IGTF
Interoperable Global Trust Federation
AP | EU | TAG

Assessing Combined Assurance

Introducing composites of DOGWOOD and BIRCH/CEDAR in EGI and beyond

David Groep
Nikhef

co-supported by the Dutch National e-Infrastructure coordinated by SURF, and by EGI Core Services

EGI Combined Assurance use case

- IOTA AP assurance level 'DOGWOOD' *is* different,
  but remainder of the assurance can be taken up somebody else
  – the user community or the registrar for the Access Platform

- Only thing you get is an opaque ID

- Stepping up to adequate assurance:
  - Real names from pseudonyms
  - Enrolling users in a community
  - Keeping audit records
  - Auditability and tracing
  - Incident response

Identity elements

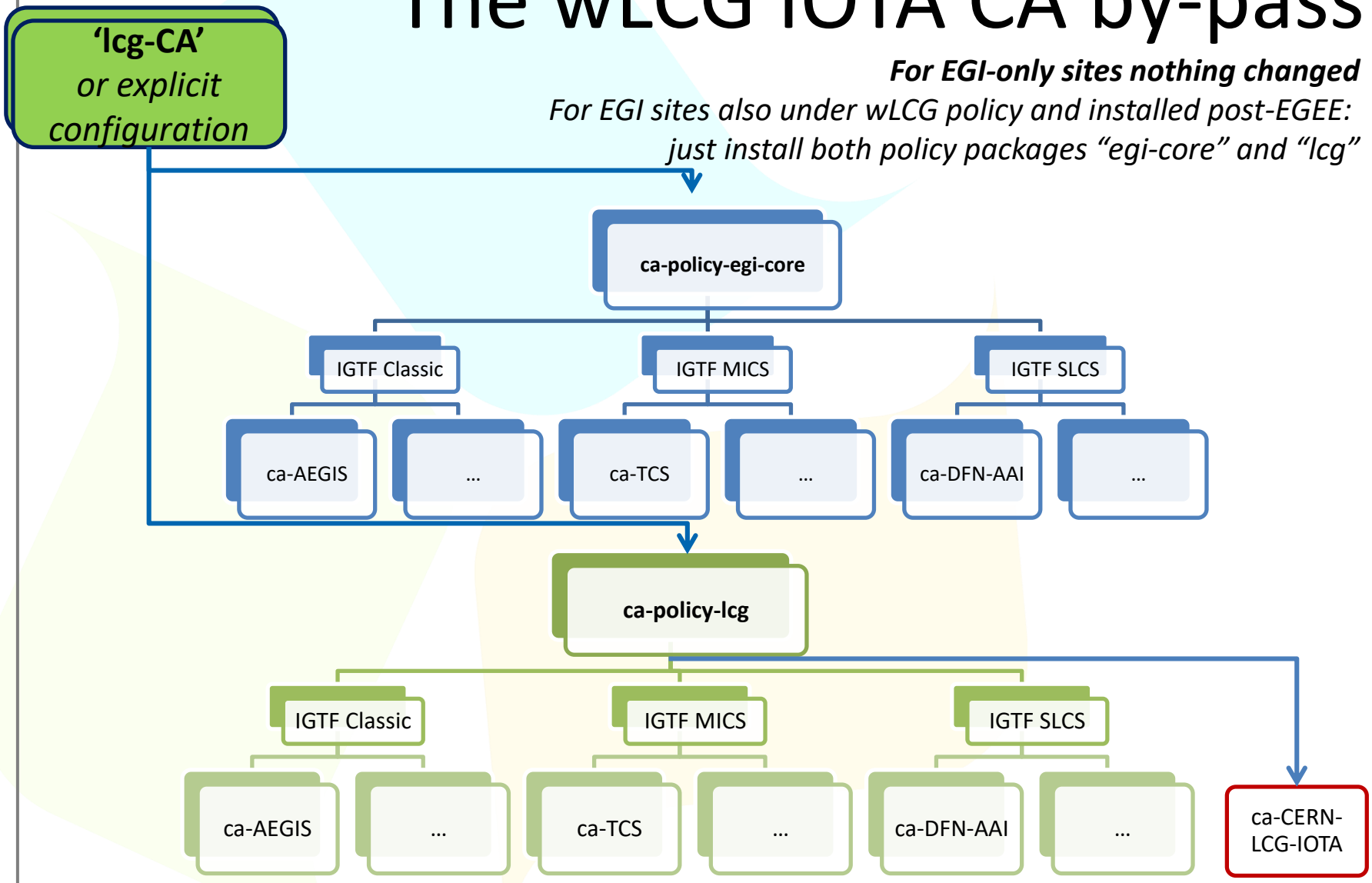
- identifier management
- re-binding and revocation
- binding to entities
- traceability of entities
- emergency communications

- regular communications
- 'rich' attribute assertions
- correlating identifiers
- access control

The wLCG IOTA CA by-pass

For EGI-only sites nothing changed

For EGI sites also under wLCG policy and installed post-EGEE:
just install both policy packages "egi-core" and "lcg"



Project MinE (ALS) use case

- Access traditional global grid resources from the CLI
- By users that have no PKIX experience
  but are all properly vetted and registered
  (in the SURFsara CUA)
- Case comparable to LHC VOs (and to ELIXIR)
- Give access based on DOGWOOD CUA ID – and prepopulate a VOMS server based on CUA details

Thanks to Mischa Sallé

INTERLUDE

A proxy from the TTS: the ad-hoc way

https://rcdemo.nikhef.nl/getproxy/

AARC Authentication and Authorisation for Research and Collaboration

AARC - one-time-password getproxy demo service

- ○ Plain grid proxy
- ◉ VOMS proxy (rcdemo.aarc-project.eu)

get proxy

Lifetime in hours (optional, default 12): 12

IdP entityID (optional, default: present WAYF):

RCauth.eu The white-label Research and Collaboration Authentication CA Service for Europe

English | Nederlands | Español | Français | Deutsch

You have previously chosen to authenticate at **Nikhef**

Login at Nikhef

eduGAIN | Research and e-Infrastructures | InCommon | Czech | Denmark | Germany | Greece | Italy | Netherlands | Sweden | Switzerland | UK | Other countries | Miscellaneous

Incremental search...

Nikhef

additional info: Mischa Sallé, msalle@nikhef.nl

A one-time URL giving a shell script

https://rcdemo.nikhef.nl/getproxy/index.php?code=https%3A%2F%2Faai.egi.eu%2Fmp-oa2-server%2FauthzGrant%2F7d20a61e6a3a393c0c209f7a81706

You can now retrieve your proxy by running:

```
curl "https://rcdemo.nikhef.nl/getproxy/?hash=b45131f115e5c0c43a1c5f1c003ed28979d59d9a7d30f439a8b4741ec4ea5a77" | sh
```

NOTE:

- This link will expire in **10 minutes** (at 21:04:56 UTC)
- You can use this link only **once**

return to client

bosui:/user/davidg (davidg:emin)

```
bosui(~) 22.55$ curl "https://rcdemo.nikhef.nl/getproxy/?hash=b45131f115e5c0c43a1c5f1c003ed28
979d59d9a7d30f439a8b4741ec4ea5a77" | sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  9572    0  9572    0     0  52108      0 --:--:-- --:--:-- --:--:-- 4673k
Successfully stored a local copy of your proxy in /tmp/x509up_u5917
bosui(~) 22.55$ voms-proxy-info | head -10
Picked up JAVA_TOOL_OPTIONS: -Xmx512M
subject   : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHkZMTHoVTtT6/CN
=1839098942/CN=1028921420
issuer    : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHkZMTHoVTtT6/CN
=1839098942
identity  : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHkZMTHoVTtT6
type      : RFC3820 compliant im
strength  : 2048
path      : /tmp/x509up_u5917
timeleft  : 11:58:59
```

```
#!/bin/sh
X509_USER_PROXY=/tmp/x509up_u$(id -u)
if [ -f $X509_USER_PROXY ];then
    chmod 0600 $X509_USER_PROXY
fi
umask 0377
cat > $X509_USER_PROXY << EOF
-----BEGIN CERTIFICATE-----
MIINLjCCDBagAwIBAgIEFh/2SDANBgkqhkiG9w0BAQsFADCBnDESMBAGCgmSJomT8ixkARkWAmV1
MRYwFAYKCZImiZPyLGQBGRYGcmNhdXRoMR4wHAYKCZImiZPyLGQBGRYOcmNhdXRoLWNsaWVudHMx
EjAQBgNVBAoMCW5pa2hlZi5ubDElMCMGA1UEAwwcRGF2aWQgR3JvZXAgUUstREhrWk1USG9WVHRU
NjETMBEGA1UEAxMKMTgzOTA5ODk0MjAeFw0xNzA5MjEyMDUyMjFaFw0xNzA5MjIwODU3MjFaMIGw
MRIwFAYKCZImiZPyLGQBGRYCZXUxEjAUBgolkiajk/IsZAEZFgZvY2F1dGgxHjAcBgolkiajk/Is
```


additional info: Mischa Sallé, msalle@nikhef.nl

Register your ssh public key – like in gitlab, sourceforge, &c

https://aai.egi.eu/sshkeys/

EGI MasterPortal

SSH Public Key Upload Portal

Via this portal you can upload one or more OpenSSH public k
authentication you can then retrieve RCauth.eu-based proxy

You need to login via EGI's test online CA.

https://aai.egi.eu/sshkeys/

EGI MasterPortal

SSH Public Key Upload Portal

logout

You are currently logged in as: ***davidg@nikhef.nl***

	Label	Public key	Description
◉	davidg-ikonet-nikhef-nl	ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAzd+YrpvDWbG65l5msiNnqv6gXGb1Qe421187RE6dHKa4Mm5oBFWh /H7JF1W9DRTRAex5seKXFHhcUKbtaT2NCTX8zdwTxAZMlMq6qeCX /DnbwjXO1P2XTC6H3jP3hwlTzITeipFnDNfMo+O9HFpByPjIcnTB/Zf7m1NEdXFkr	
○	davidg@lapdavidg	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCvXT9wFN0xVg33suYb6t5Il18MpIy5KXM/SWpMkFzjCJJCH1dh0K /x8YInvFfo/nBdN81 /jPDxww9VzSV2ZwDx1Sj3YwTRRubG1nEvTkKfSmnbY0FMUoPa6kOHWJOahpA+zTBS8yz	

Add new SSH Key

Upload *new* SSH public key Browse... No file selected.

or enter value of *new* public key

Specify label for *new* key (optional)

Specify description *new* key (optional)

add new public key

Update selected SSH Key

Upload *updated* SSH public key Browse... No file selected.

or enter value of *updated* public key

Specify description *updated* key

update selected key remove selected key

additional info: Mischa Sallé, msalle@nikhef.nl

Hiding PKIX – just like KRB

- Implicit retrieval of proxies using ssh-agent
- Resulting proxies can decorated with VOMS without need for passphrases or other credentials

```
bosui:/user/davidg (davidg:emin)
Using username "davidg".
Authenticating with public key "davidg-ikonet.nikhef.nl [2048 bit RSA]" from age
nt
Last login: Thu Sep 21 22:46:10 2017 from 2a07:8500:120:e03b::1000
bosui(~) 22.47$ ssh proxy@ssh.aai.egi.eu > /tmp/x509up_u$(id -u) && chmod 0400 /tmp/x509up_u$(id -u)
PTY allocation request failed on channel 0
Connection to ssh.aai.egi.eu closed.
bosui(~) 22.47$ grid-proxy-info
subject  : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHkZMTHoVTtT6/CN=1839098942/CN=267447935
issuer   : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHkZMTHoVTtT6/CN=1839098942
identity : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHkZMTHoVTtT6
type     : RFC 3820 compliant impersonation proxy
strength : 2048 bits
path     : /tmp/x509up_u5917
timeleft : 11:59:48
bosui(~) 22.47$
```

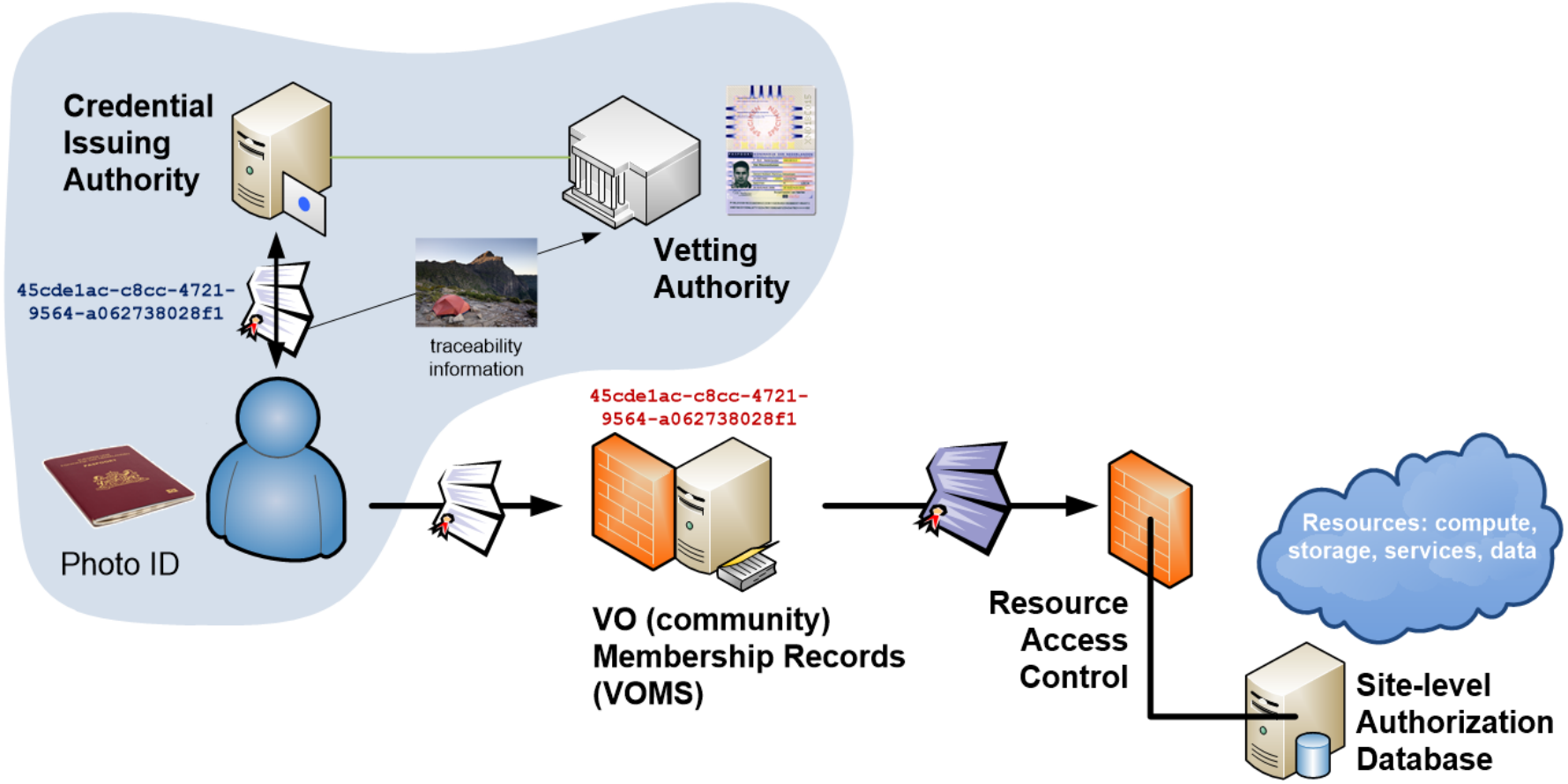
- Predictable RCauth subject naming (USR) allows pre-registering in VOMS, COmanage, &c

additional info: Mischa Sallé, msalle@nikhef.nl

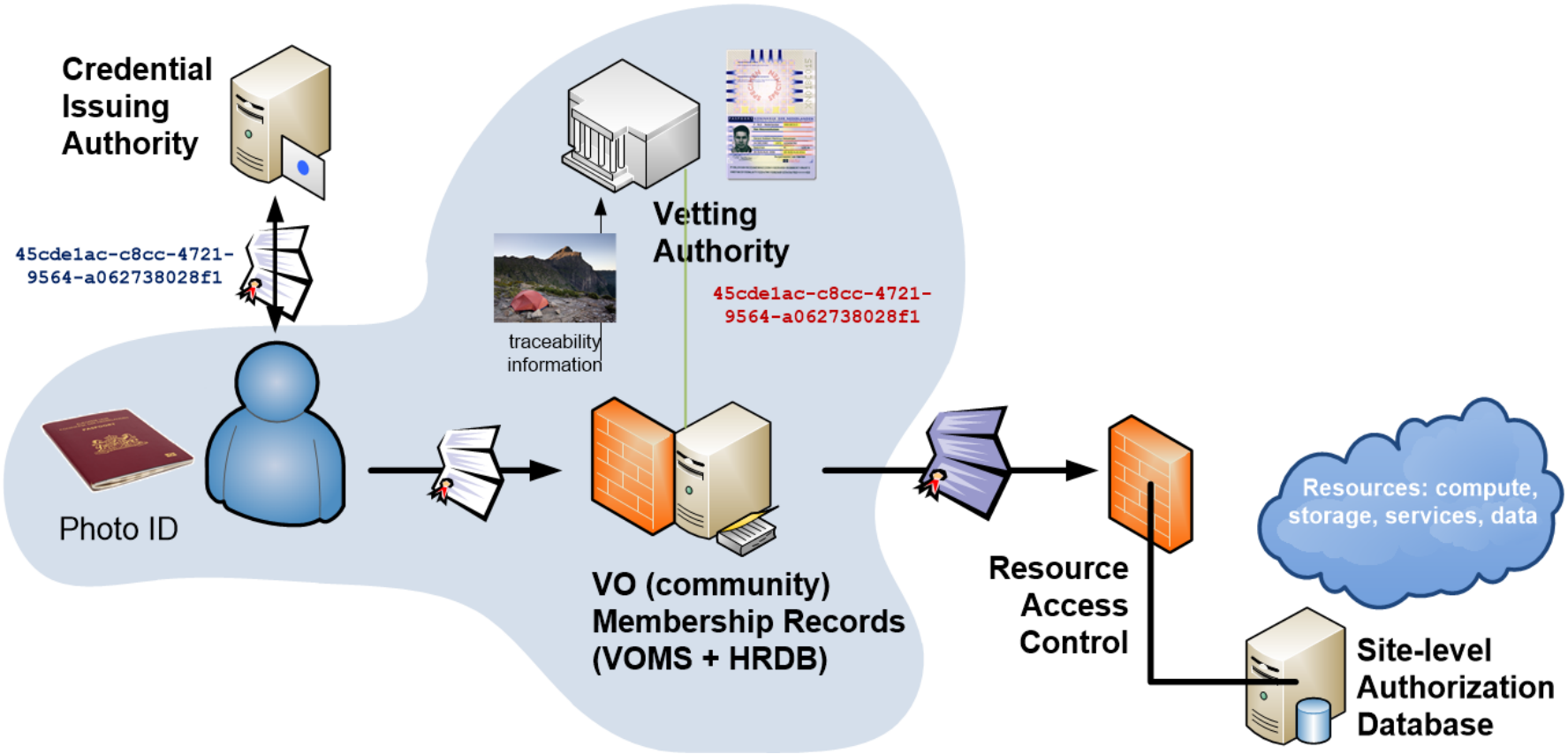
Beyond DOGWOOD (CERN IOTA, RCauth, CILogon Basic)

- Old model: CERN STS tight VO binding model
  - With the EGI and WLCG specific exception
- EGI combined assurance model
  - Make assurance combination part of service AuthZ
  - Implemented by major AuthZ frameworks: Argus (1.7.1+), LCMAPS, dCache (3.1+)
  - Configuration shipped via EGI and WLCG
- But: which ‘other’ assurance providers qualify?

Distributed Responsibilities I: Trusted Third Party



Distributed Responsibilities II: Collaborative Assurance & Traceability



IOTA in the EGI context

EGI – by design - supports loose and flexible user collaboration

- 300+ communities
- Many established ‘bottom-up’ with fairly light-weight processes
- Membership management policy* is deliberately light-weight
- Most VO managers rely on naming in credentials to enroll colleagues

Only a few VOs are ‘special’

- LHC VOs: enrolment is based on the users’ entry in a special (CERN-managed) HR database, based on a separate face-to-face vetting process and eligibility checks, including government photo ID + institutional attestations
- Only properly registered and active people can be listed in VOMS

Developing an assessment framework

SPG:Drafts:Assessment Community IDvetting adequacy

Authentication and identification is considered adequate, for each User authorised to access Services, if the combined assurance level provided by the end-user credential issuing authority, and either the e-Infrastructure registration service and/or the VO registration service, meets or exceeds the requirements of the approved IGTF authentication assurance profiles [AAP].

The Community or e-Infrastructure wishing to prove the adequacy of its identity vetting, in order to use its members' credentials in conjunction with the IGTF Assurance Profile DOGWOOD, must submit a request for assessment by the EGI Security Policy Group to EGI operations.

The request shall include the following information:

- a statement of their compliance with the Community Membership Management Policy
- a statement of their compliance with the Community Operations Security Policy
- a documented description of the membership life cycle process and practices meeting the requirements of the IGTF BIRCH, CEDAR (or ASPEN) assurance level, in which
  - the *credential* of the user is the membership registration data and community-issued assertions
  - the *Issuing Authority* is the collection of membership management and assertion-issuing systems and services
  - the *credential life time* corresponds to the renewal periods as defined in the Community Membership Management Policy
- a description of the method of binding between the membership information and the DOGWOOD user credential

Based on this information, the EGI SPG shall advise the EGI Operations Management Board with respect to suitability of the Community or e-Infrastructure for such combined adequacy in accordance with the Policy on Acceptable Authentication Assurance.

The SPG may make available an evaluation matrix. Applicant communities are welcome to use the assurance evaluation matrix to prepare the requisite documents, bearing in mind the evaluation *Method* and the *Persistent registry (community membership) implementation and assessment hints*. The most relevant community assurance profiles for the joint adequacy purpose are BIRCH and CEDAR. Registries and membership services at ASPEN level are strongly discouraged. The credential (registration) life time of 11 days necessitates re-registering members with this frequency, and re-validating their eligibility. This model is likely to both confuse and upset members.

The need for guidance

Category:
Status: Endorsed
igtf-authn-assurance-1.1-20161026.docx
Editor: David Groep
Last updated: Fri, 09 June 2017
Total number of pages: 7

IGTF Levels of Authentication Assurance

Version 1.1-2016

Abstract
The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.
The IGTF Levels of Authentication Assurance (LoA) generalization process aims to extract those elements from 'Authentication Profiles' the IGTF has developed that are of general value to the community. The LoAs described in this document represent the consensus on acceptable levels for

Assessment Matrix

- Mapping for PKIX/RFC3647 is trivial
- How to apply out BIRCH/CEDAR guidance to community registries?

	Profile							
	URI							
	Template	*v01-20170612*						
	Authority			Peer				
Profile	AP source	Description	See also	Method	PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints	Hints for other renderings	Scoring
all	2, line 1	operated as a long-term commitment		contact data should refer to an organisation, not a project, and the description should (implicitly) address sustainability	1.3.1	specific obligations are put on the registry, so a persistent organsiation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator.		
all	3.1, line 1	credentials bound to act of vetting	See also 4.2	description of the proof of posession of key material (asymmetric private keys, symmetric passwords or pin codes, authentication devices delivered or assorciated with users). The process must ensure that the vetting and	3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry.		

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

- Relevant for COmanage & VOMS communities, but maybe wider?

Discussion!

BUILDING A GLOBAL TRUST FABRIC