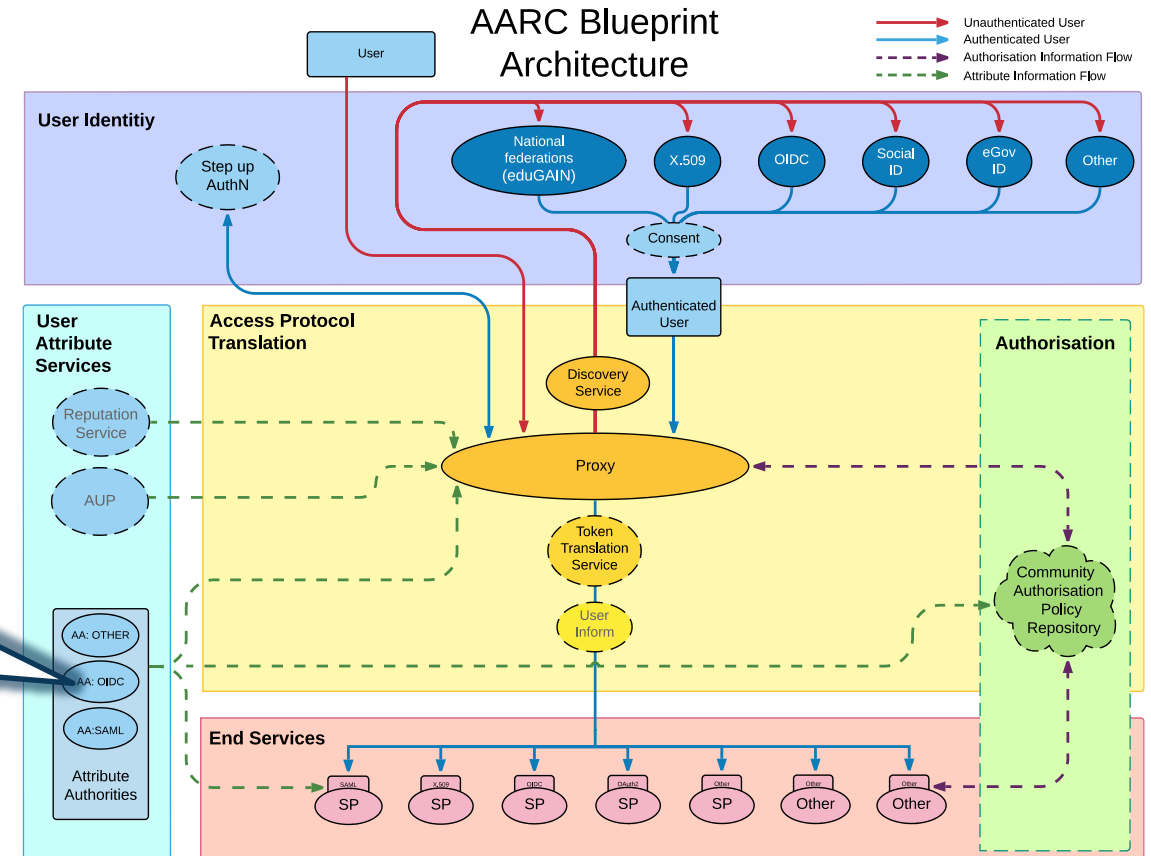
- AA: Other
- AA: OIDC
- AA: SAML
- Attribute Authorities



Operational security in the BPA: beyond just IdPs

Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity



Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements (AARC-I048, in collaboration with IGTF AAOPS)



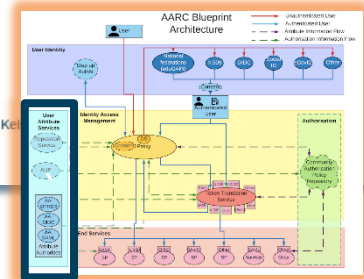
AARC-G048: keeping users & communities protected, moving across models

trusted delegation of response from communities to operators, and from services to communities in recognizing their assertions

Structured around concept of “**AA Operators**”, operating “**Attribute Authorities**” (technological entities), on behalf of, one or more, **Communities**

Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements

Publication Date: 2018-11-22
Authors: David Groep, David Ke Paetow, Maarten Kremers
Document Code: AARC-G048



3.3. Attribute Assertions

1. Assertions provided by an AA must be integrity-protected. They must be signed by the identified AA, or be transmitted over an integrity-protected channel where the server has been authenticated, and preferably both.

Push model

Where the protocol supports it, enable protection also of the messages conveyed over the established channel.

Good examples: SAML Attribute Query should enable message signing and use TLS.

Pull model

As a good example: LDAP should enable TLS protection of the channel

3.4.1. Key Management

1. A key used to protect assertions should be dedicated to assertion protection functions.

Push model

If the AA both signs assertions and provides functionality over protected channels, the keys used to sign assertions shall be different from those protecting those channels.

Pull model

The key of the AA must be used solely for protecting connections to its protocol endpoint and ensure an integrity protected and mutually authenticated channel.



09 March 2020

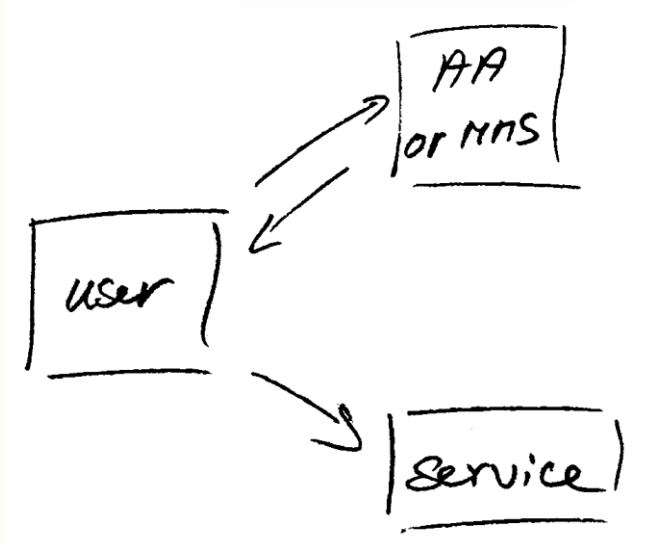
<https://www.igtf.net/guidelines/aaops/>

IGTF and EUGridPMA development - APGridPMA March 2020 Taipei meeting

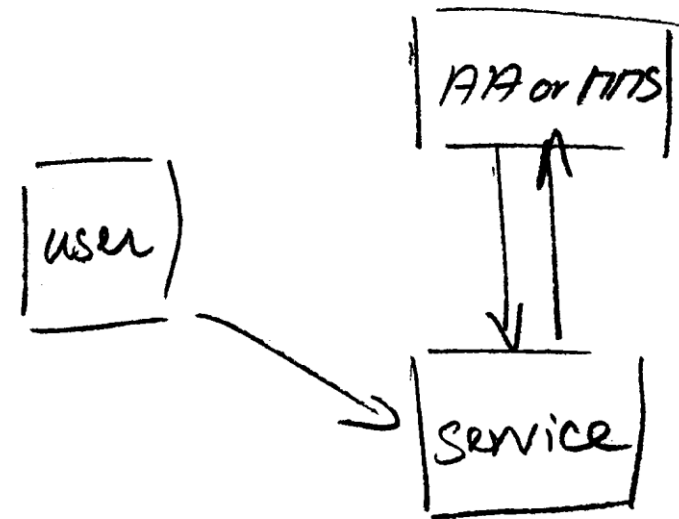
<https://aarc-community.org/guidelines/aarc-g048/>

Protecting the community membership data and its proxy

- Intentionally targeted broader than just BPA-style communities, since operational security spans data centres and infrastructures using other forms of AA membership management
- PRACE: 'pull model' directory-based communities
- BPA: encourages 'push model' attribute-carrying service requests



*push model – the common BPA method
(e.g. SAML AttributeStatement, VOMS AC)*



*pull model – common when using directories
(e.g. LDAP in PRACE, GUMS in OSG)*

When the AA is managed (and in a data centre) ...

- Many of the recommendations are already implemented ‘implicitly’
- because common software implements it: e.g. signing SAML assertions and JWTs
- because a good data centre already has network monitoring and central logging in place
- because you signed up to Sirtfi (didn't you?) – so you collaborate in incident response
- because you have trained IT operations personnel looking after the service

- And some are intuitive best practice
- like assigning a unique and lasting name to a group
- because implemented controls follow ought to be those that have been documented

Forward looking and specific requirements

Some controls are specific to AA operations and protect against current and future threats:

- minimum signing key length so that the community is not broken in the next few years (at least 112-bit symmetric, i.e. ≥ 2048 bit RSA keys)
- protect the key from data breaches, compromise, ransomware, and exfiltration by using HSM Hardware Security Modules or equivalent controls (and the HSMs you need are not that expensive, or you can even rent them in AWS...)

Or deal with commensurate incident response (you don't want just a big red button):

- re-issuance of attribute statement must be based on fresh data
- release them only in accordance with the community's policy and maximum life time
- require appropriate client authentication before releasing attributes to prevent data breaches
- for non-revocable tokens (like OAuth Access Tokens or PKIX 3820 proxies), limit life time < 24 hrs (for OIDC, these are anyway typically 15 minutes)



G048 AA Ops guidelines and AA hosting

Guideline was written with both physical and virtual deployment in mind

“An AA may be run in a virtual environment that has security requirements the same or better than required for the AA, and for all services running in this environment, and it must not leave this security context. **Any virtualization techniques employed** (including the hosting environment) **must not degrade the context** as compared to any secured physical setup. Only AA Operator designated personnel should have control over the virtualisation and security context of the AA.”

- if you can host it on-prem, the easiest solution is to host it on your security-service VM infrastructure (e.g. alongside your IdP, your AD, or your master LDAP servers) to limit guest compromise)
- If you run it in a cloud provider, select a provider that offers proper security and network controls, implement account role separation, and deploy the offered protections. E.g. in AWS you have *a lot* of controls available to do so. But Azure & co hve the same. – and rent a netHSM



Deployment guidance included ...

1. Assertions provided by an AA must be integrity-protected. They must be signed by the identified AA, or be transmitted over an integrity-protected channel where the server has been authenticated, and preferably both.

Push model

Where the protocol supports it, enable protection also of the messages conveyed over the established channel.

Good examples: SAML Attribute Query should enable message signing and use TLS.

Pull model

As a good example: LDAP should enable TLS protection of the channel

6. The network to which the AA system is connected must be highly protected and suitably monitored.

Service access should be protected by at least two distinct control layers not running the same software or operating system, and the AA system must not run any unnecessary services. The network should be monitored for anomalous events, such as detection of data exfiltration, credential probing, and brute-force attacks. It should preferably also be protected



Security Communications Challenge Coordination Joint Working Group –
IGTF, WISE-Community, GEANT SIG-ISM, Trusted Introducer / TF-CSIRT, REFEDS

SCCC JWG

Communications Challenges

Based on *Sirtfi* incident role play of AARC in eduGAIN:
testing communications channels identified as high-prio target
Initial model might be along the IGTF RAT CC challenges – can be extended later

Question	Response summary (9 responses received)
What went well?	The initial investigation was quick and responsive and Sirtfi contacts largely worked. eduGAIN support was helpful and included federation operators.
What didn't go well?	Lack of coordination. Delay in official alert. It was unclear who should be contacted. eduGAIN was brought in too late. The incident trigger was too vague. Investigation incomplete.



Planned progress

- More exercises, coordinated via WISE
- Improve available tooling
- Set defined roles, including a *coordinator*, and promote eduGAIN security capability GN4-*



Proper OpSec needs to be exercised!

Like the IGTF RAT Communications Challenges, and TF-CSIRT processes, opsec really needs to be exercised often and in-depth to ensure readiness

**Logical candidates that could all run the test against IdPs, CAs, SPs, RPs ...
... and 'legitimately' claim an interest in their results**

- eduGAIN
 - IGTF
 - GEANT.org
 - EOSC-HUB ops, or EGI CSIRT
 - each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, HPCI, ...
 - every research infra with an interest: WLCG, LSAAI, BBMRI, ELIXIR, ...
 - any institution (or person) with access to <https://mds.edugain.org/>
- so soon: all the email in the world will be about Sirtfi Incident Response tests??*



WISE SCCC-WG – participate!

WISE Community:

Security Com
Coordination

Introduction and bac

Maintaining trust between dif
responses by all parties involv
coordinated e-Infrastructures,
contact information, and have
and level of confidentiality ma
verified becomes stale: securi
infrastructure may later bound

One of the ways to ensure cor
compare their performance ag

[Dashboard](#) / ... / [SCCC-JWG](#)

Communications Challenge planning

Created by David Groep, last modified on Oct 12, 2019

Body	Last challenge	Campaign name	Next challenge	Campaign
IGTF	November 2015		October 2019	IGTF-RATCC
EGI	March 2019	SSC 19.03 (8)		
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a h
detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to differe
sources to testing if the communication contacted could custom message for analysis and response effectiveness with I.E. The success level

IGTF-RATCC4-2019

Campaign	IGTF-RATCC4-2019
Period	October 2019
Initiator contact	Interoperable Global Trust Federation IGTF (rat@igtf.net)
Target community	IGTF Accredited Identity Providers
Target type	own constituency of accredited authorities
Target community size	~90 entities, ~60 organisations, ~50 countries/economic areas
Challenge format and depth	email to registered public contacts expecting human response (by email reply) within policy timeframe
Current phase	Completed, summary available
Summary or report	<i>Preliminary result: 82% prompt (1 working day) response, follow-up ongoing</i>

WISE, SIGISM, REFEDS, TI joint working group
see wise-community.org and join!

<https://wiki.geant.org/display/WISE/SCCC-JWG>



IGTF RATCC4 Results

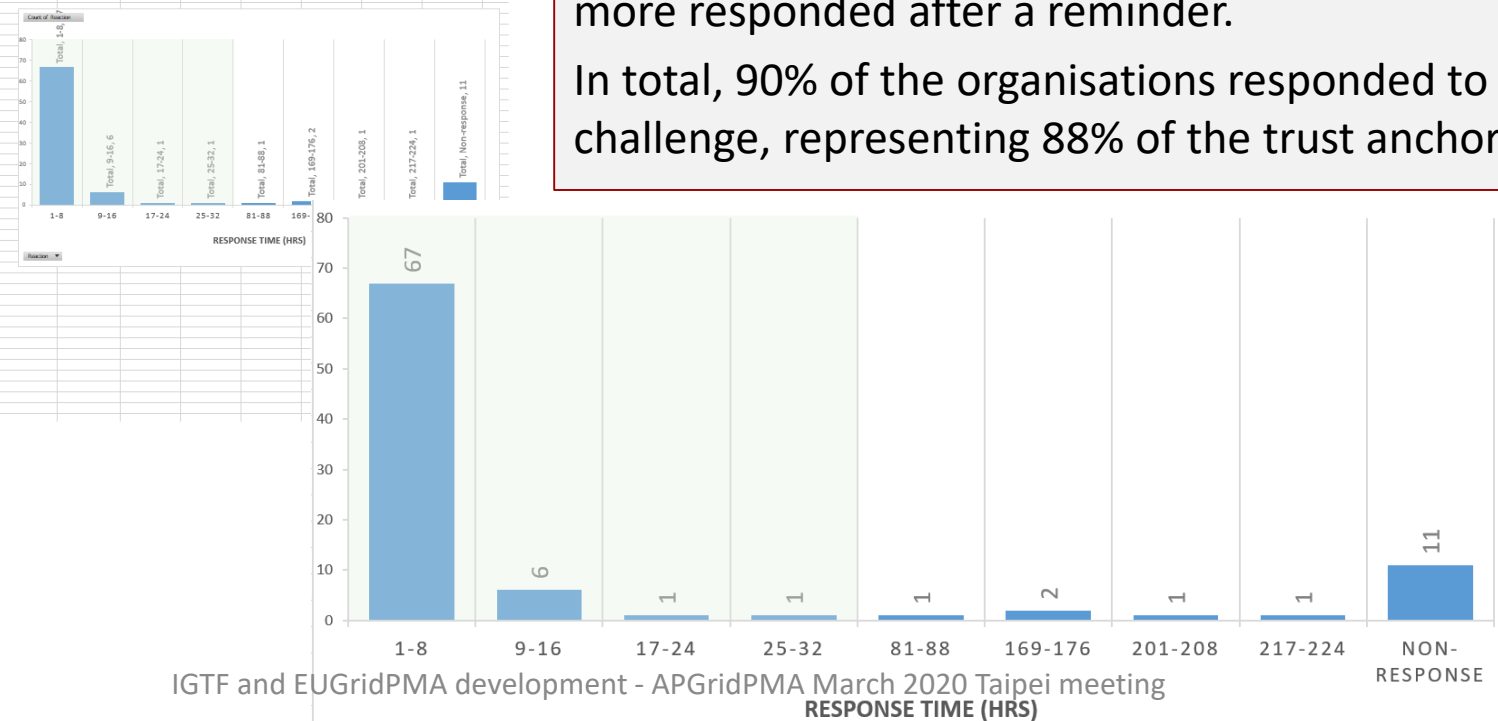
Sent	Prompt	Reminder	Earliest	Reaction	Campaign/Duration
2019-10-07 06:31	2019-10-07 07:48		2019-10-07 07:46	2.00	
2019-10-07 06:31	2019-10-07 07:46		2019-10-07 07:46	2.00	Response - Count of Reaction
2019-10-07 06:31	2019-10-07 07:46		2019-10-07 07:46	2.00	1-3
2019-10-07 06:31	2019-10-07 07:46		2019-10-07 07:46	2.00	9-16
2019-10-07 06:31	2019-10-07 06:34		2019-10-07 06:34	1.00	17-24
2019-10-07 06:31	2019-10-07 07:30		2019-10-07 07:30	1.00	25-32
2019-10-07 06:31	2019-10-07 06:17		2019-10-07 06:17	81.88	81-88
2019-10-07 06:31	2019-10-07 08:22		2019-10-07 08:22	2.00	169-176
2019-10-07 06:31	2019-10-07 08:13		2019-10-07 08:13	4.00	201-208
2019-10-07 06:31	2019-10-07 08:41		2019-10-07 08:41	3.00	217-224
2019-10-07 06:31	2019-10-07 07:02		2019-10-07 07:02	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:50		2019-10-07 06:50	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:50		2019-10-07 06:50	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:50		2019-10-07 06:50	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:51		2019-10-07 06:51	3.00	Non-response
2019-10-07 06:31	2019-10-07 08:51		2019-10-07 08:51	3.00	Non-response
2019-10-07 06:31	2019-10-07 13:08		2019-10-07 13:08	7.00	Non-response
2019-10-07 06:31	2019-10-07 13:08		2019-10-07 13:08	7.00	Non-response
2019-10-07 06:31	2019-10-07 07:46		2019-10-07 07:46	2.00	Non-response
2019-10-07 06:31	2019-10-07 07:46		2019-10-07 07:46	2.00	Non-response
2019-10-07 06:31	2019-10-07 07:46		2019-10-07 07:46	2.00	Non-response
2019-10-07 06:31	2019-10-07 07:46		2019-10-07 07:46	2.00	Non-response
2019-10-07 06:31	2019-10-07 07:02		2019-10-07 07:02	1.00	Non-response
2019-10-07 06:31	2019-10-07 07:02		2019-10-07 07:02	1.00	Non-response
2019-10-07 06:31	2019-10-07 07:02		2019-10-07 07:02	1.00	Non-response
2019-10-07 06:31	2019-10-07 07:02		2019-10-07 07:02	1.00	Non-response
2019-10-07 06:31	2019-10-07 07:02		2019-10-07 07:02	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:36		2019-10-07 06:36	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:43		2019-10-07 06:43	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:43		2019-10-07 06:43	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:43		2019-10-07 06:43	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:43		2019-10-07 06:43	1.00	Non-response
2019-10-07 06:31	2019-10-14 12:48		2019-10-14 12:48	176.00	Non-response
2019-10-07 06:31	2019-10-07 14:08		2019-10-07 14:08	0.00	Non-response
2019-10-07 06:31	2019-10-07 09:04		2019-10-07 09:04	3.00	Non-response
2019-10-07 06:31	2019-10-07 07:49		2019-10-07 07:49	2.00	Non-response
2019-10-07 06:31	2019-10-07 07:07		2019-10-07 07:07	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:36		2019-10-07 06:36	4.00	Non-response
2019-10-07 06:31	2019-10-08 07:39		2019-10-08 07:39	26.00	Non-response
2019-10-07 06:31	2019-10-07 14:36		2019-10-07 14:36	8.00	Non-response
2019-10-07 06:31	2019-10-07 13:53		2019-10-07 13:53	0.00	Non-response
2019-10-07 06:31	2019-10-07 06:59		2019-10-07 06:59	1.00	Non-response
2019-10-07 06:31	2019-10-07 07:14		2019-10-07 07:14	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:54		2019-10-07 06:54	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:54		2019-10-07 06:54	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:54		2019-10-07 06:54	1.00	Non-response
2019-10-07 06:31	2019-10-07 06:43		2019-10-07 06:43	10.00	Non-response
2019-10-07 06:31	2019-10-07 08:48		2019-10-07 08:48	3.00	Non-response
2019-10-07 06:31	2019-10-07 06:32		2019-10-07 06:32	11.00	Non-response
2019-10-07 06:31	2019-10-14 08:24		2019-10-14 08:24	171.00	Non-response
2019-10-07 06:31	2019-10-08 04:38		2019-10-08 04:38	23.00	Non-response
2019-10-07 06:31	2019-10-07 12:32		2019-10-07 12:32	7.00	Non-response

In total there are 91 trust anchors (root, intermediate, and issuing authorities) currently in the accredited bundle, managed by 60 organisations.

Of the 60 organisations, 49 responded within one working day (82%), representing (incidentally) also 82% of the trust anchors.

Within a few days more, 3 additional ones came in, and 4 more responded after a reminder.

In total, 90% of the organisations responded to the challenge, representing 88% of the trust anchors.



Specific IGTf actions following RATCC4

- DigiCert contact was updated and verified
- BYGCA (.by) is migrating operations to new entity
- INFN will discontinue its CA by January 2021 (and move to TCS)
- TSU GRENA communications ongoing
- SDG, CNIC information updated





Questions?

BUILDING A GLOBAL TRUST FABRIC