IGTF

Interoperable Global Trust Federation

AP | EU | TAG

European IGTF update

David Groep

davidg@nikhef.nl

Nik|hef

Maastricht University

eu gridpma

Enabling Communities through Trust, Identity, and Security in our Open Science era

TCS Update

Meanwhile in the EUGridPMA+ …
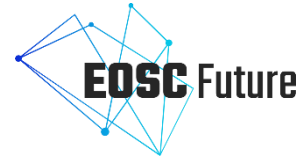
- EUGridPMA - constituency and developments
- GPG Package Signing Key updates
- S/MIME BR – separating authentication and email signing
- Attribute Authority Operations guideline
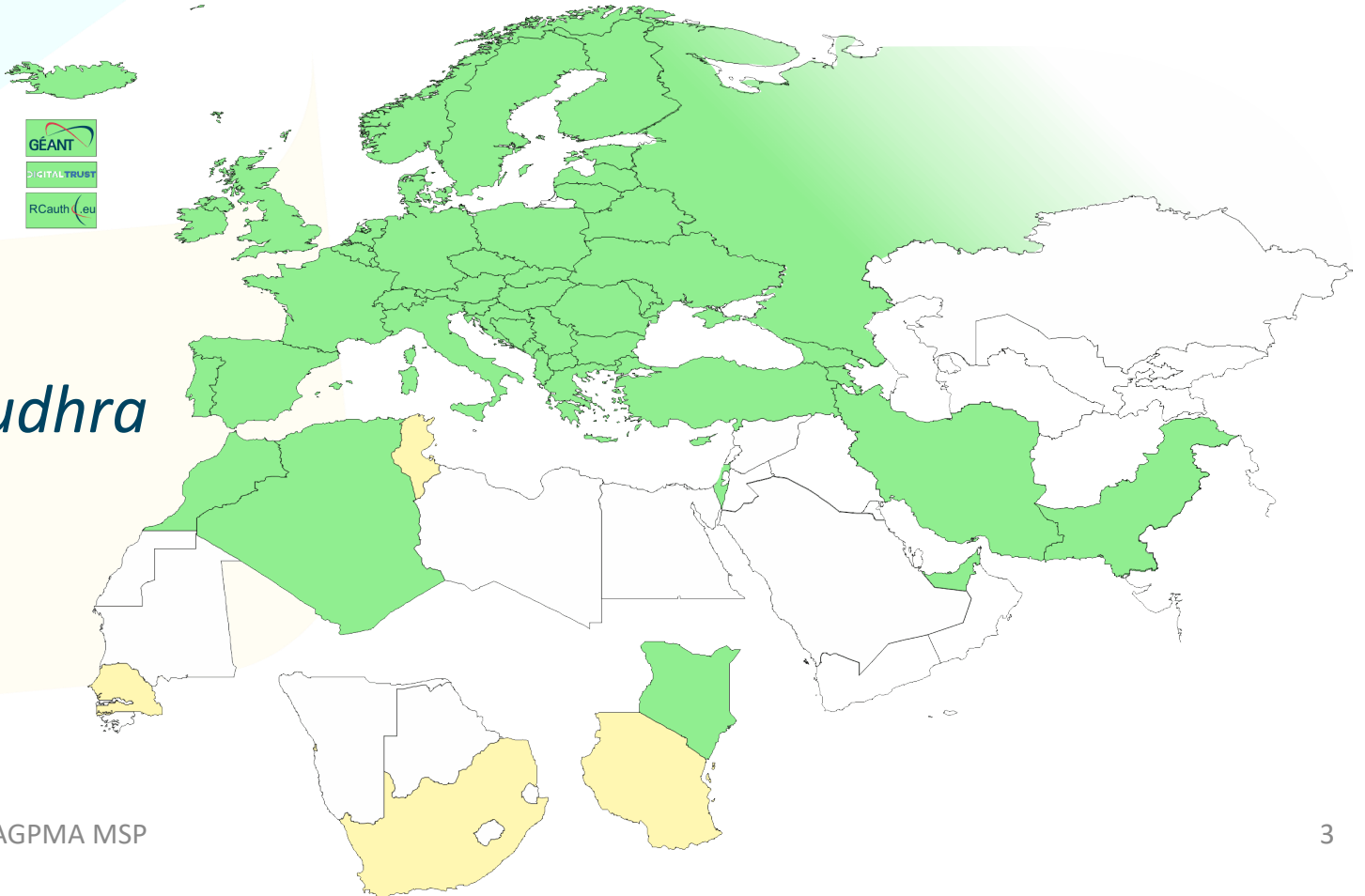- SHA-1 roots update for RHEL9+

EMEA area membership evolution

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

the Swiss moved from the imploded DigitalTrust to eMudhra
(via a legacy DutchGrid transition)

Emphasis on collaboration across the whole T&I space

Membership and other changes

- Identity providers: both reduction and growth
  - migration to GEANT TCS continues: +DE
    https://wiki.geant.org/display/TCSNT/TCS+Participants+Sectigo
  - CERN joining TCS via Renater (FR)
- Self-audit review
  - Cosmin Nistor as review coordinator
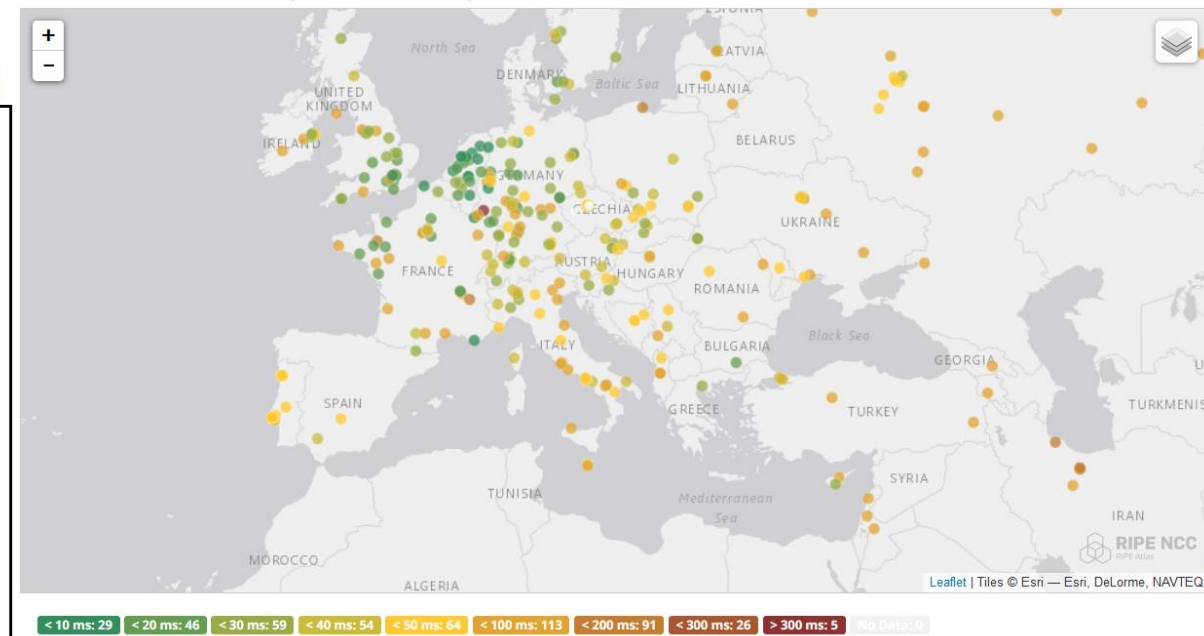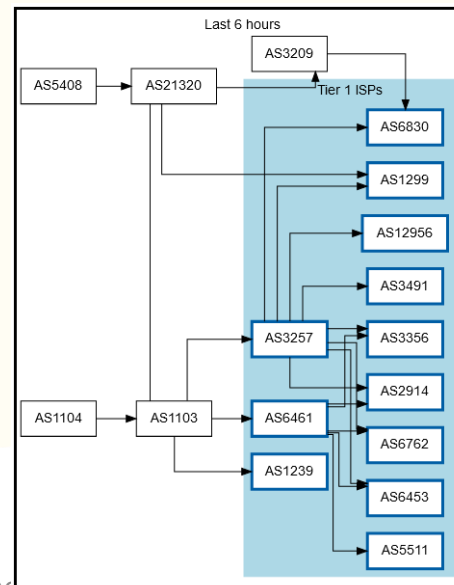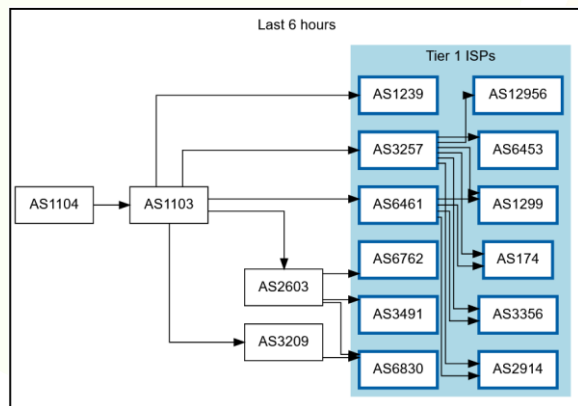 - new self-audit model: real-time interaction between authority and reviewers helps!

- **Next meeting in Abingdon, UK (Coseners) October 4-5, 2023! Joint GN5-1, AARC Community, EOSC ISM**

RCauth.eu – the ubiquitous federated IOTA

- IGTF accredited IOTA (DOGWOOD) CA
  - Online credential translation, connected to eduGAIN for all R&S+Sirtfi IdP
  - Inspired by & leveraging CILogon delegation service

- Now EOSC Future implemented High Availability setup across 3 sites: GRNET, Nikhef/SURF, STFC/RAL

map: RIPE NCC RIPE Atlas - 500 probes, distributed across Europe
(https://atlas.ripe.net/measurements/50949024/)

Distribution signing key update

```
error: Verifying a signature using certificate
D12E922822BE64D50146188BC32D99C83CDBBC71
(EUGridPMA Distribution Signing Key 3 <info@eugridpma.org>):
Key C32D99C83CDBBC71 invalid: not signing capable
```

In Fedora Core 38+ (and thus later in its derivatives, and maybe soon in Debian), RSA 1024 package signing no longer supported

Distribution signing key update

In future releases we move
to a **new GPG package key**

- RSA-2048

- called GPG-KEY-EUGridPMA-RPM-4

- distributed with 1.122+ releases

- Retrieve new public key file from
  https://dl.igtf.net/distribution/GPG-KEY-EUGridPMA-RPM-4

- or from the public key servers: rsa/2048 dated 2023-07-29T12:06:23Z

- fingerprint: 565f 4528 ead3 f537 27b5 a2e9 b055 0056 **7634 1f1a**

1.122/	2023-08-07 09:38	-
1.123-GPSK3/	2023-09-01 14:22	-
1.123-GPSK4/	2023-09-01 14:22	-
1.123-is-current	2023-09-04 12:46	0
1.123/	2023-09-01 14:22	-
LICENSE	2010-10-12 09:48	2.0K

Specific downstream distribution (like EGI) follow

- EGI uses the same signing key, since – for now – the packaging is integrated and co-supported by EGI

- Plan is to move on the next major change, but not before Q1 2024

- RHEL SHA-1 Root issue may be a good time to also make this change the default?

Index of /distribution/egi

Name	Last modified	Size
Parent Directory		-
ca-policy-egi-cam-1.123-1-GPSK3/	2023-08-31 13:43	-
ca-policy-egi-cam-1.123-1-GPSK4/	2023-08-31 13:42	-
ca-policy-egi-cam-1.123-1/	2023-08-31 13:43	-
current/	2023-08-31 13:43	-
1.123-is-current	2023-08-08 15:16	0
GPG-KEY-EUGridPMA-RPM-3	2023-08-31 13:42	889
GPG-KEY-EUGridPMA-RPM-4	2023-08-31 13:42	1.8K
ls-IR	2023-08-31 13:43	76K

CA/B Forum developments

S/MIME BASELINE REQUIREMENTS

CA/BROWSER Forum

S/MIME BASELINE REQUIREMENTS

Table of Contents

Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- Current Version
- Previous Versions

BASELINE REQUIREMENTS FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED S/MIME CERTIFICATES

CURRENT VERSION

S/MIME Baseline Requirements v1.0.0 – adopted by Ballot SMC01

PREVIOUS VERSIONS

NA

Public Trust S/MIME (personal) is getting regulated

- It was basically a 'free-for-all', as long as the email address worked

- most 'useful use' for the general public signing was in bespoke certificates types (Adobe) or in Qualified Certificates (EC regulated)

- until now, the IGTF personal requirements were much stricter than 'public' email signing, in that we did insist on a reasonable name and a 'sponsor' (organization) that was validated

- Now CA/BF is putting requirements on S/MIME for the first time

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-SMIMEBR-1.0.0.pdf

Different 'profiles' and validations

- **Strict**
  - 825-days (2yr), limited RDN attributes allowed
  - intended only for S/MIME

- **Multi-purpose**
  - 825 days (2yr), slightly more eKUs allowed
  - crossover use cases between document signing and secure erossover use cases between document signing and secure emailmail

- **Legacy**
  - 1185 days (3yr)
  - transitional profile (likely to be phased out in the end)
  - bit more freedom in subject, still allows DC naming, but otherwise not much more than MP

- **mailbox-validated**
  - just the rfc822name (only!)

- **organization-validated**
  - includes only Organizational (Legal Entity) attributes in the Subject

- **sponsor-validated**
  - Combines Individual (Natural Person) attributes and organizationName (associated Legal Entity) attribute

- **individual-validated**
  - Includes only Individual (Natural Person) attributes in the Subject

Sponsor validated

Sponsor-validated:

'Refers to a Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA where the subject:organizationName is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject Organization.'

Certificate Type	Description
Mailbox-validated	Subject is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes.
Organization-validated	Includes only Organizational (Legal Entity) attributes in the Subject.
Sponsor-validated	Combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA.

Validation requirements

1. If the Certificate Request is for an `Organization-validated` or `Sponsor-validated` profile, the CA SHALL confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.2.1 or Section 3.2.2.3. The CA SHALL confirm that the `subject:organizationName` name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are Affiliated as defined in Section 3.2 or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested email domain falls within the subdomains of ABC Co.'s Registered Domain Name.

commonName

7.1.4.2.2 Subject distinguished name fields

a. **Certificate Field:** `subject:commonName` (OID 2.5.4.3)
   Contents: If present, this attribute SHALL contain one of the following values verified in accordance with Section 3.2.

Certificate Type	Contents
Mailbox-validated	Mailbox Address
Organization-validated	`subject:organizationName` or Mailbox Address
Sponsor-validated	Personal Name, `subject:pseudonym`, or Mailbox Address
Individual-validated	Personal Name, `subject:pseudonym`, or Mailbox Address

If present, the Personal Name SHALL contain a name of the Subject. The Personal Name SHOULD be presented as `subject:givenName` and/or `subject:surname`. The Personal Name MAY be in the Subject's preferred presentation format or a format preferred by the CA or Enterprise RA, but SHALL be a meaningful representation of the Subject's name as verified under Section 3.2.4.

Where does that leave us?

- The 'Legacy' profile (still) allowed 'other' attributes, so *for the moment* e.g. DC prefixing would have been OK-ish

- However the commonName is regulated, and:
  - must be derived from (and include!) givenName and surname
  - **must not** contain any other elements (like ePPN), impacting uniqueness (as used in TCS)
  - does *not* allow for 'Robot's in the commonName
    these would go to Pseudonym, which is an ill-supported attribute
  - this anyway inflicts a subjectDN change

- who knows when the legacy profile will be deprecated! Will not be long ☹

However …

… contrary to the host-cert issue, there is no joint-trust needed for email signing and client authentication!

- separating these should always have been done:
    - using TCS Personal certs for authentication is bad (since they are not unique), and
    - using TCS IGTF MICS client certs for S/MIME email is bad (since it's 7-bit ASCII only)

- this just formalizes that move beyond restricting keyUsage & eKU

What TCS did

- Have S/MIME personal certs, organization-verified, continue to be publicly trusted
    - sponsor-validated (multi-purpose) BR-compliant (for 'humans') or org-validated ('robot email')
    - we define all TCS members as Enterprise RAs (clarified in Ballot SMC-03
    - does require all orgs to be revalidated using a Government Information Source or LEI (3.2.3.2.1)
    - their subject name will be filled with the required fields (such as LEI, jurisdiction, address)
    - the /clientgeant SAML endpoint (the only way for personal certs!) auo-upgrades Validation to "High"

- Move the *client authentication* trust to a 'private CA' (non-public trust anchor), retaining *exactly the same subject DNs*, just a different ICA issuerDN and Root
    - Add some additional ICAs and non-public Roots to the IGTF distribution
      so for IGTF RPs the change is minimal and transparent
    - Inform relying parties, *also outside of the IGTF*, that client trust will become a specific decision. This is probably good, also for OpenVPN services, web access (.htpasswd), &c. The IGTF RPs are not impacted, others likely will be.

User awareness

- This is a change in communications and documentation as well, not only a set of technical changes

- In request systems, have to clearly distinguish for users *which product to order*. For example:

  – "Personal" stays the same, but is called now "Email signing and Encryption"

  – renaming "IGTF MICS Personal" to "Personal Authentication" and explain

  – renaming "IGTF MICS Robot Personal" to "Personal Automated Authentication"

  – forking "IGTF Classic Robot Email"

    - Authentication-only (IGTF) profile "Classic Robot Email"

    - Email signing profile "Organisation-validated S/MIME signing" (i.e. team-based or role-based)

The new TCS Private hierarchies

Two new "RE Trust Roots" (RSA+ECC)

- the cost is (apparently) there
- can be re-used in R&E
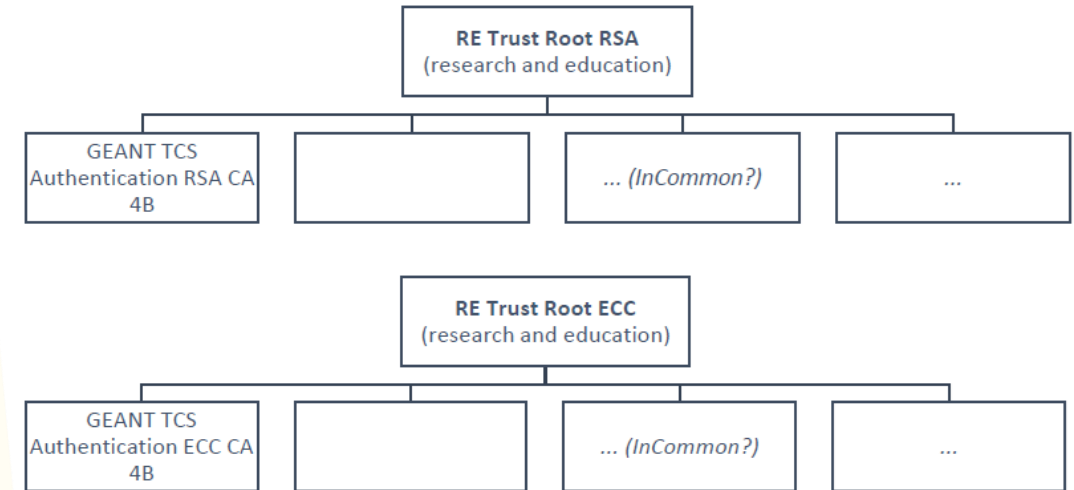
GEANT TCS Authentication RSA/ECC CA 4B issuing subordinate CA

- move all authentication use cases here
- clarify that this is wider than 'just e-science': web site auth, IdP login, any client auth, network login, …
- minimize disruption (at least in theory)

The guidance doc for TCS …

GEANT TCS Gen4 private CA extension

Introduction
The upcoming changes introducing a baseline and specific technical profiles for S/MIME certificates affect the way we have deployed a joint-trust S/MIME and authentication client certificate profile for the 4th generation GEANT Trusted Certificate Service. While the trust and assurance levels defined in the S/MIME Baseline Requirements are currently already met (or exceeded) by the GEANT TCS Personal CAs Certification practices (https://wiki.geant.org/display/TCSNT/TCS+Repository) the technical profiles envisioned for S/MIME BR make it exceedingly hard to continue to use a single issuing CA and publicly-trusted Root CA for both email-signing and client authentication.

Review in the IGTF community, in this case the largest user of client authentication certificates, as well as in the TCS community in general, have concluded that it is both possible and desirable to separate the email S/MIME use cases and the client authentication use cases, with the client authentication being services by an independent, community specific trust model (i.e., a *private CA*) as well as keeping the publicly-trusted S/MIME CA service available for email signing and encryption use cases that are also ubiquitous in the TCS community. Both a public-trust service as well as a private-CA service will be operated in parallel, and both will be available to the entire TCS constituency based on the current assurance practices.

Public trust S/MIME service
For S/MIME public trust certificates, the *current* GEANT TCS Certification practices provide assurance sufficient to meet *sponsor validated* certificates with either a 'legacy' or 'multi-purpose' profile. Sponsor-validated combines Individual (Natural Person) attributes and organizationName (associated Legal Entity) attributes, and through the identity federation and the specific entitlement that is asserted by the organization itself (eduPersonEntitlement combined with the schacHomeOrganisation) the sponsor (i.e. the IdP) is providing validated and verifiable proof of the natural person attributes and takes responsibility for those attribute values.

Hence for the 'GEANT Personal' certificate profile, we can continue to use the current process as-is, using the same entitlements and their provisioning mechanism by their associated home organisations mediated through eduGAIN, to issue publicly-trusted sponsor-validated S/MIME certificates with either a legacy or multi-purpose profile for a (currently) 3-year period.

The GEANT IGTF Robot Email profile
The current GEANT IGTF Robot Email profile is an organizational-mailbox bound certificate, issues based on an invitation process initiated by a (D)RAO in SCM. It has a dual function today: it serves for S/MIME email signing (for automated mailing systems, re-mailing mailing lists, and role-based email sources – all under the control of a designated responsible individual natural person), as well as for use in client authentication where a software agent acts on behalf of a (group of) people.

Since the latter (authentication) case needs a specific technical certificate profile to ensure uniqueness of the subject name of the credential, and needs consistent rendering of that subject name in relying part software systems, its profile is incompatible with the new Baseline Requirements for the legacy and

For the end-entity certificates issued by the GEANT TCS Authentication RSA/ECC CA 4B:

- The subject distinguished name shall be exactly the same as the one generated today based on the (ascii-fied) organsiation name (secondary validation) and ascii-fied state or locality name
- The subject name shall hence be prefixed (in the ASN.1 DER SEQUENCE) with "DC=org", "DC=terena","DC=tcs", followed by country ISO code and organization name, and then followed by the commonName that must include (like today) the common or displayname of the applicant and the applicant uniqueness-identifier (eduPersonPrincipalName) ("/DC=org/DC=terena/DC=tcs/C=NL/O=Nikhef/CN=David Groep davidg@nikhef.nl")
- Personal and Email Robots will follow the current naming scheme as well
- Validation of organization name shall be done in the same way as for all OV validation public trust (CABF BR OV) validations, including the DCV validation of domain association with the organization (for matching the 'academic code', i.e. the *schacHomeOrganization* attribute)
- It shall be possible to specify printable 7-bit stings for the Organization field of the subject name during organization enrolment, and have this validated according to usual standards (CABF OV BR), taking into account that organization names have a printable 7-bit representation that is in line with acceptable national practice and aligned with CABF OV BR guidance.
- The certificate extensions shall be almost the same as today, with the one exception being the policy OIDs for the TCS Personal CA Practice Statement which will be changes to reflect the

https://www.nikhef.nl/~davidg/tcsg4/TCS-Personal-CPS-2.2/GEANT-TCSG4-private-CA-extension-20230712.pdf

In practice …

- … the current state …

Other CABF things to keep in mind

- Server SSL BR has already been updated
  - the provision for using DC prefixing has been retained

- But expect shorter validity periods in the future
  - start preparing for 90-day max in your service deployment automation systems
  - increased use of automation (ACME OV using client ID+secret)
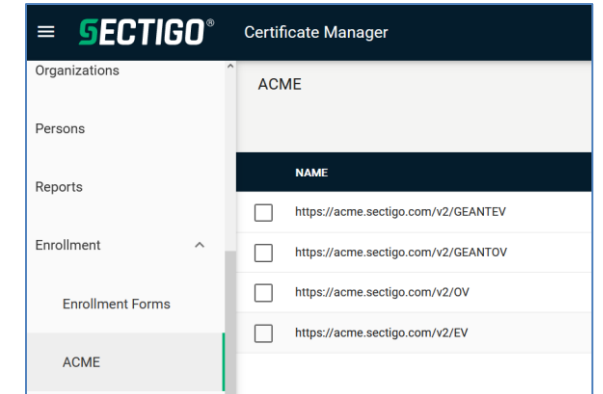
```
[root@hekel ~]# certbot certonly \
  --standalone --non-interactive --agree-tos --email davidg@nikhef.nl \
  --server https://acme.sectigo.com/v2/GEANTOV \
  --eab-kid DUniqueID_forthisclient --eab-hmac-key mv_v3ryl0n9s3cr3tK3y \
  --domain hekel.nikhef.nl --cert-name OVGEANTcert
```

AARC-G071

IGTF AAOPS (https://www.eugridpma.org/guidelines/aaops/)

ATTRIBUTE AUTHORITY OPERATIONAL SECURITY

Taking proper care of trust sources

Protections for (IGTF)
identity providers are known
and documented

- RFC3647
- IGTF Guidelines
- Technical profiles

The AAI relies also on other
attribute sources, and on the
hubs & AARC Proxies

- only generic guidance
- proxies fully hide ID source
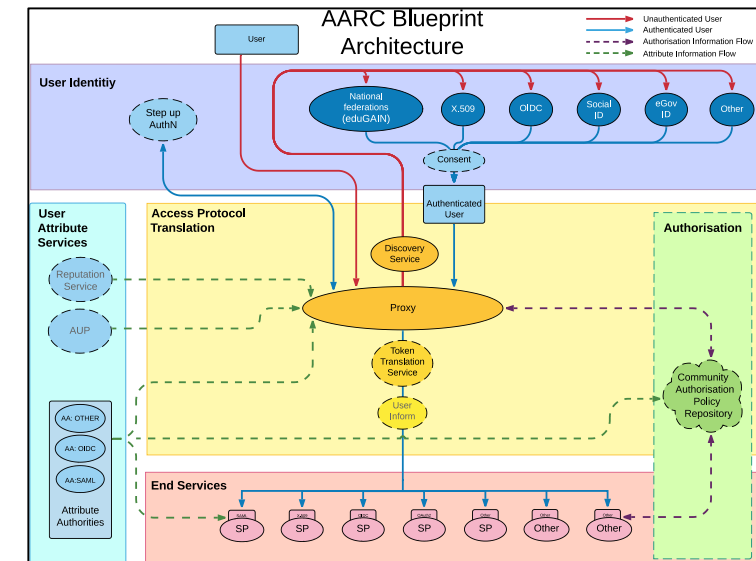
# Operational guideline landscape for - proxy or source - AAI components

RFC6238/4226
FIPS140
NISTSP800-53

AARC Blueprint Architecture

Authentication/identity sources
Sirtfi
(eduGAIN) baselining, RAF
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
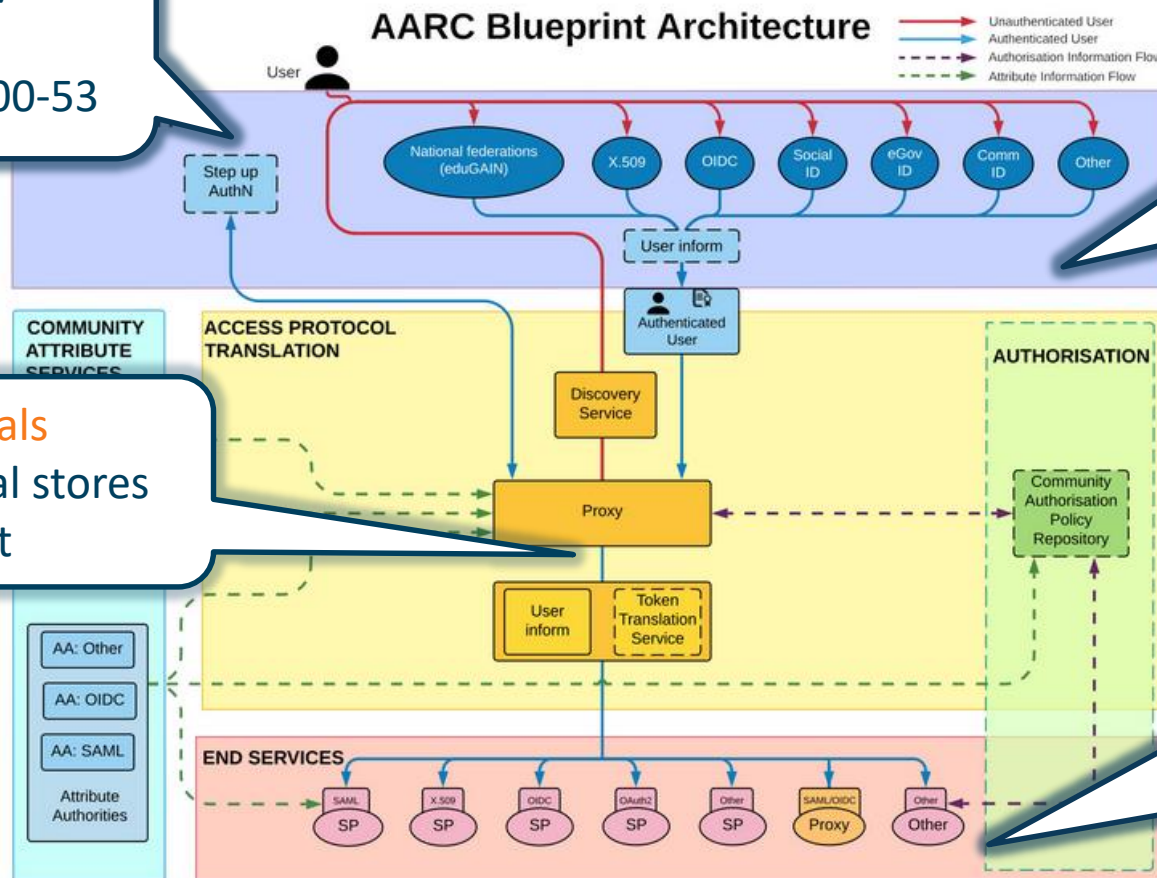
Operational security focus in the BPA: beyond just the IdPs

AARC Blueprint Architecture

Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity
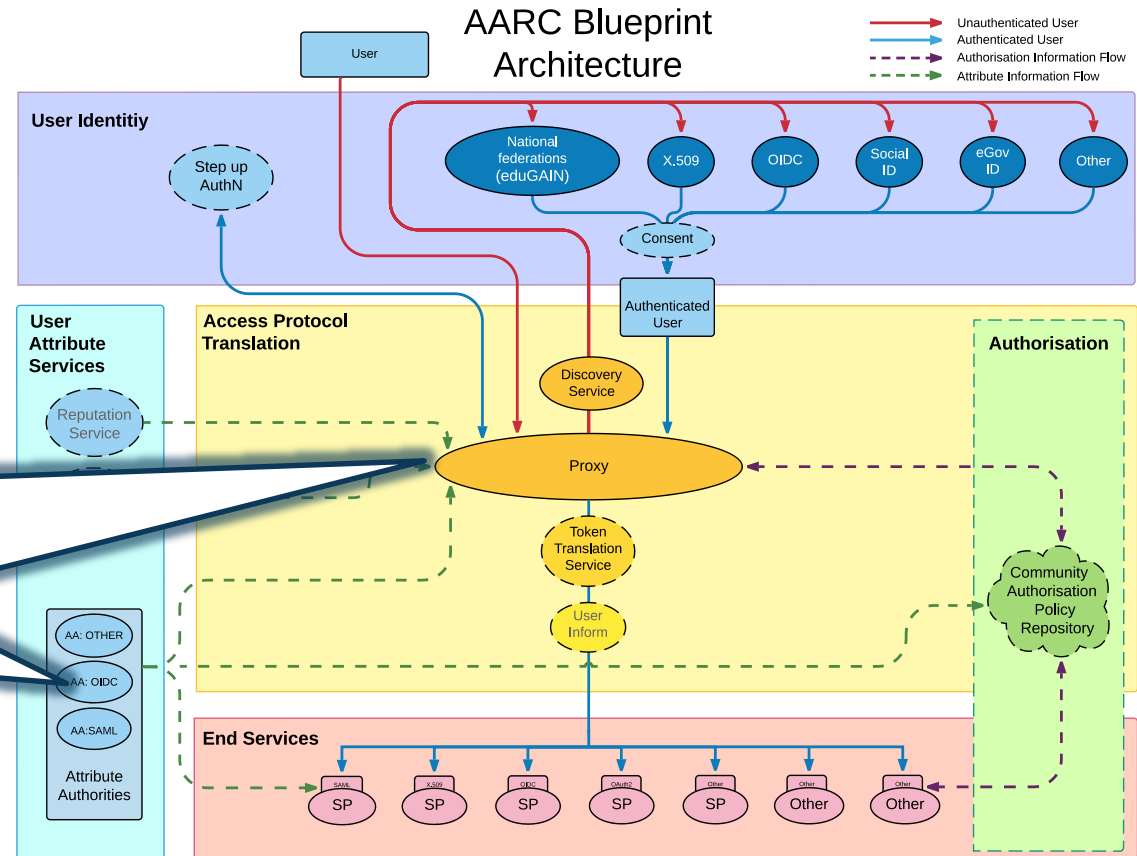
Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements
(AARC-I048, in collaboration with IGTF AAOPS)

AARC-G071: keeping users & communities protected, moving across models

Structured around concept of "**AA Operators**",
operating "**Attribute Authorities**"
(technological entities or proxies),
on behalf of, one or more, **Communities**, that are
trusted by **Relying Parties**

formerly AARC-G048bis

AARC-G071

*Guidelines for Secure Operation of Attribute Authorities
and issuers of statements for entities*

Table of Contents

https://www.igtf.net/guidelines/aaops/   https://aarc-community.org/guidelines/aarc-g071/

Implementation of the AA Operations ("AAI proxy") Security guidelines

1. Major RPs and Infrastructures reviewed it based on current use cases and models

2. Guideline aimed at both Infrastructure and Community use cases

3. Useful input to e.g. 'EOSC' connected proxies as a good practice guideline

4. Assessment or review process is separate – could be IGTF or an RP consortium, but does state what needs to be logged and saved to do a (self) assessment

https://aarc-community.org/guidelines/aarc-g071/

AARC-G071 Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

These guidelines describe the minimum requirements and recommendations for the secure operation of attribute authorities and similar services that make statements about an entity based on well-defined attributes. Adherence to these guidelines may help to establish trust between communities, operators of attribute authorities and issuers, and Relying Parties, infrastructures, and service providers. This document does not define an accreditation process.

Document URL: https://wiki.geant.org/download/attachments/123766269/AARC-G071-Secure-Operation-of-Attribute-Authorities-rev2.pdf
Development information: https://wiki.geant.org/display/AARC/Attribute+Authority+and+Proxy+operational+security
Status: under AEGIS review
DOI: https://doi.org/10.5281/zenodo.5927799 (reserved)
IGTF reference: https://www.igtf.net/guidelines/aaops/
Errata: none
Supersedes: AARC-G048

Deployment guidance included ...

4.2. Attribute Management and Attribute Release

AMR-1

The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.

The community should follow the guidance from relevant policy documents. In particular, the Policy Development Kit has recommendations on Community Membership Management. It is recommended to use standardised attributes where possible, e.g. from eduPerson [EPSC] or SCHAC [SCHAC], and their semantics must be respected.

If Communities make modifications to the attribute set, their semantics, or release policies, it is recommended that they inform both their relying parties as well as the AA Operator thereof, since the AA operator may have implemented checks for schema consistency. The Community is ultimately responsible for the values and semantics of the attributes.

AMR-2

The AA Operator must implement the community definitions as defined and documented, for all the AAs it operates.

By implementing these requirements, the AA operator will support the chain of trust between Community and the RPs. An AA Operator must only host those communities for which it can implement the requirements.

AMR-3

It is recommended that the AA Operator provide a capability for the community to

G071 self-assessment process

- Self-assessment by WLCG, UK-IRIS, eduTEAMS, and SRAM

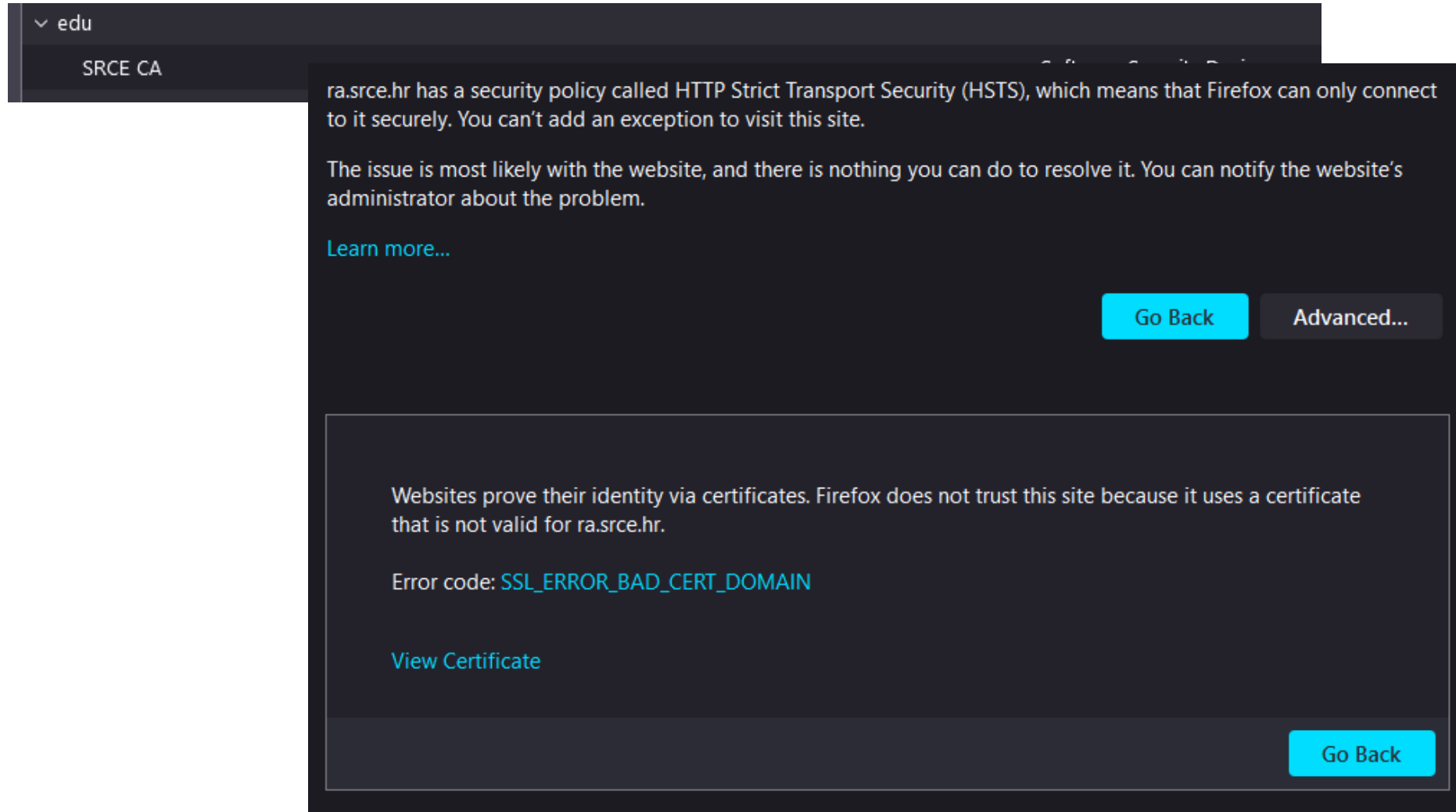- mutual review process also improves on the G071 guideline itself!

https://edu.nl/88dwf

THE CHALLENGE OF SELF-SIGNED ROOTS
AND FF & REDHAT' S IDEA OF WHAT SELF-SIGNED MEANS ...

What happened in FF103? And in RHEL9?

Although it conceptually makes no sense ...

- We know SHA-1 is no longer secure – and all EECs and ICAs moved away – when used as a secure hash algorithm. But …
- now, some projects and distros are (uselessly!) deprecating SHA-1
  also for self-signed (root) certificates

- This affects at least
  - FF103+
  - RHEL9+ (and rebuilds)
- yet … in the cases we could find *only* for CA certs
  that are not in the WebPKI (and distro) public trust list

This impacts both joint-trust and igtf-only trust when installed in a non-system location. But thy system locations are different is not obvious from the doc …

Rocky9+, AlmaLinux9+, RHEL9+ and

With RHEL9 also deprecating SHA-1, but *at the same time*
still having self-signed SHA-1 based root certs in the ca-certificates
package, depends on a RedHat/OSSL proprietary set of 'bonus bits'
appended to the end of the ASN.1 certificate blob.

For the others, there is – for now – a policy override:

update-crypto-policies --set DEFAULT:SHA1
update-crypto-policies --set LEGACY

even if that is a rather course-grained and blunt tool

The ca-certificates package in RH9

Interestingly, EL9 *does* ship with a lot of SHA-1 root CAs in
    ca-certificates-2022.2.54-90.2.el9.noarch.rpm
and the p11-kit sources thereof (and thus e.g. /etc/pki/tls/certs/ca-bundle.crt)
contain SHA-1 self-signed roots that do work on EL9.

- this relies on the OSSL proprietary 'trust bytes' in a BEGIN TRUSTED CERTIFICATE blob
- such blobs allow SHA-1 for self-signed roots, but are not standarised

Yet the 'simple' solution, to ship both the EL/OSSL proprietary 'trust' bytes as well as a regular PEM formatted root does *not* work (thanks to Brian Lin for testing that!)

Mitigations?

Meanwhile,
- if you still have a SHA-1 root
- and you are able to re-issue with the same key (and new serial)
- and your EECs *do not* have dirname+serial in their AKI

your CAs should probably re-issuing its root because that is easier.

But for the large ones, esp. the DigiCert Assured ID Root from 2006 for instance, that will be hard.
And migrating to another (SHA-2 rooted) signing hierarchy will take at least 395 days ... and a lot of engineering on the RP and CA side

The root cause is with RH not understanding what a self-signed trust anchor is, but that will not help us in the short term.

Reissuance of roots?

ASGCCA-2007
BYGCA
CNIC
DZeScience
DigiCertGridRootCA-Root
KEK
MARGI
RDIG
SRCE
TRGrid

ArmeSFo
CESNET-CA-Root
DFN-GridGermany-Root
DigiCertAssuredIDRootCA-Root
IHEP-2013
LIPCA
QuoVadis-Root-CA2
RomanianGRID
SiGNET-CA
seegrid-ca-2013

Fixed by now: GridCanada, CILogon basic/silver/OpenID, UKeScienceRoot-2007

Questions?

BUILDING OUR GLOBAL TRUST FABRIC

David Groep *davidg@nikhef.nl*

https://www.nikhef.nl/~davidg/presentations/

https://orcid.org/0000-0003-1026-6606

this work is co-supported by the Trust and Identity work package of the GEANT project (GN5-1)

in collaboration with many, many people in the AARC+ Community, including Christos Kanellopoulos, Nicolas Liampotis, Licia Florio, Hannah Short, Maarten Kremers, Niels van Dijk, David Crooks, Dave Kelsey, Ian Neilson, Mischa Sallé, Jens Jensen, and so many others!

Thank you

davidg@nikhef.nl

GÉANT
Networks · Services · People
www.geant.org