



Authentication and Authorisation for Research and Collaboration

The RCauth.eu CILogon-like service in the EGI AAI

*The CILogon-like TTS Pilot, its scalability and applicability
in the EGI Infrastructure landscape*

David Groep

AARC NA3 coordinator

Nikhef PDP (Advanced Computing for Research) group



EGI AAI TCB

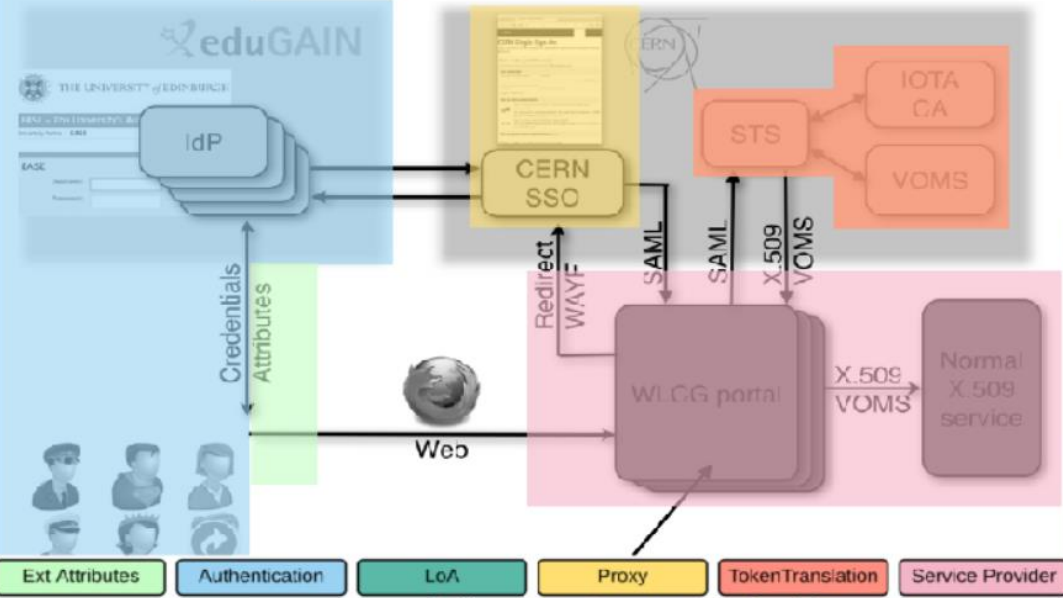
Feb 8th, 2017

The AAI evolution of e-Infrastructures and Research Infrastructures

- Most infrastructures move to completely hiding PKIX from the end-user
 - Less credentials to manage, appearing 'simpler' to the user, but ...
 - EEPKI + RFC3820 proxies **did solve both the CLI and delegation use case rather nicely!**
- Bridging and translation is the pragmatic approach
 - Does not require major technical changes in existing R&E federations
 - Allows for community-centric identities-of-last-resort (or first resort, for that matter!)
 - Time line is more predictable, because fewer entities are involved – and those entities have a stake in and the benefits off the results
- Emerging as a pattern in many Research Infrastructures that use CLI or brokerage
 - ELIXIR, UMBRELLA, WLCG, INDIGO DC
 - SAML->OIDC, SAML->X509, X509->OIDC, X509->SAML, OIDC->X509, ...

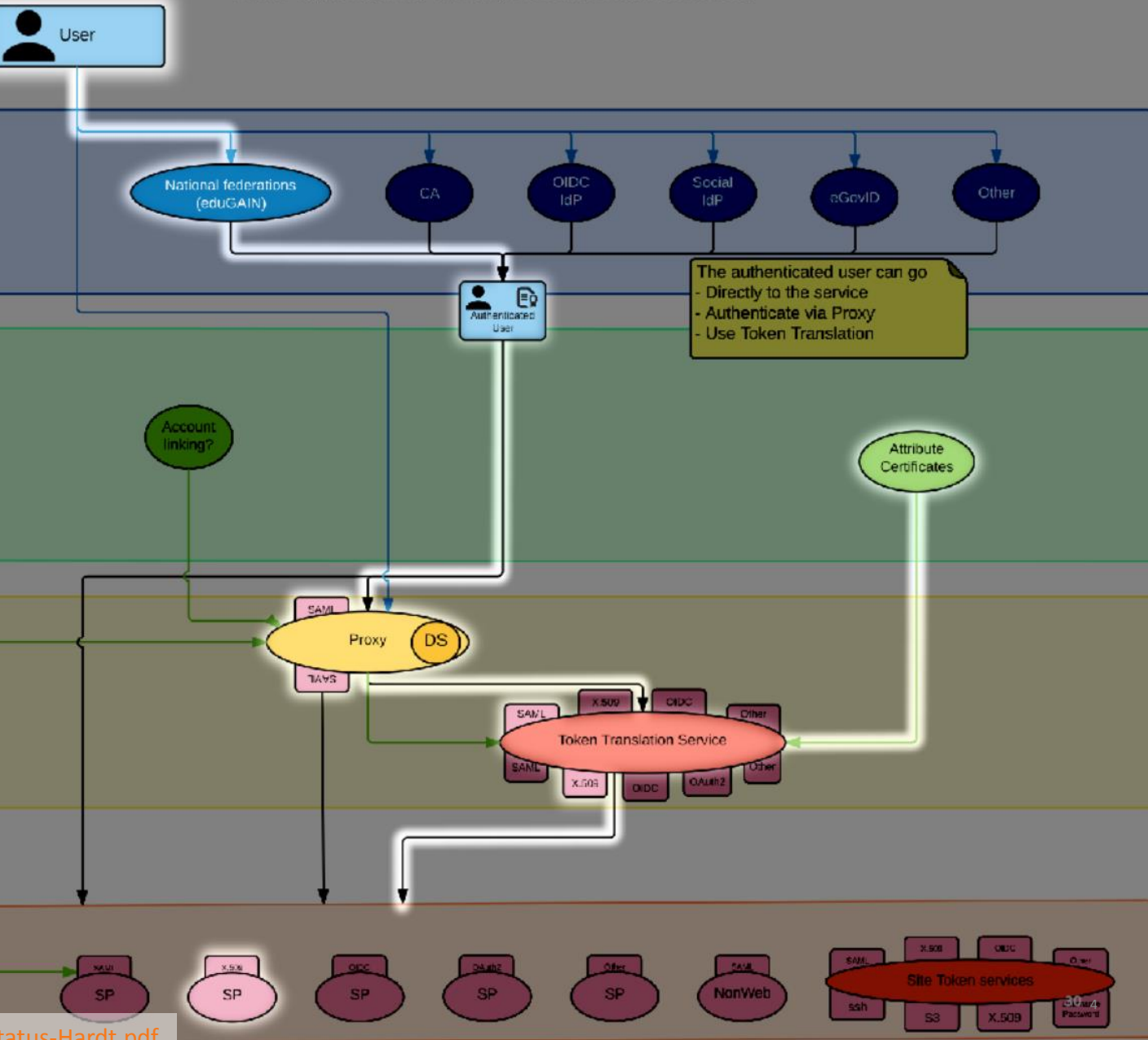
RCauth and 'CILogon-like Pilot' - aims

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



AAI: The e-Infrastructure view

What is happening on top of existing Federation infrastructures today



Example: WLCG

Although the TTS looks like a 'box', it is an interactive component that usually requires initially the user to be 'in the loop'

PKI targeting translation services – an overview



CI Logon Service

NCSA (IL,USA) operated service and project
InCommon backed MICS and IOTA



CERN w/ LCG IOTA CA
*eduGAIN backed with added
CERN HR DB controls*



Generic 'opaque' certificate in Europe
*Helps with PII data protection and
integration with ESFRIs and e-Infrastructure*

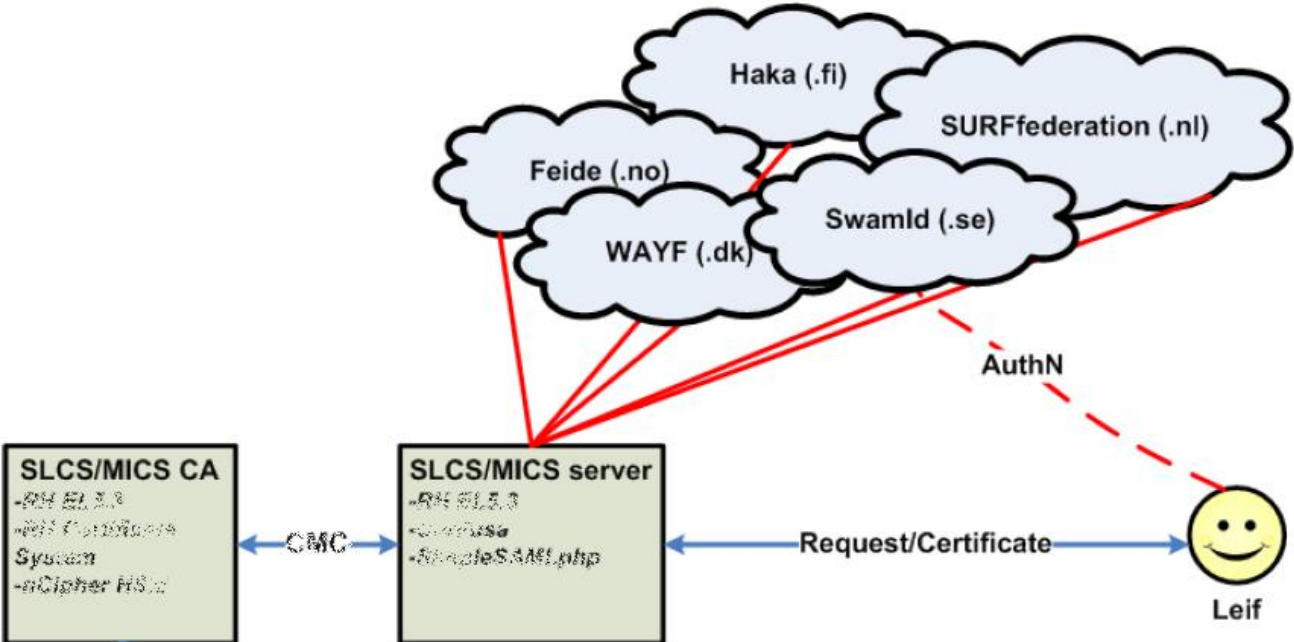


GEANT Trusted Certificate Service TCS
*could be turned into a translation service,
when each subscriber would enable that since
it has a subscriber-centric validation model*

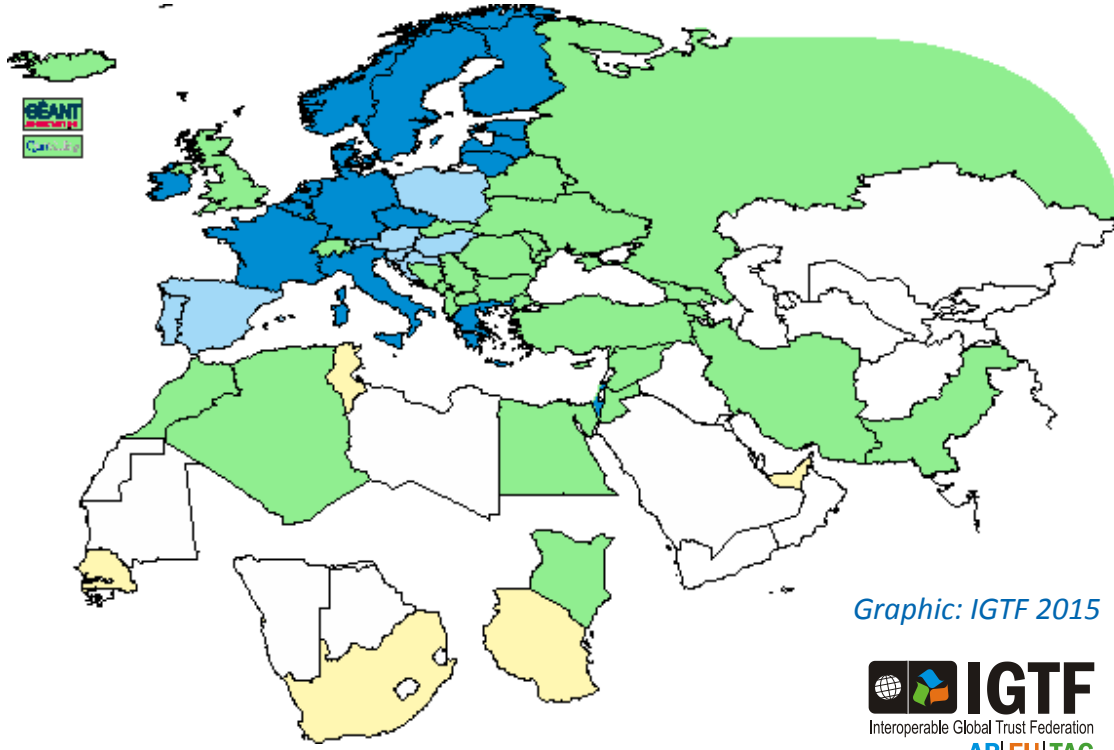
Leveraging R&E federations: TCS, DFN SLCS, CILogon ... - with extended LoA

Bridging conventional R&E federated organisations to the trusted e-Infra world requires more

- Release of relevant attributes, unique non-reassigned ID, higher assurance profile **via contracts**



Graphic from: Jan Meijer, UNINETT



Graphic: IGTF 2015



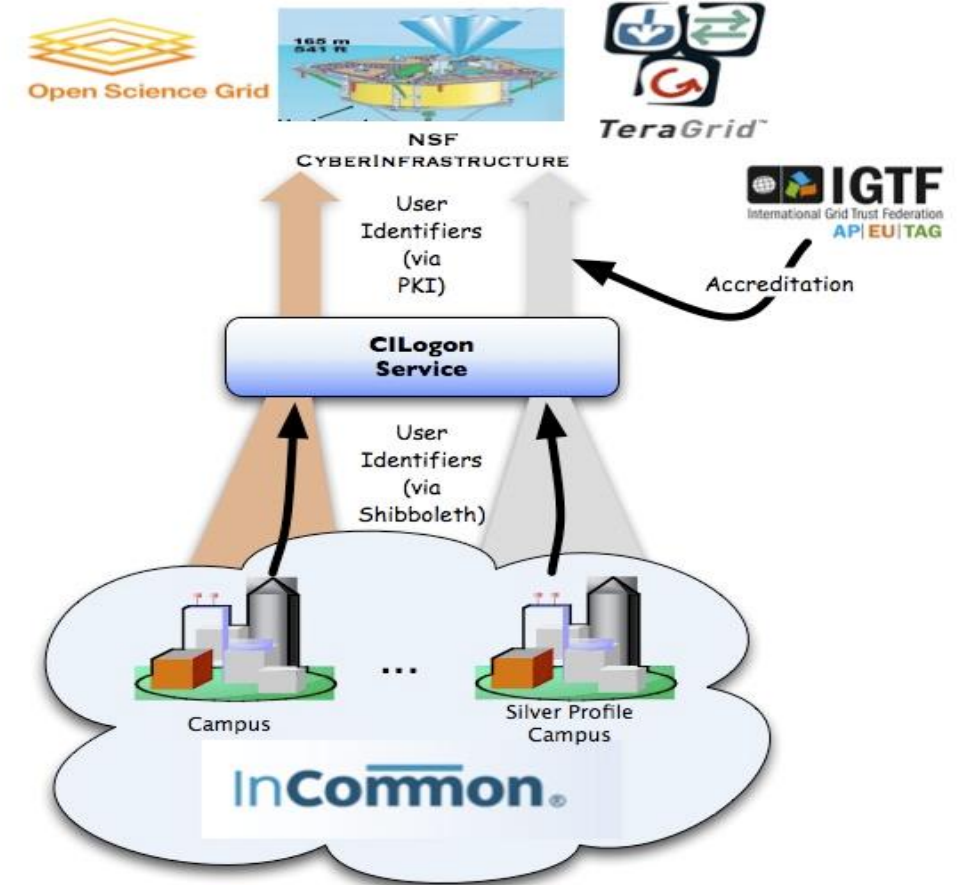
CILogon service and project (Jim Basney et al.)



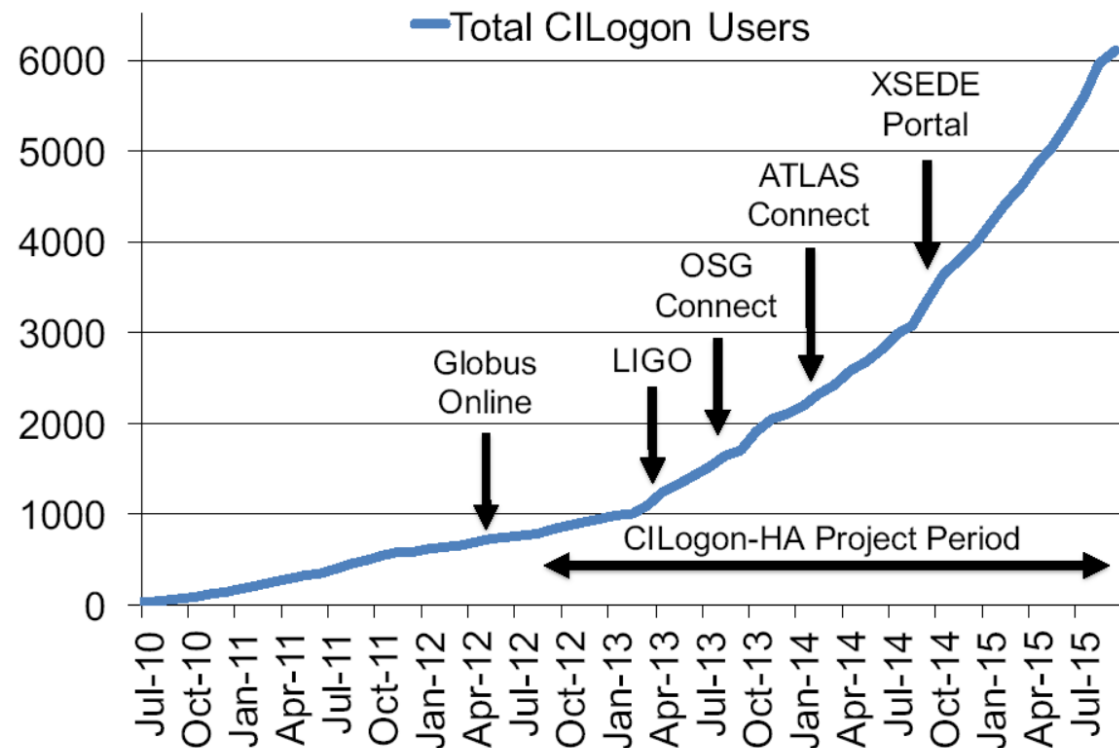
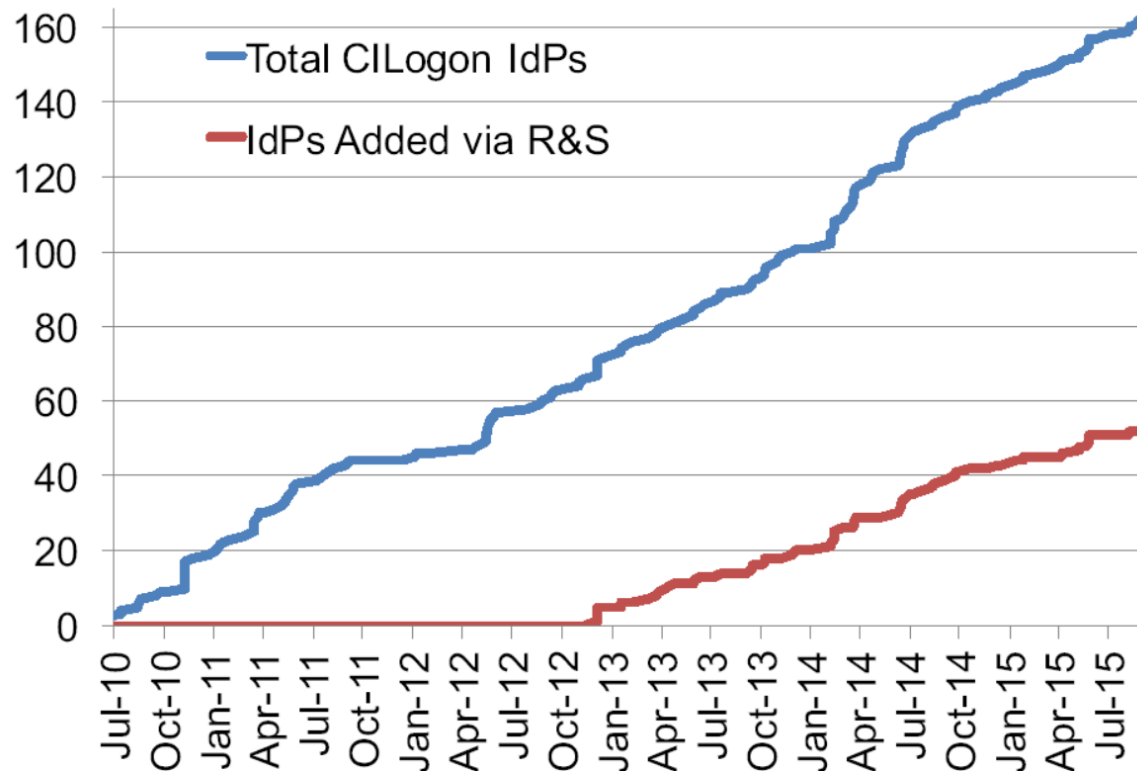
- Enable campus logon to CyberInfrastructure (CI)
 - Use researchers' existing security credentials at their home institution
 - Ease credential management for researchers and CI providers

Multiple interfaces

- SAML/OpenID Web Browser SSO
 - PKCS12 certificate download
 - Certificate issuance via OAuth
 - OpenID Connect token issuance
 - SAML ECP for CLI issuance



CILogon adoption in the US/InCommon



But many elements are coming together now!

- e-Infrastructure & IGTF differentiated assurance profiles: DOGWOOD (IOTA), CEDAR/BIRCH (Classic, MICS)
- Research communities establishing themselves higher-quality attribute stores
- Better community management and more structured user communities

- Attribute release conventions and scalable methodologies like REFEDS R&S
- Higher awareness of multi-actor AAI and ‘VOs’ within the traditional R&E federation world
- “Operationalizing” federations, e.g. through traceability and incident response (Sirtfi)

- Software evolution for non-web use cases (OIDC – OAuth2, SAML ECP, MyProxy, ...)

Selective trust for (federated) baseline assurance credentials in EGI *based on the Acceptable Authentication Assurance policy*



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

A few VOs provide independent assurance elements

- LHC VOs: enrolment is based on the users’ entry in a special HR database, based on a separate face-to-face vetting process and eligibility checks, including government photo ID + institutional attestations
- ELIXIR directory and bona-fide management
- NGI-consultancy-backed vetting for LToS community (likely, though as of yet unconfirmed)
- ... *a few more, probably ...*

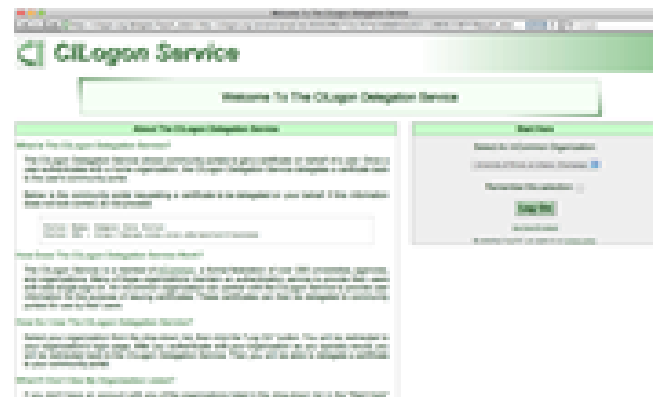
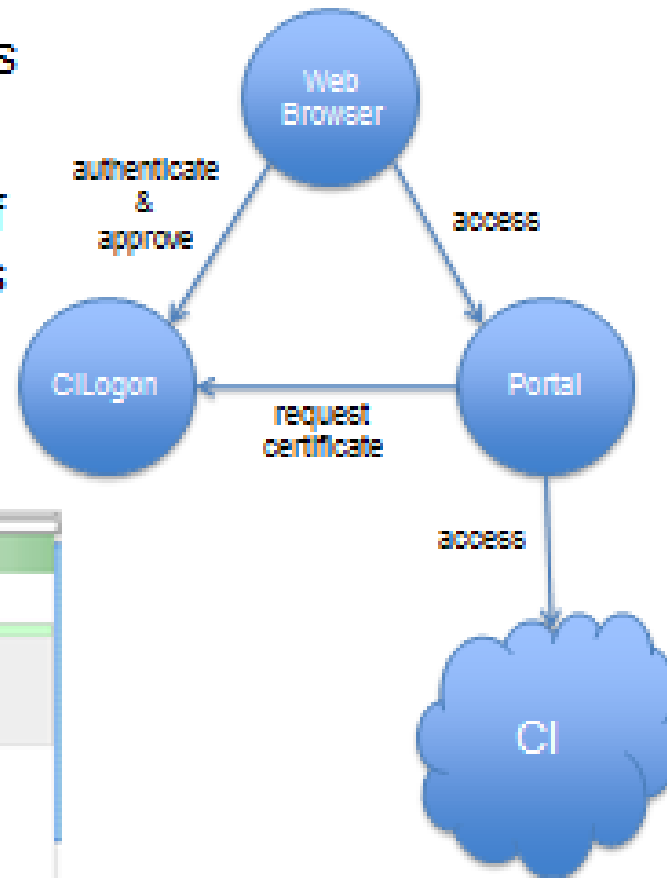
for these communities, combined IOTA identifiers + VO enrolment assurance is adequate for entry

EGI ‘combined-adequacy-model’ (or ‘cam’) policy bundle to be distributed in v1.81, due Feb 28th 2017

All the elements in place: Credential Translation & Management

CILogon Portal Delegation

- Grid Portals and Science Gateways provide web interfaces to CI
 - Portals/Gateways need certificates to access CI on researchers' behalf
- CILogon Delegation Service allows researchers to approve certificate issuance to portals (via **OAuth**)
- www.cilogon.org/portal-delegation



www.cilogon.org

Slide: Jim Basney,
NCSA and CILogon

AARC SA1 “CILogon-like Pre-Pilot”

Establish a CILogon (like) service in Europe

- Integrated closely with R&E federation landscape (with all of full-mesh, H&S, mixed-models)
- Integration with user community services and attribute services
- Close co-operation with the CILogon Project (Jim Basney et al.)

Pilot work based on AARC (and also EGI) requirements gathering

- FIM4R requests, alignment with known user communities (EGI evolution, ELIXIR)
- Potential to support the EGI ENGAGE community ‘competence centre’ work
- Leveraging existing components and services: CILogon + ‘OAuth4MyProxy’ components, VOMS Attribute Certificate service, OIDC libraries, ...
- Fit in the existing policy framework: Approved Robots (and “PUSPs”), Trusted Credential Stores, PKP Guidelines, IGTF ‘DOGWOOD’ ...

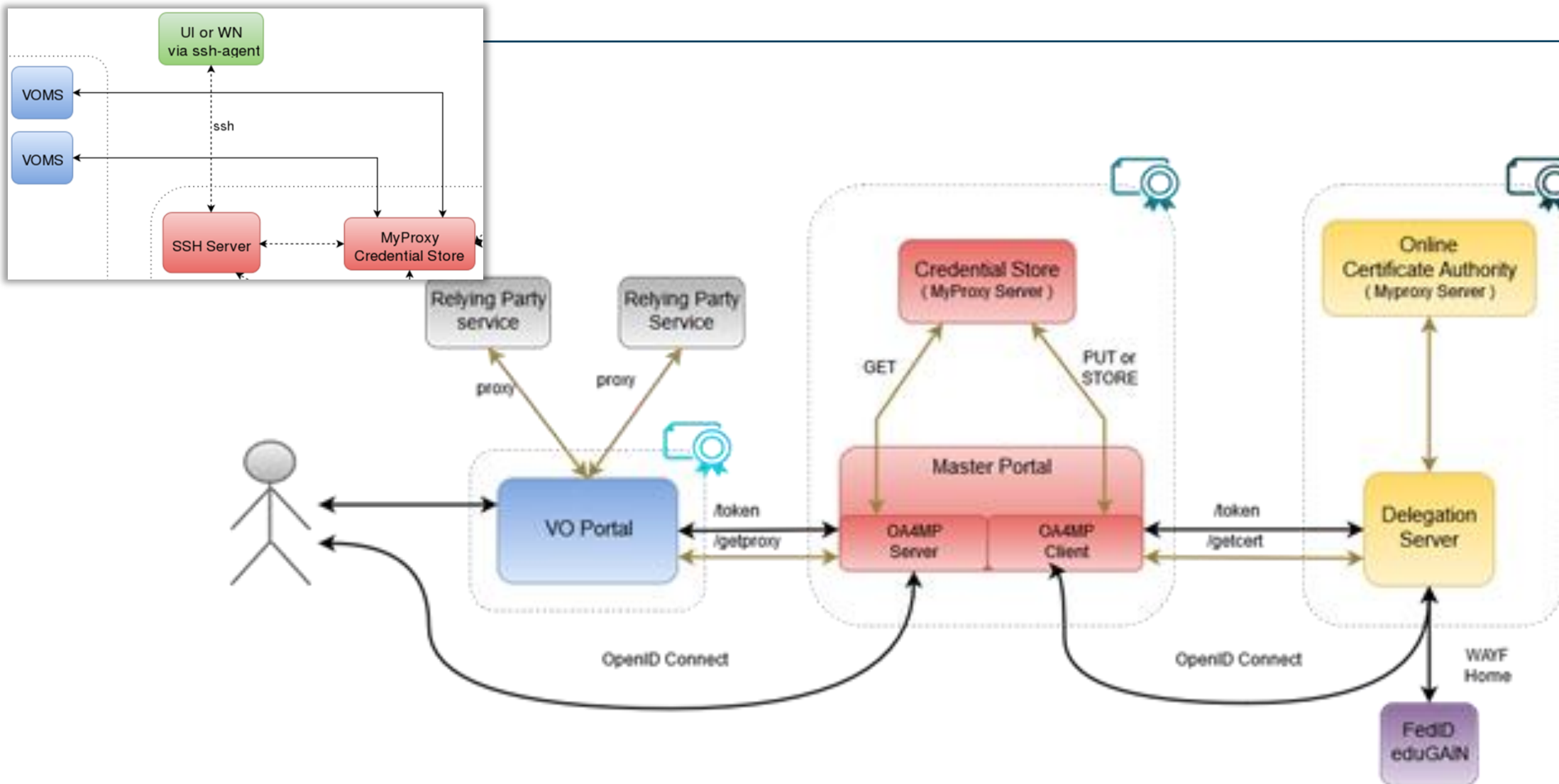
End-user credential hiding in the AARC CILogon-like Pilot

- Do **not assume any changes** in the IdPs: no ECP, no new policies, no nothing (reality, sorry!)
- Assume no major changes in the e-Infrastructures: interfaces remain a mix of Web and PKIX, policies remain mostly as-is
- Should show results ‘fairly soon’ (concrete demos and integration that works quickly)
- Leverage existing CILogon and MyProxy, thanks to the collaboration of AARC-CTSC/MyProxy

Beyond CILogon

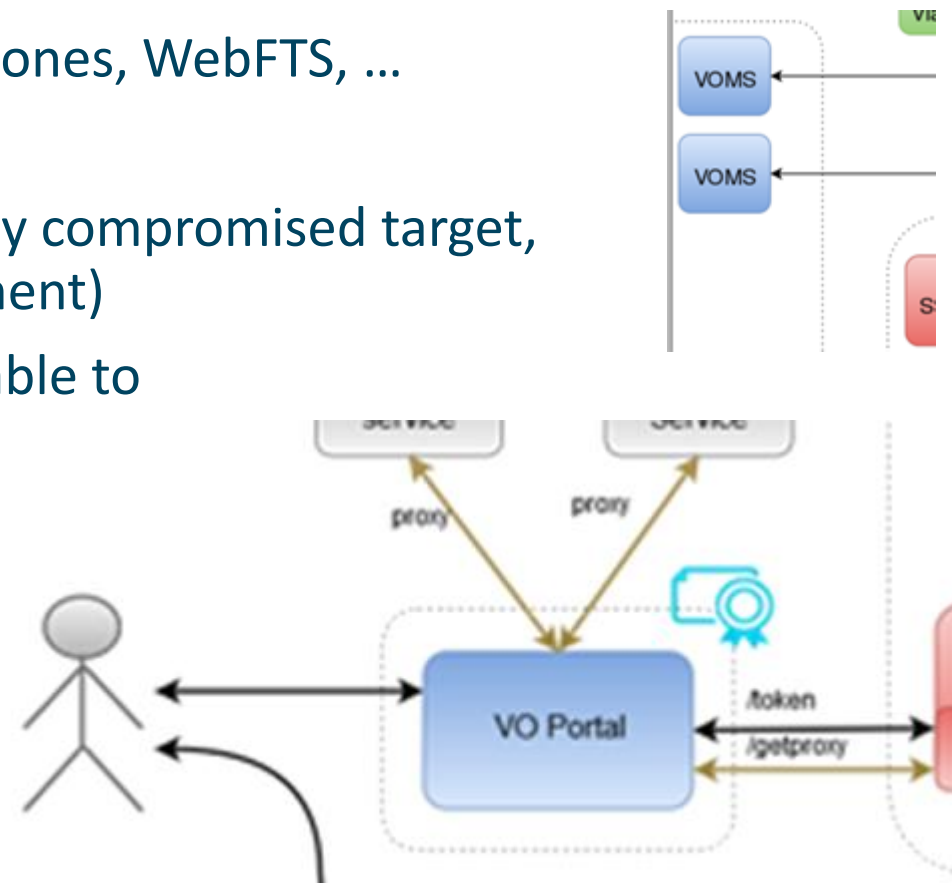
- CILogon assumes the e-Infrastructures (CIs) build the portals and interfaces
- CILogon assumes that users in the end might retrieve certificates explicitly
- Larger RIs and e-Infra in Europe could do it, but not the large number of small communities
- So the AARC Pilots adds additional control elements: credential management, light-weight portal interfacing, (VOMS) attribute management, *optional: opaque credential retrieval*

CILogon-like TTS Pilot - distributable elements



Blue: VO services and resources

- Are around today, either self-managed or hosted, in most communities
- Science gateways, portals, e.g. HADDOCK, Galaxy, generic ones, WebFTS, ...
- Omnipresent (and has unfortunately proven to be an easily compromised target, especially when end-user instantiated in a cloud environment)
- Will have to get credentials from the MPs, but should be able to do so only for authenticated users
- Downtime will impact its' own users, but there will be many of these (same service by different sites?)
- *VO management* impact high (VOMS but usually hosted)



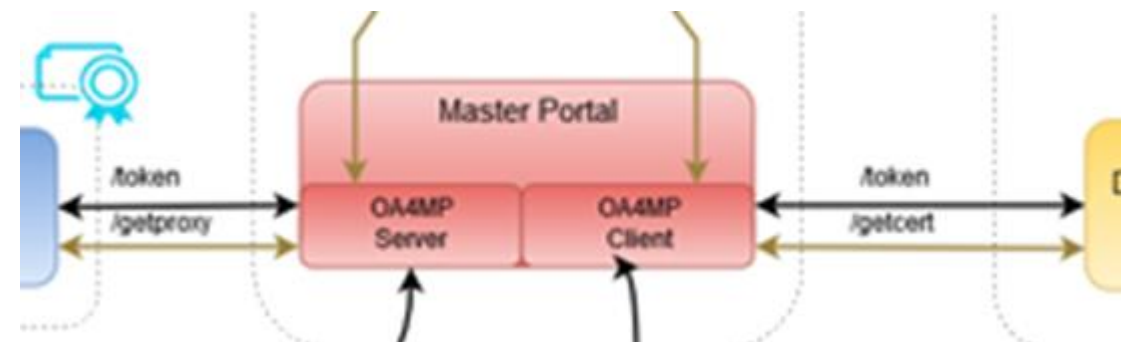
Considerations:

Ease of deployment, trust by MPs and end-users, usability, containment of incidents

Red: the Master Portal (MP) and Credential Repository

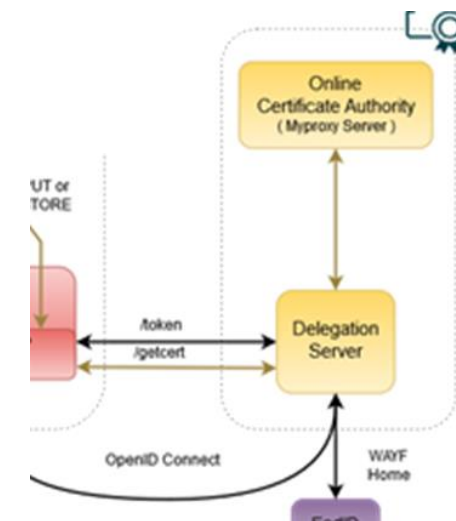
- Needs to be a trusted element (to permit credential storage by the TTS)
- Requires some operational and security expertise (managed data centre, locked racks, access controls, ability to designate infrastructure for security operations, trained staff)
- Connects to (many) workflow-specific VO portals
- Connects to a (single, we hope!) Delegation Service/TTS-CA
- The credential repository is a highly valuable resource for attackers
- Similarly, a downtime of the MP/Credential Repo disables resource access for connected VO portals – so it can (and usually will) be a SPoF

Considerations:
scalability, A/R, trust by the VO portals



Yellow: the Token Translator/OA4MP/CA service

- Is a highly trusted element: security and policy expertise, ability to maintain accreditation
 - Needs operational and technical capabilities: hardware security modules, managed data centres, off-line and on-line secure areas, ROBAB-proof trained personnel, ability to designate infrastructure for security operations
 - Connects to (a few, we hope) Master Portals (MPs)
 - Connects (many, we hope scalably) federations, IdPs and (few) SP-IdP-Proxies
 - *May have to present a WAYF, if the VO portal does not pass IdP entityID*
 - Deal with heterogeneity in global federations (uniqueID, heuristics, &c &c &c)
-
- Needs to be a trusted element for Relying Parties (resource owners), users, and federations
 - Becomes extremely valuable target for attackers, and
downtime impacts all connected MPs, and (with delay) impact all VO portals anywhere



Considerations:

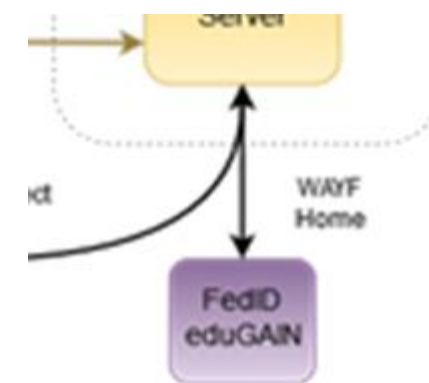
trust, recoverability, A/R, compliance, need to conclude specific agreements with MPs

Purple: connected federations and IdPs (proxies)

- In the generic case (conventional R&E federations) limited control possible
- RI/eI proxy IdPs will provide more specific capabilities (uniqueness, user management ability)
- Connects to many services, of which the DS/TTS is just one
- Build on common technology (keep with SAML, no OIDC here)
- Shared policy compliance: REFEDS R&S, Sirtfi
- Negotiate non-scaleably only when needed (but a TTS must serve all users to prevent fragmentation!)
- Cope with heterogeneity (i.e.: use a ‘filtering WAYF/entity filter proxy’)

Considerations:

Trust, scalability, non-intrusiveness, service-specific filtering

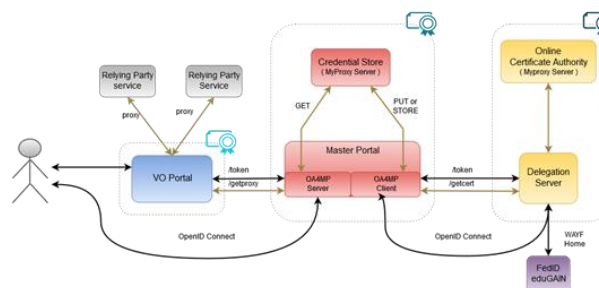


Some appeal?

Pilot appears to be appealing to RIs and e-Infrastructures

- ELIXIR instance (demo) managed under SA1 on CESNET resources for EBI
- EGI AAI (that's why we are here at the AAI TCB):
initiated under ENGAGE JRA1 on GRNET resources for EGI
- Continuing discussions on alignment with WLCG ... (but who already have a setup anyway ;-)

Effect: expressions on interest received to host 'the service' (various elements) from many



With EGI being the most concrete by including support for it in the planned core activities

Where are we now?

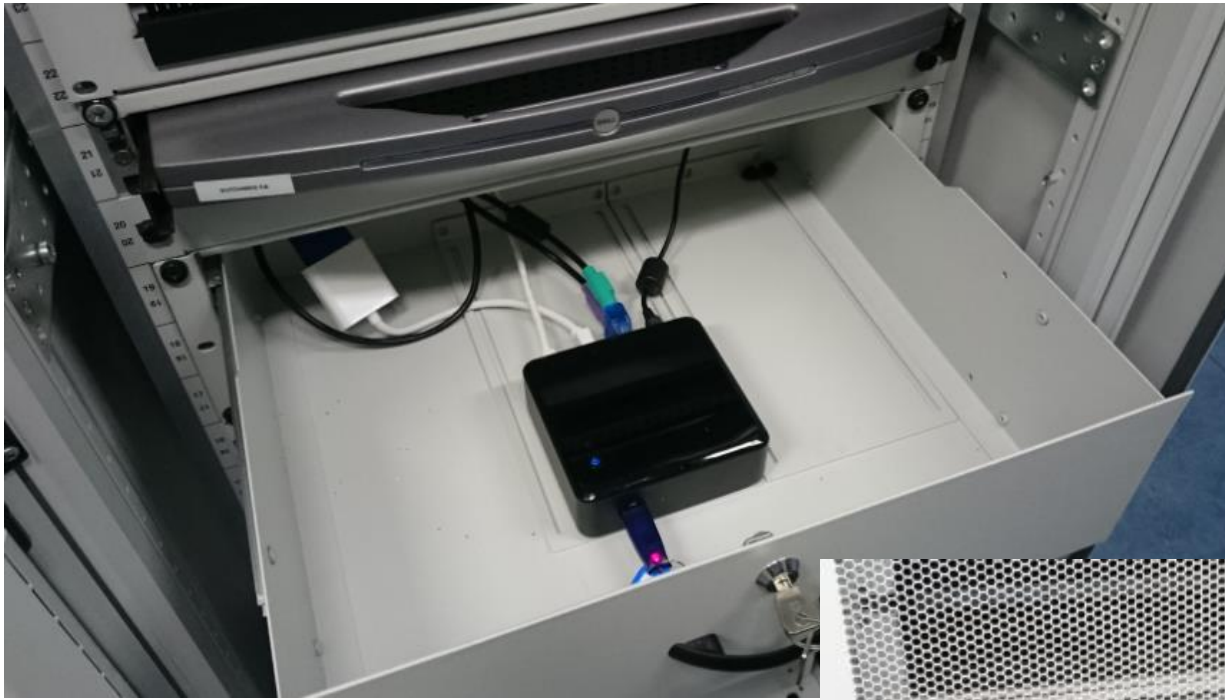
- Several instances deployed, for EGI and ELIXIR (usually co-managed by Nikhef)
- Accredited ‘production demonstrator’ instance of the TTS set up in conceptually the ‘right way’:
 - Dedicated servers, secure environment, FIPS 140 level 3 approved HSM, anchored in a stable way
 - Policy and practices accredited (under the ‘unique-identifier-only’ DOGWOOD profile) at the IGTF
 - is good enough for some infrastructures, and expected to be enough in EGI combined with managed communities
 - Scalable negotiation model based on Sirtfi and REFEDS R&S section 6
 - Model requirements on attached MPs defined (for key protection)
 - Trust anchors in production (RCauth.eu and its “DCAROOT” HLCA)
- Includes also the policy-filtering ‘proxy-WAYF’ to link to eduGAIN & individual authentication sources



But it’s a production demonstrator, *not ensured* production, so *without* an SLA, with limited capacity

- ... and it’s a bit of a ‘Heath Robinson’ service, using mostly pre-available hardware

Pretty pictures



Physical controls are quite OK 😊

- Located at Nikhef, Amsterdam, NL
- Nikhef-specific part of the DC Housing Facilities
- Room capacity 400kW, total ~ 2MW, 2N+ no-break
- ID based access control, 24hr guard on-site, 2nd floor (above sea-level)
- CA and security systems in locked dedicated cabinet. On-line CA signing system in locked drawer



RCauth  .eu

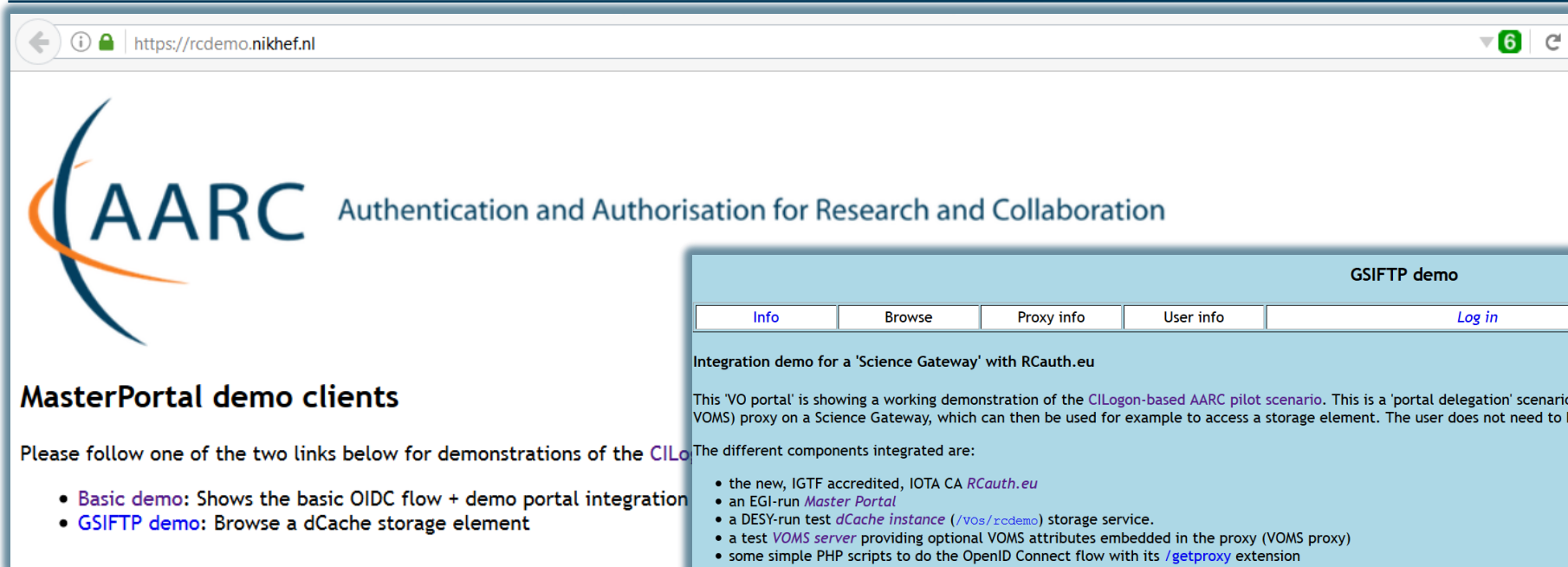
CA signing system




Delegation Server



https://rcdemo.nikhef.nl/ -- with optional IdP hint for Infrastructures ...




AARC Authentication and Authorisation for Research and Collaboration

MasterPortal demo clients

Please follow one of the two links below for demonstrations of the CILogon-based AARC pilot scenario.

- **Basic demo:** Shows the basic OIDC flow + demo portal integration
- **GSIFTP demo:** Browse a dCache storage element

GSIFTP demo

Info	Browse	Proxy info	User info	Log in	Log in with VOMS
----------------------	------------------------	----------------------------	---------------------------	------------------------	----------------------------------

Integration demo for a 'Science Gateway' with RCauth.eu

This 'VO portal' is showing a working demonstration of the CILogon-based AARC pilot scenario. This is a 'portal delegation' scenario, where the user uses federated credentials to leave a personal (optionally VOMS) proxy on a Science Gateway, which can then be used for example to access a storage element. The user does not need to know anything about the underlying PKI infrastructure.

The different components integrated are:

- the new, IGTF accredited, IOTA CA [RCauth.eu](#)
- an EGI-run [Master Portal](#)
- a DESY-run test [dCache instance \(/vos/rcdemo\)](#) storage service.
- a test [VOMS server](#) providing optional VOMS attributes embedded in the proxy (VOMS proxy)
- some simple PHP scripts to do the OpenID Connect flow with its [/getproxy](#) extension

Some notes:




MasterPortal is completely agnostic concerning the VOMS server. The requested VO plus the corresponding necessary 'vomses' string is passed in via the client, and goes transparently through the proxy.

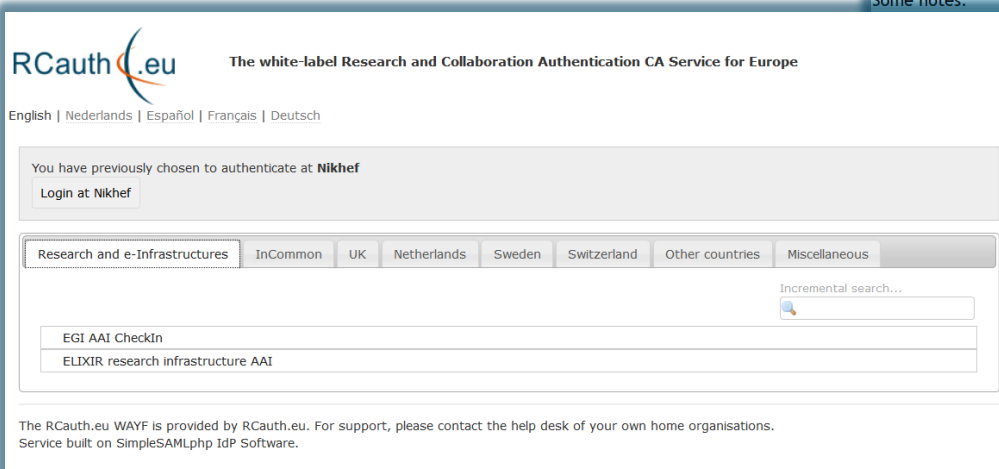
The test instance is completely wiped everyday, so do NOT rely on it for permanent storage (-); to access the storage element, the user needs to be authorized for accessing (either on identity or VOMS attributes). This provisioning is *not* part of the current demonstrator. The user needs to be enrolled in the VO. How to (semi-)automate this provisioning is currently under investigation within AARC.

Use either the [login](#) or [login with VOMS](#) tabs above to do a federated login and obtain a valid plain or VOMSified proxy.

Once logged in, you can [browse](#) the storage element.

The [user info](#) tabs show information about the underlying X.509 credential and the OpenID-Connect claims respectively.



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](#)


[Research and e-Infrastructures](#) | [InCommon](#) | [UK](#) | [Netherlands](#) | [Sweden](#) | [Switzerland](#) | [Other countries](#) | [Miscellaneous](#)

Incremental search...

[EGE AAI Checkin](#)
[ELIXIR research infrastructure AAI](#)

The RCauth.eu WAYF is provided by RCauth.eu. For support, please contact the help desk of your own home organisations. Service built on SimpleSAMLphp IDP Software.

The Master Portal – necessary consent ...



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

RCauth.eu Online CA consent page

The Master Portal below is requesting access to your person

If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and For further information on the CA see the [RCauth.eu homepage](#)

Remember

Master Portal Information:

Name: EGI Master Portal
Description: EGI Master Portal
URL: <https://masterportal-pilot.aai.egi.eu>

Information that will be sent to the Master Portal:

sub : davidg@nikhef.nl
idp : <https://sso.nikhef.nl/sso/saml2/idp/metadata.php>
eduPersonTargetedID : <https://sso.nikhef.nl/sso/saml2/idp/metadata.php!3960c9bec163785afd515c33>
idp_display_name : Nikhef
cert_subject_dn : CN=David Groep QK-DHKZMTHoVTtT6,O=nikhef.nl,DC=rcauth-clients,DC=rcauth-clients
name : David Groep
eduPersonPrincipalName : davidg@nikhef.nl
given_name : David
family_name : Groep
email : davidg@nikhef.nl

Info
Browse
Proxy info
User info
Logged in as *davidg@nikhef.nl*

Download

You can [download](#) your proxy

Proxy information:

```

subject      : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHKZMTHoVTtT6/CN=1257956691/CN=778492964
issuer       : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHKZMTHoVTtT6/CN=1257956691
identity     : /DC=eu/DC=rcauth/DC=rcauth-clients/O=nikhef.nl/CN=David Groep QK-DHKZMTHoVTtT6/CN=1257956691
type         : RFC compliant proxy
strength     : 2048 bits
path         : /tmp/x509up_uVIDWxT
timeleft    : 11:59:44
key usage    : Digital Signature, Key Encipherment, Data Encipherment
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 778492964 (0x2e66dc24)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC=eu, DC=rcauth, DC=rcauth-clients, O=nikhef.nl, CN=David Groep QK-DHKZMTHoVTtT6, CN=1257956691
    Validity
      Not Before: Feb  7 11:49:11 2017 GMT
      Not After : Feb  7 23:54:11 2017 GMT
    Subject: DC=eu, DC=rcauth, DC=rcauth-clients, O=nikhef.nl, CN=David Groep QK-DHKZMTHoVTtT6, CN=1257956691, CN=778492964
    Subject Public Key Info:
          
```

The Most Transient VO Portal in the World (the expedited data life cycle :-)



GSIFTP demo




Info Browse Proxy info User info Logged in as *davidg@nikhef.nl*

gsiftp://prometheus.desy.de: /

○ d-----	1	davidg	davidg	512	Feb 7 06:00	lost+found
○ dr-x-----	1	davidg	davidg	512	Feb 7 06:01	VOs
○ dr-x-----	1	davidg	davidg	512	Feb 7 06:01	Users
○ dr-x-----	1	davidg	davidg	512	Feb 7 06:02	UTF-8
○ dr-x-----	1	davidg	davidg	512	Feb 7 06:03	Music
○ dr-x-----	1	davidg	davidg	512	Feb 7 06:04	Video
○ d--x-----	1	davidg	davidg	512	Feb 7 11:21	upload

Delete selected entry No file selected.

Remote name:

<https://wiki.geant.org/display/AARC/Models+for+the+CILogon-like+TTS+Pilot>

Sustainability models for the future: functional decomposition

Deployment and (financial) sustainability models

VO portals

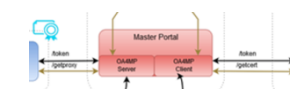
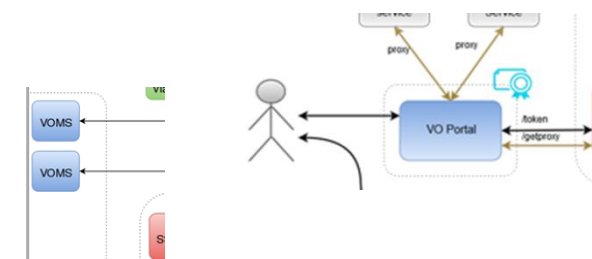
- High volatility of services and platforms – best left to user groups and (sub) communities
- Light-weight linkage – technically OIDC, with need to connect explicitly with an MP (MP will distribute user credentials, and has some responsibility for trust) – frequent communications between VO portal and MP operators foreseen

- Suggest to keep with users and (sub) communities

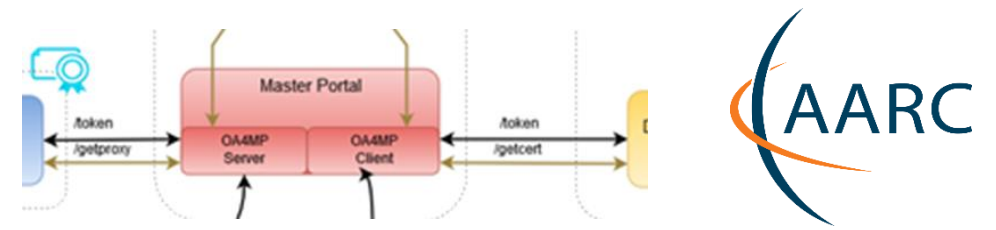
VO membership services: assume unchanged from today

Master Portal & Credential Store (plus CLI token acquisition)

- More costly: runs specific glue software (maintenance cost), needs to have some secure infra
- Needs to gain trust from users (for which it manages credentials), VO portals, and the TTS ICA
- Some distribution options – but it needs professional hosting and management



MP operating options



- At home institutions and research labs
 - Easy to gain user trust: they ‘know’ the operator. With a small per-institutional user base not likely to get traction
 - As soon as use of the service extends to VO portals outside the home org, branding (and trust) conflicts emerge
- At generic e-Infrastructures (EGI, EUDAT, GEANT, ...)
 - Close to relying parties, so easier to gain trust, and connected to managed data centres that do secure hosting
 - Pretty remote from the typical researchers, so unlikely to ‘know’ the many connecting VO portals
 - VO portal builders/operators may not easily find a ‘generic e-Infra’ that is beyond their research domain
 - Yet may work well for largish VOs, and for VOs whose management service is already outsourced to centres that are closely linked to a generic e-Infrastructure
- At the (ESFRI) Research Infrastructures (like ELIXIR, ...)
 - Usually have a good IT (and trust) capability
 - Are logically close to the VO portals and may feel ‘dutybound’ to support community portals in their research domain
 - Are few enough in number so that the negotiation with a (single) back-end TTS ICA remains feasible
- Outsourcing this as “SAAS” by the RIS
 - can work – but outsourcing the management of connecting VO portals defeats the purpose – and needs a multi-tenant MP management implementation

Scale is important: if master portal is down, dependent VO portals may not work. Scope (#users), available service agreements, and (implicit) expectations may drive relationship between end-users (portals) and the MP operators.

DS/TTS back-end ICA options



Delegation service (with the ‘filtering proxy WAYF’) and the ICA are a joint trust enclave

- Must jointly be run under the same policy management controls
- Maintains the ultimate trust link to the generic relying parties (through IGTF accreditation)
- Visible to end-user since user must knowingly permit transfer of the tokens to the MP store
- May also become visible to the user if it has to present a WAYF
- Has to establish relationships with the MPs and the upstream IdPs/federations
- WAYF redirection may be primary factor to decide between single or multiple instances:

widest possible user base – and not steering user away from her or his only working IdP

DS/TTS back-end ICA options (I)



- At 'natural home' organisation of the user or of the VO operator: *not feasible trust-wise*
- At the generic e-Infrastructures (EGI, EUDAT, GEANT, ...)
 - They will have participating centres that can do secure hosting, and operational link eases trust
 - May be unlikely to agree on a single one, so the WAYF problem emerges and creates silo's
 - Potential for 'lock-in' between the TTS and specific relying parties only within same infrastructure ... if global accreditation is bypassed in favour of instantaneous easy satisfaction
 - Cost may be prohibitive for even some of these entities, but they all have cost recuperation systems in place
- At the (ESFRI) Research Infrastructures (like ELIXIR, ...)
 - The RIs also have access to capable participating hosting centres and could do it (or outsource it!)
 - Same issue in creating silos, easy rapid bypasses, and lock-in
 - There are even more RIs than there are generic e-Infras: scalability issues emerge stronger
 - Smaller user base makes for higher per-user costs, but operational need may make it easier to bear
- A single one for Europe
- A single one for the world: *great!*

DS/TTS back-end ICA options (II)



- At the generic e-Infrastructures (EGI, EUDAT, GEANT, ...)
- At the (ESFRI) Research Infrastructures (like ELIXIR, ...)
- A single one for Europe
 - prevents silos and does away with any fronting-WAYF issues
 - but the fact that it needs to ask user to trust the master portal leads to branding questions ☹️
 - cost per user is lower due to scale, so recuperation could be easier – yet it has to be independent and thus has to hunt for funding through either fees (per user, per MP, per authentication?) or through contracts with e-Infra s or RIs
 - lack of clear ‘ownership’ leaves it vulnerable to vendor longevity – too few subscribers give spiraling costs
 - can maybe go through joint procurement (e.g. TCS has option for ‘enterprise-specific TA’ hosting)
 - each e-Infra wants to be the exclusive provider of the back-end IdP, to provide *the* uniqueID
 - and certainly not allow the user to ‘escape out’ of the e-Infra/RI silo (can be done with entityID forwarding)
- A single one for the world: *great!*
 - *but:* legal issues in DP from the EU
 - needs extremely high reliability, and probably regional distribution anyway for acceptable latency and 24x7 support

Costing the services

Highly depends!

- what is 'the service'? Delegation Service & WAYF? Master Portals?
- technical elements only, or operational service implementation?
- desired service level (support & availability)
- extent of the service (number of users, communities, ...)

Recuperation model very much a business decision as well:

- can be anywhere between few kEur to well over 100+kEur cost per year (for >3year service)
- EGI plans foreseen (co) support of the Delegation Service, CA back-end, and integration of (at least one) Master Portal
- Collaboration working towards a single one for Europe is part of the plan
this necessitates a closely coordinated management authority for the Delegation Service/CA

Current State

- Pilot working with the Research and e-Infrastructures supported through AARC SA1
- Nikhef (and the Dutch National e-Infrastructure coordinated by SURF) run the operations today
- Will continue to operate central parts (CA, DS) for as long as relevant, but *without any capacity increase and at the current SLA (“Nikhef Best Effort”)*
- We surely hope that a long-term sustainability model in place by end of 2017
- That inclusively satisfies the pan-European e-Infrastructures and Research Infrastructures
- EGI planning is well aligned with these wishes 😊

References

<https://rcauth.eu/>

<https://wiki.geant.org/display/AARC/Models+for+the+CILogon-like+TTS+Pilot>

Thank you

Any Questions?

davidg@nikhef.nl



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).