Authentication and Authorisation for Research and Collaboration

Evolving the trust fabric with AARC and EGI

The AARC CILogon pilot and redistributed responsibility

David Groep
AARC NA3 Activity Lead
Nikhef, Physics Data Processing Group

EGICSIRT F2F Prague meeting
29 January 2016

Incorporating element from
EGI-ENGAGE funded under SA1 and JRA1

You all remember the bad old days …

NIKHEF

NATIONAAL INSTITUUT VOOR KERNFYSICA EN HOGE-ENERGIEFYSICA

Guest / students form (pleas

1. This form is completed in connection with:

☐ work experien

☐ otherwise, viz

CERN/User Registration

CERN COMPUTER CENTRE - US

http://cern.ch/it/documents/ComputerUsage/CompA

To be returned to the User Registration box at the en
completed by a user who requires a computer accou
Department, and is not yet registered in another grou

To be completed by the User :

It is **MANDATORY** to provide the following infor
treated confidentially and only be used for ensuring
Supply name as registered by the Users' Off

FAMILY NAME(S): .....

FIRST NAME(S) : .....

SEX [M] [F] BIRTHDATE: Day ..... Month ..... Year .....

HOME INSTITUTE/FIRM: .....

NATIONALITY: .....*CERN SUPERVISOR.....

*CERN DEPARTMENT: . . . . . *CERN ID NUMBER (as on CERN card).....

To be completed by the Group Administrator:

Fermilab

For Office Use Only

ID:	**Action:**	**ID Exp:**	
Insurance:	**Medical:**	**Safety:**	
Computer:	**Stkrm:**	**Family:**	
NON-473:	**Sensitive:**	**Verifier:**	**Date:**

Name:

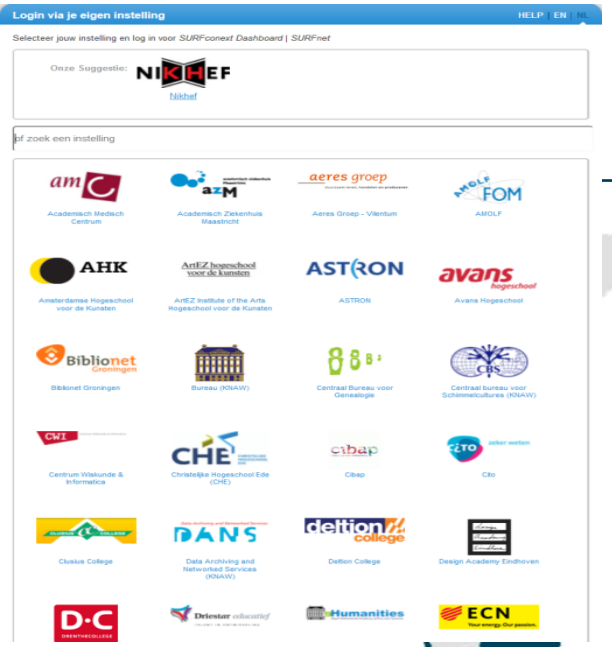
SWIETZER	JOHN	JAMES
Last	First	Middle

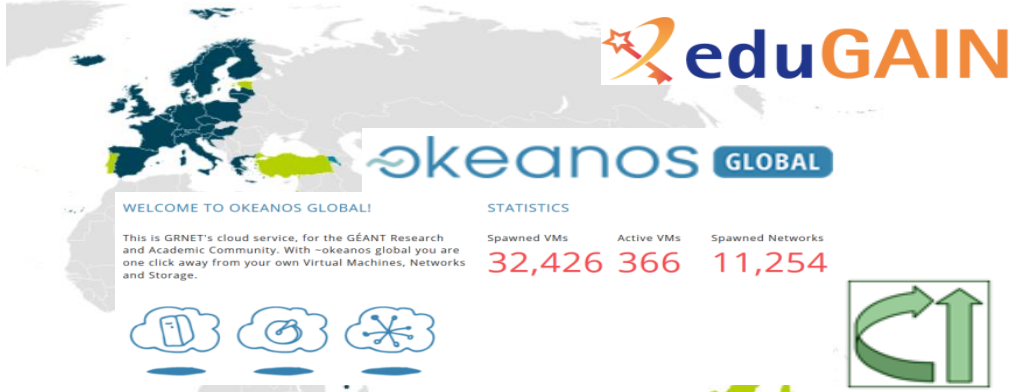
University or Institution Name:	Telephone:
FLORIDA STATE UNIVERSITY	850-644-XXXX

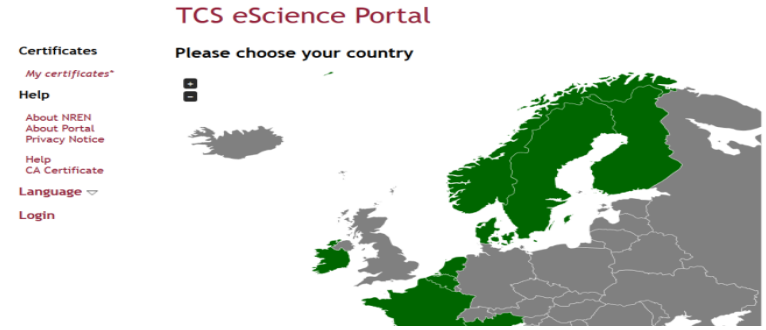
Experiment/Department:

Exp. / Dept.	Spokesperson	Home Institution Contact	Contact Telephone
D0	WOMERSLEY/WEERTS	SHARON HAGOPIAN	850-644-4777

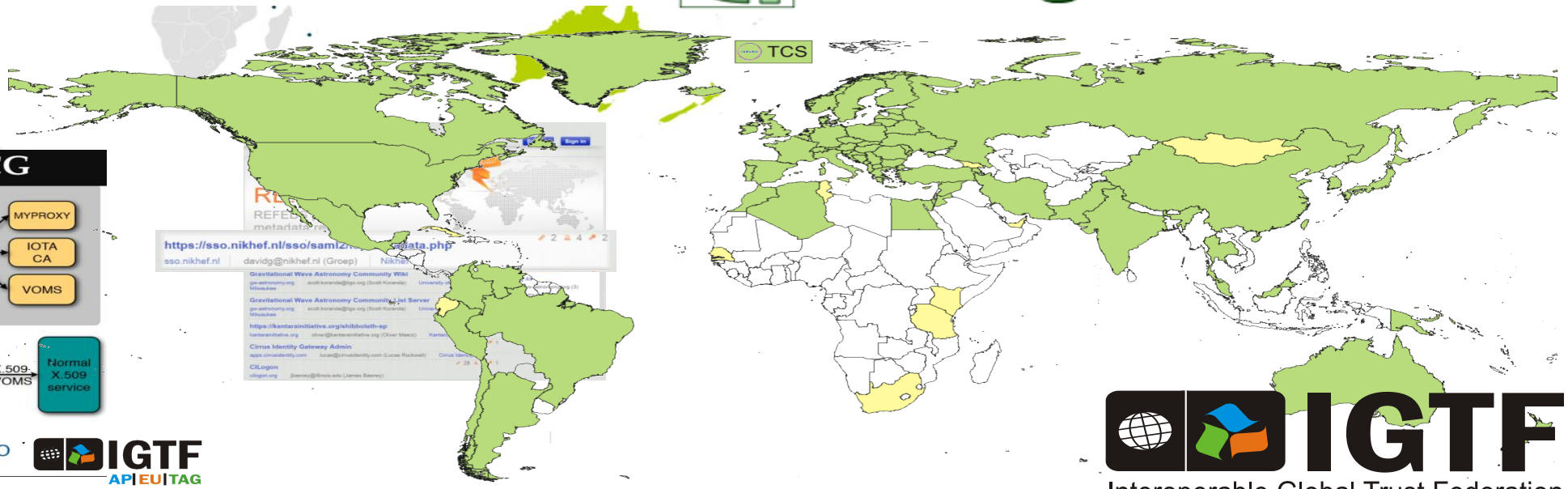
And now we have this!



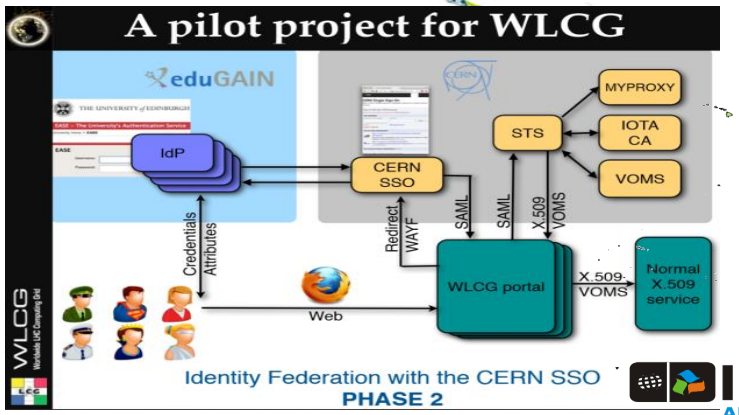




CILogon Service



wLCG FIM4R pilot



IGTF
Interoperable Global Trust Federation
AP | EU | TAG

background: eduGAIN connected federations as of November 2014 – Brooke Schofield, TERENA

AARC Vision and Objectives – link to EGI

Improve federated access by addressing current challenges

Integrate existing R&E AAIs to create a highway for identities

Avoid the creation of project-specific AAIs by enabling researchers to use their existing credentials to access different resources

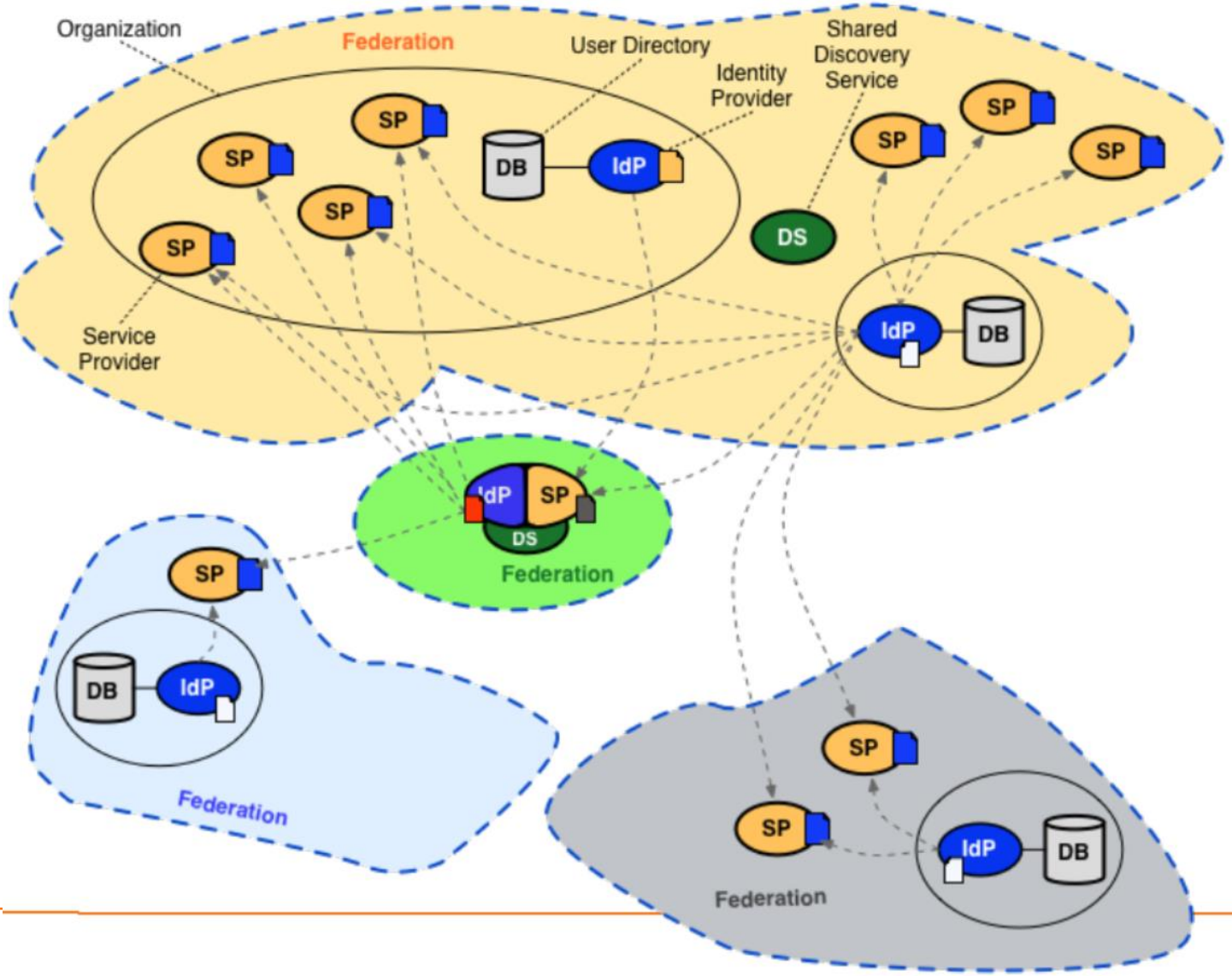
Harmonise policies among e-Infrastructures to ease service delivery

Define a training package for institutions and services to support federated access

EGI JRA1 and CCs

Other RIs and e-Infra

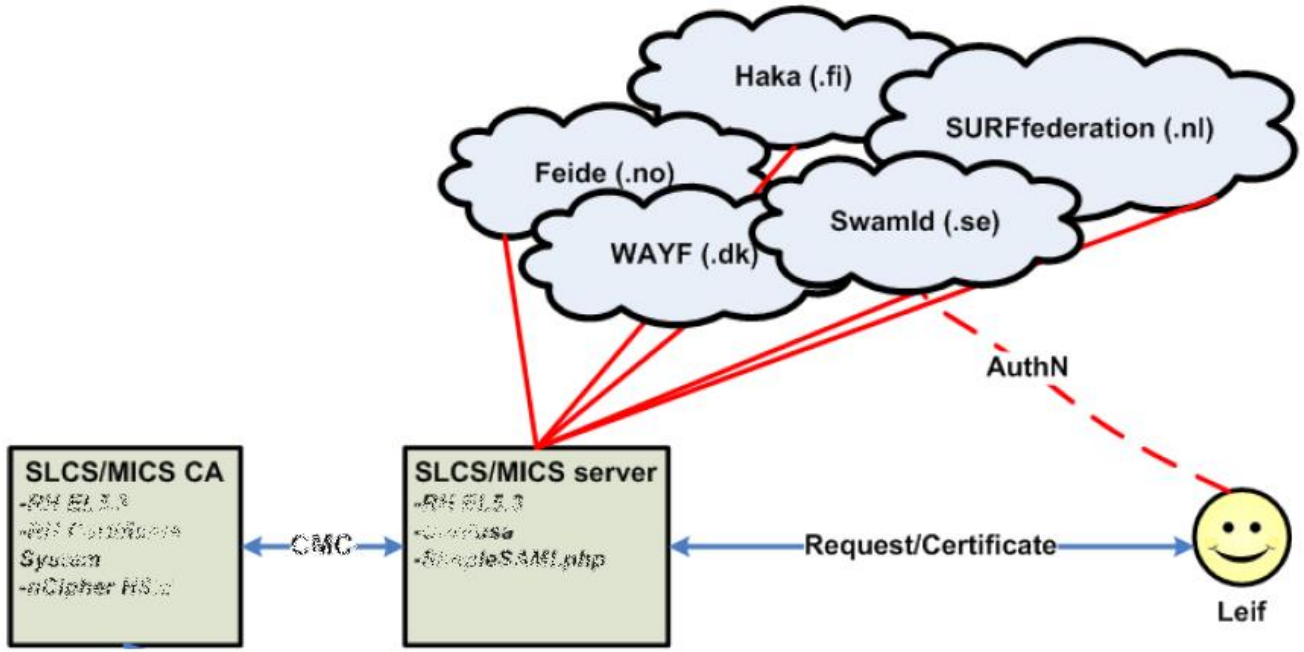
Conventional R&E federations (web-only, selected services only)



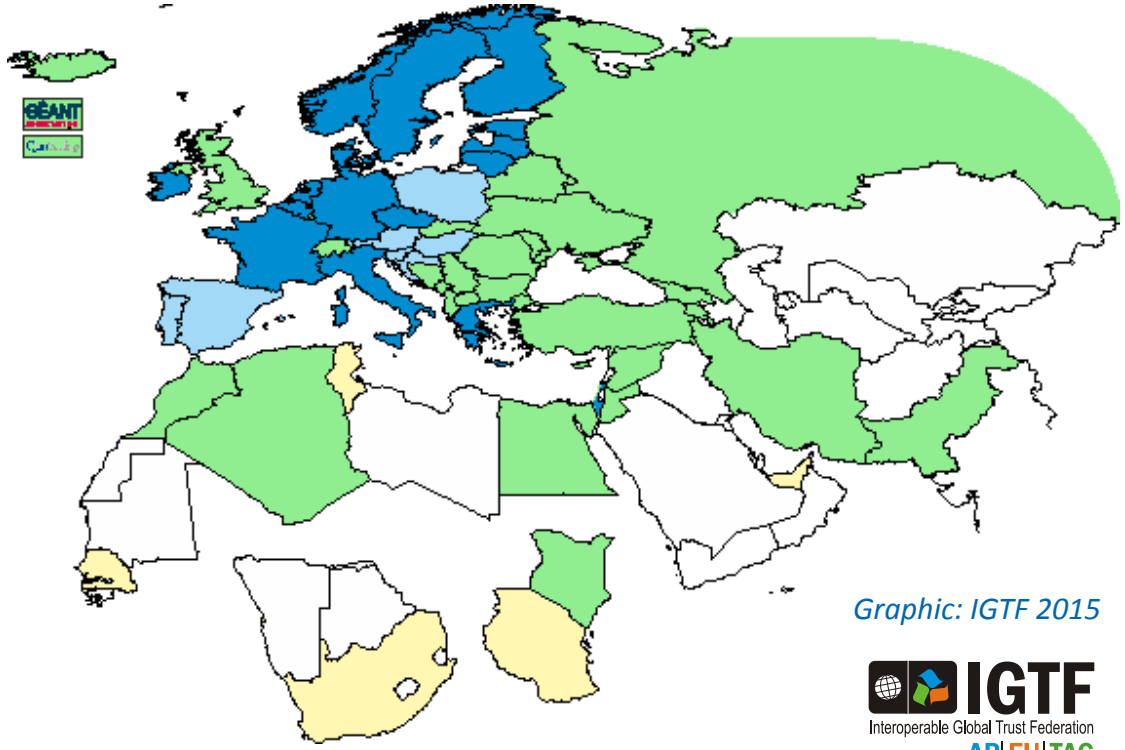
Leveraging R&E federations: TCS, DFN SLCS, CILogon … - with extended LoA

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**

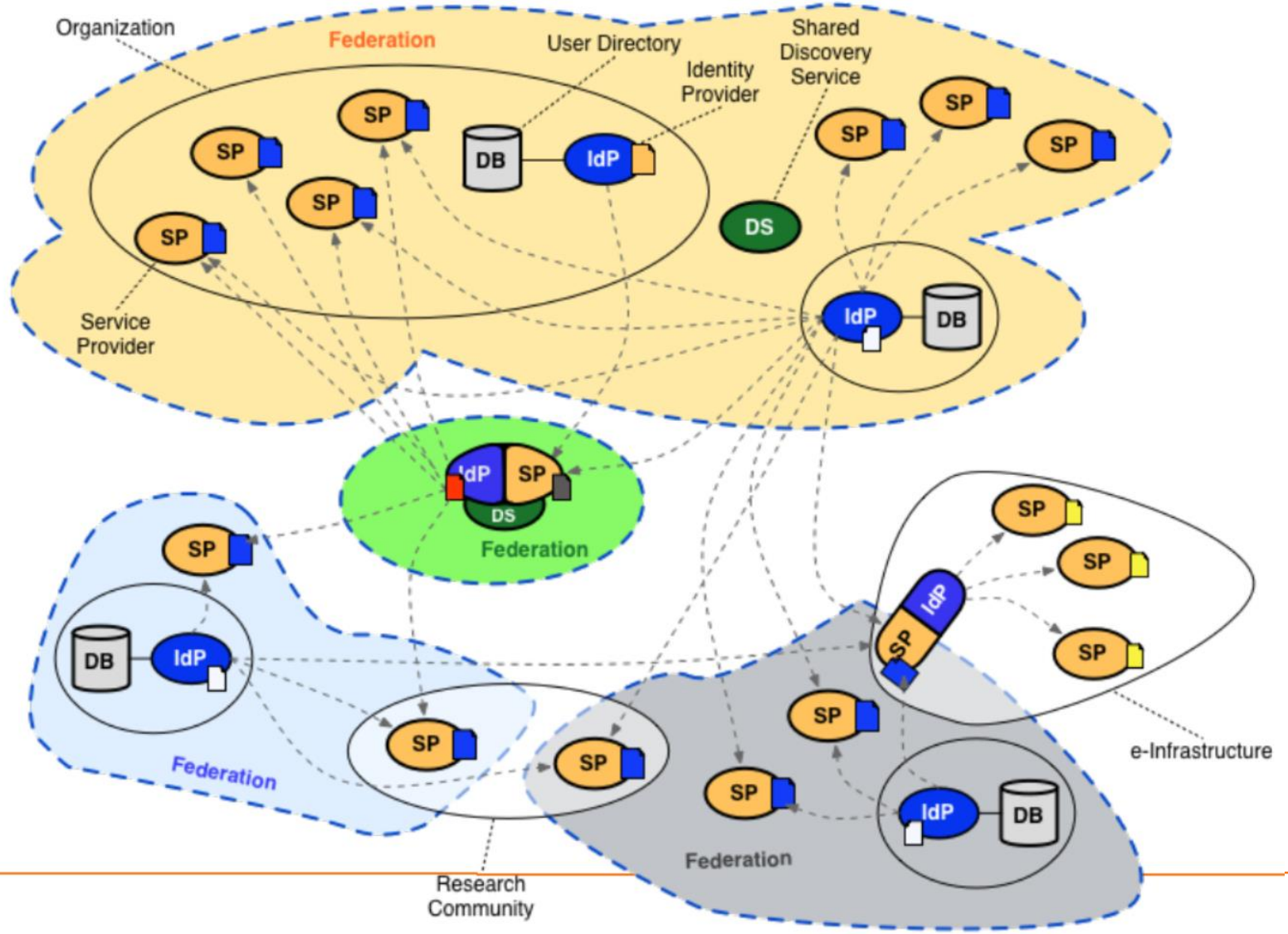


Graphic from: Jan Meijer, UNINETT



Graphic: IGTF 2015

Complex and composite federations space – integrating RIs and e-Infra



- Technical bridging
- Federation LoA challenges
- Distributed responsibilities in EGI with WLCG VOs

- Bridging services
- CILogon in Europe
- Science Gateways and Credential Management
- Full credentials, proxies, or Robots with '*PUSP*'?
- Towards non-Web SSO

- Eligibility of federated IDs
- SirTFi trust framework

- *What have we missed?*

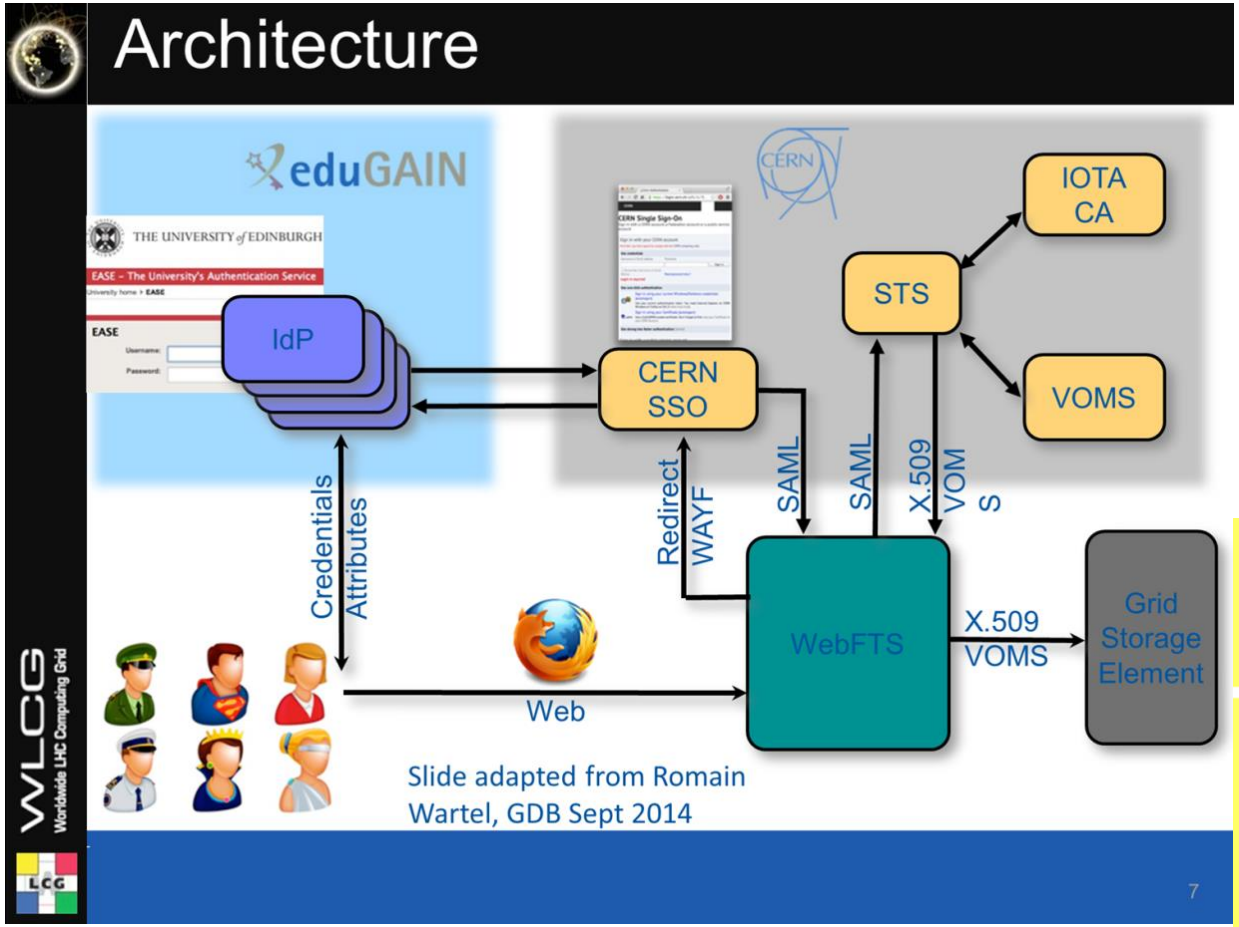
AARC Pilots and the EGI AAI evolution

- Most infrastructures move to completely hiding PKIX from the end-user
  - “we’ve found all people in the world who understand PKI” (and they by now all got a certificate ;-)
  - EEPKI + RFC3820 proxies **do 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

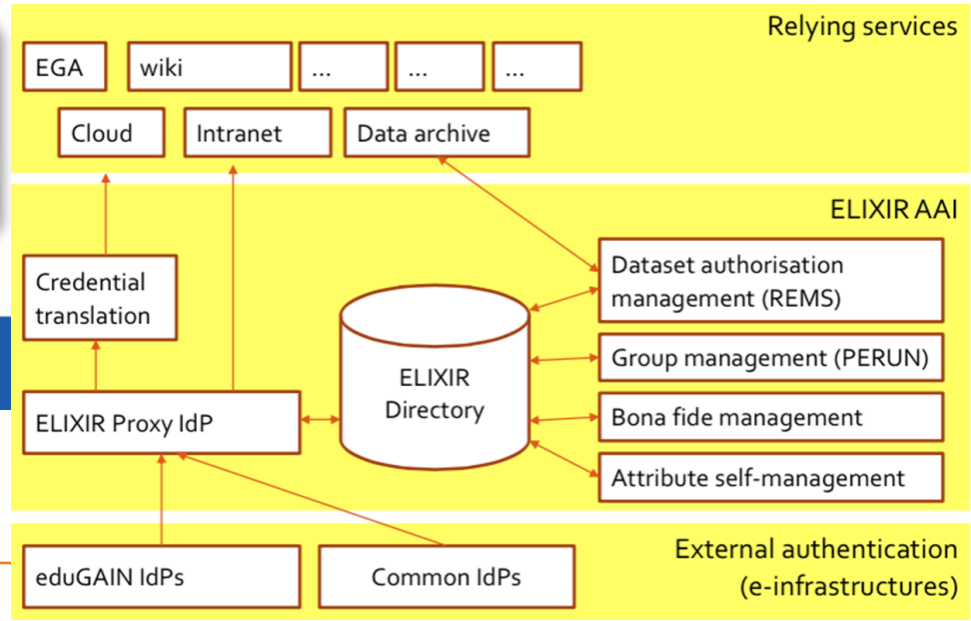
- Emerging as a pattern in many Research Infrastructures that use CLI or brokerage
  - ELIXIR, UMBRELLA, WLCG, INDIGO DC
  - SAML->OIDC, SAML->X509, X509->OIDC, X509->SAML, OIDC->X509, …

Just R&E federation is not enough for RIs and e-Infrastrucutures



WebFTS 'FIM4R' in wLCG
Romain Wartel

ELIXIR reference architecture
Mikael Linden et al.



Background: WebFTS

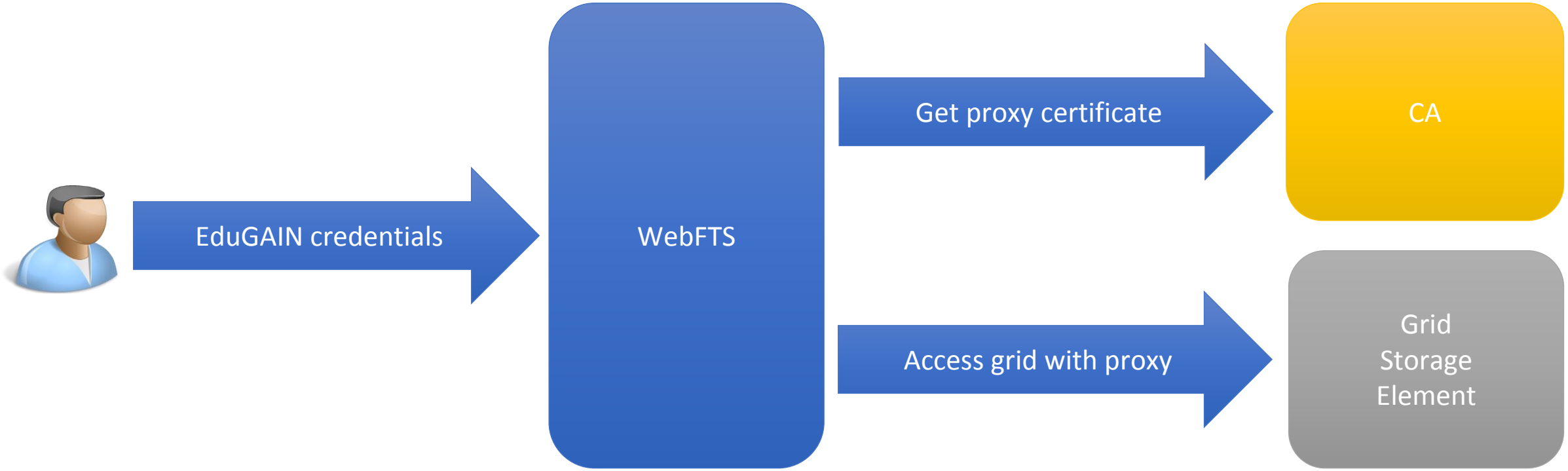
Web based tool to transfer files between grid/cloud storages

- Protocols: gsiftp, https, xrootd and srm
- Cloud extensions: dropbox, CERNBox

Based on FTS3

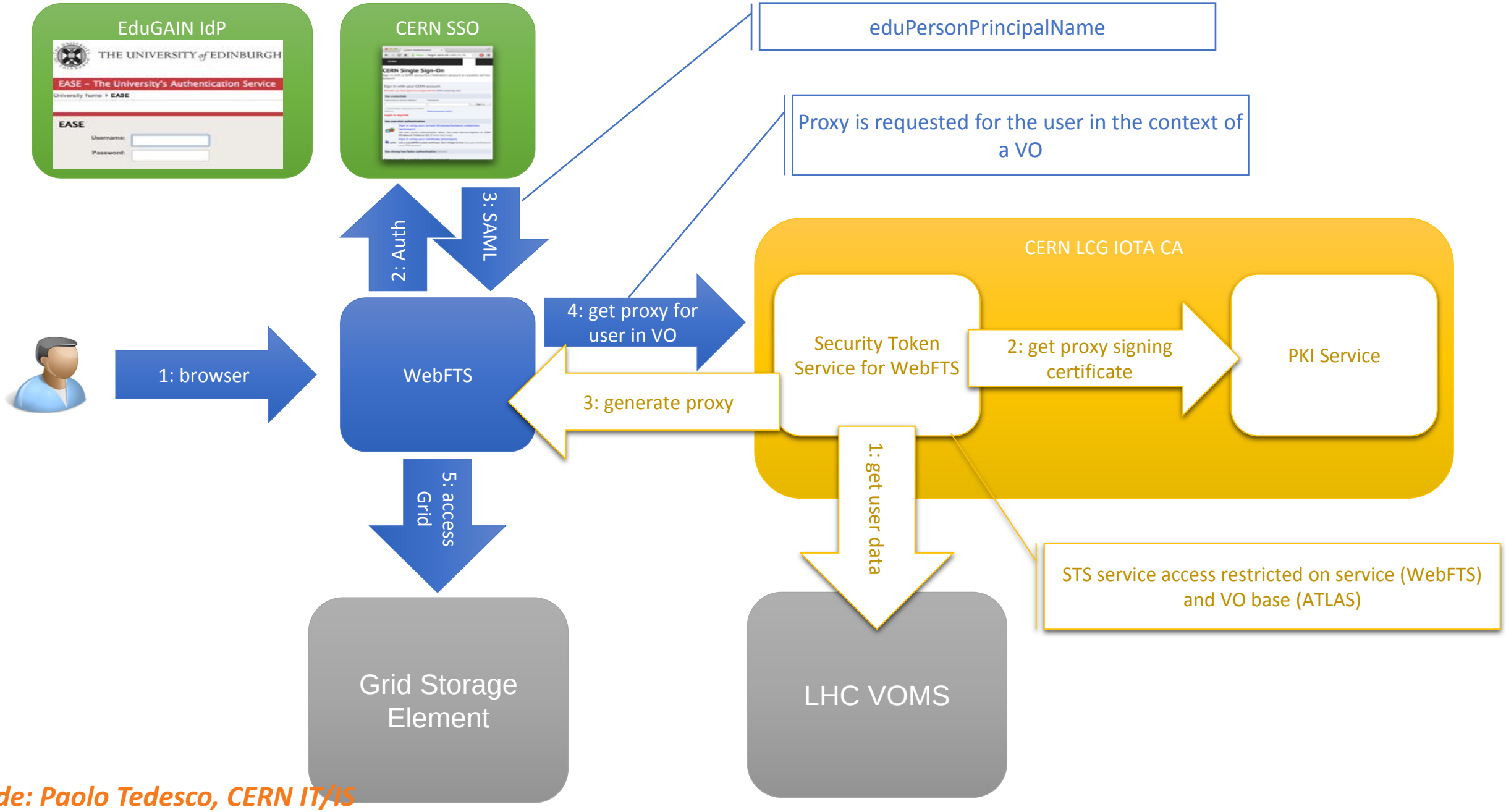
- Low-level data movement service
- Moves LHC data across WLCG infrastructure
- Allows participating sites to control usage of network resources
- 20PB per month (max: 2PB/day) transfer volume

Current prototype



Current working prototype based on “internal” CA

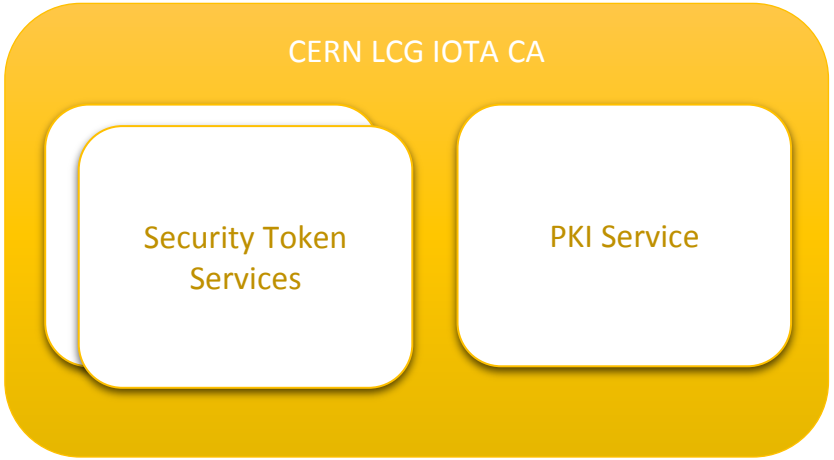
➔Must move to accredited CA



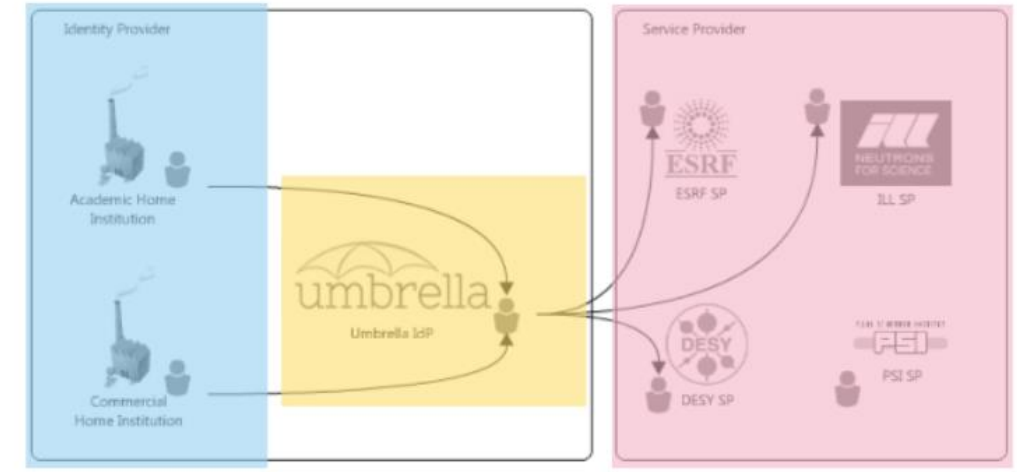
Slide: Paolo Tedesco, CERN IT/IS

CERN LHC IOTA CA

- CA Infrastructure consists of
  - PKI Service
  - STS Services (one per client)
- PKI Service:
  - Issues certificates only to STS
  - Issues CRLs
- STS Service
  - Issues certificates (proxies) to client applications
  - Enforces restrictions on VO membership
  - Enforces restriction on unique user ID

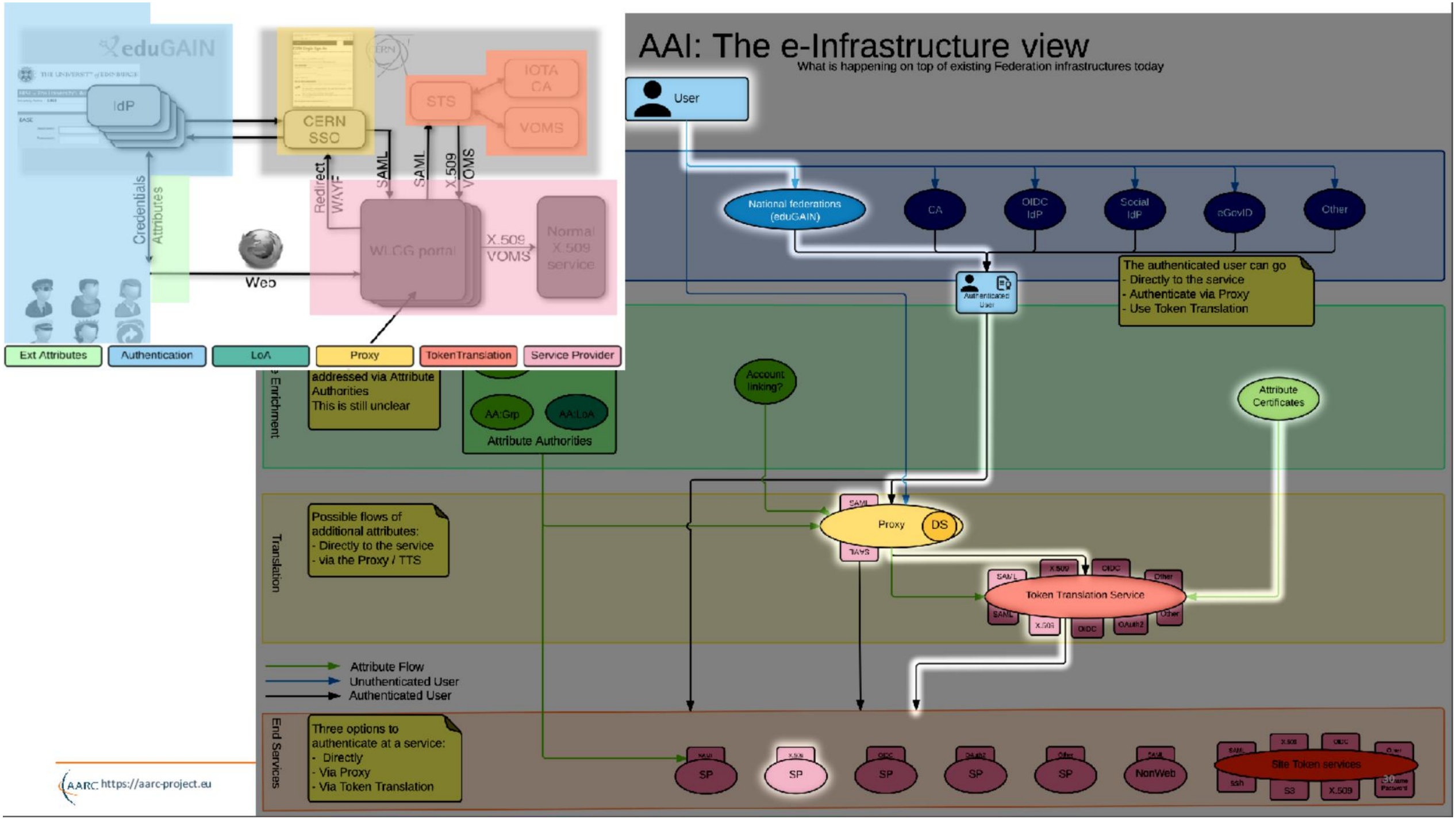


Example: Umbrella



Marcus Hardt, KIT and AARC

https://aarc-project.eu/wp-content/uploads/2015/11/20151102-JRA1.2-Blueprint-Status-Hardt.pdf


AAI: The e-Infrastructure view
What is happening on top of existing Federation infrastructures today
User
eduGAIN
IdP
CERN SSO
STS
IOTA CA
VOMS
Credentials
Attributes
Redirect
WAYF
SAML
SAML
X.509
VOMS
Web
WLCG portal
X.509 VOMS
Normal X.509 service
Ext Attributes
Authentication
LoA
Proxy
TokenTranslation
Service Provider
National federations (eduGAIN)
CA
OIDC IdP
Social IdP
eGovID
Other
Authenticated User
The authenticated user can go
- Directly to the service
- Authenticate via Proxy
- Use Token Translation
Enrichment
addressed via Attribute Authorities
This is still unclear
AA:Grp
AA:LoA
Attribute Authorities
Account linking?
Attribute Certificates
Translation
Possible flows of additional attributes:
- Directly to the service
- via the Proxy / TTS
SAML
Proxy
DS
WAYF
SAML
X.509
OIDC
Other
Token Translation Service
SAML
X.509
OIDC
OAuth2
Other
Attribute Flow
Unauthenticated User
Authenticated User
End Services
Three options to authenticate at a service:
- Directly
- Via Proxy
- Via Token Translation
SP
SP
SP
SP
SP
NonWeb
Site Token services
SAML
X.509
OIDC
Other
ssh
S3
X.509
Username Password
https://aarc-project.eu
30

Issues hindering the adoption of FedAuth

Although many production federations are pretty good, and quite a few IdPs have good processes …

- public documentation, self-assessment and peer-review are missing
- it's **not consistent** across IdPs

and processes are not designed for collaboration use cases

- **re-use of identifiers** occurs (also an issue for social IdPs)
- the identity providers provide no identity … or it's non-consistent
- identifiers generated are specific to each SP (defeating brokering)

and may not provide traceability needed for valuable resources

- some allow **users to change their own data** (including e.g. their email address and all contact data), or do not collaborate in case of issues

engage help of others, in particular some well-organised user communities

Baseline Assurance Profile for low-risk use cases

AARC MNA3.1 (Mikael Linden et al.):
“Recommendation on minimal assurance level relevant for low-risk research use cases”

- Accounts belong to a known individual (i.e. no shared accounts)
- Persistent identifiers (i.e. are not re-assigned)
- Documented identity vetting (not necessarily F2F)
- Password authN (with some good practices)
- Departing user’s account closes/ePA changes promptly
- Self-assessment (supported with specific guidelines)

Redistributing responsibilities with IOTA

Who can absorb the responsibilities, if not the identity providers?

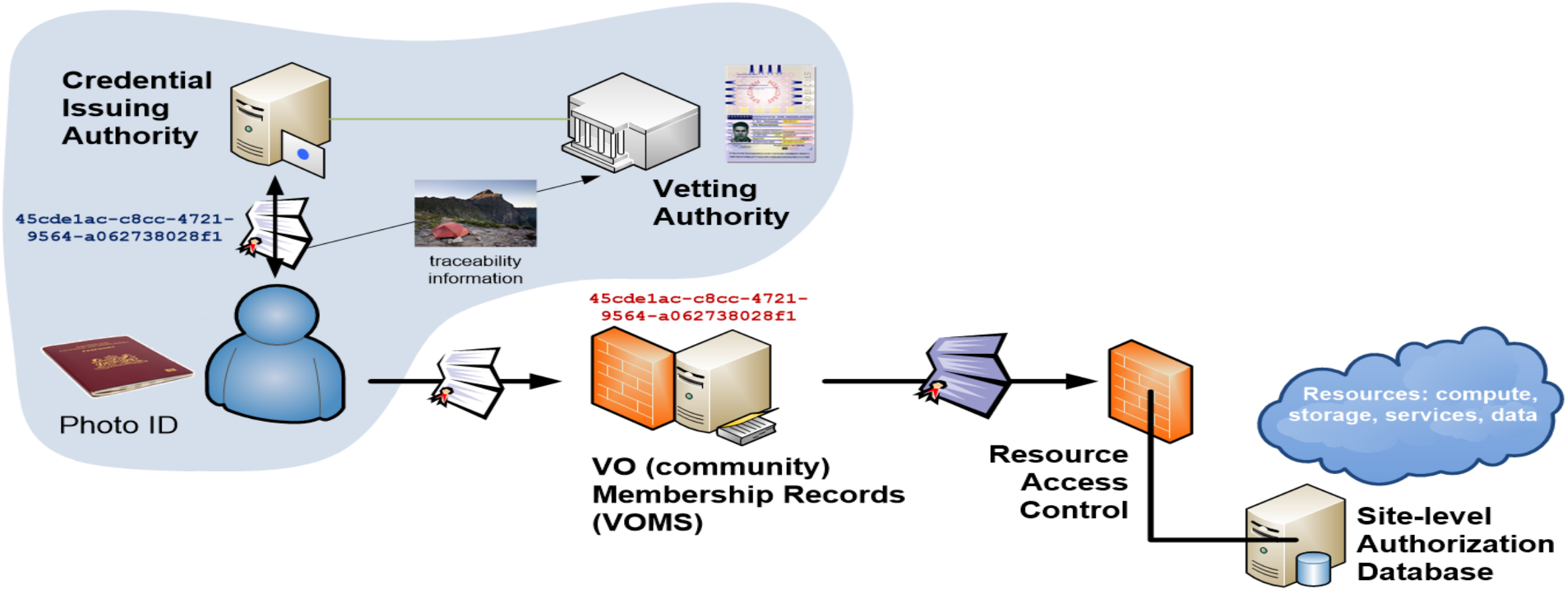
Requirements:

- End-to-end traceability must remain the same
- Changing or documenting federation and IdP processes is a ‘lengthy’ process – but adding some requirements does work (e.g. SiRTFi on incident response)

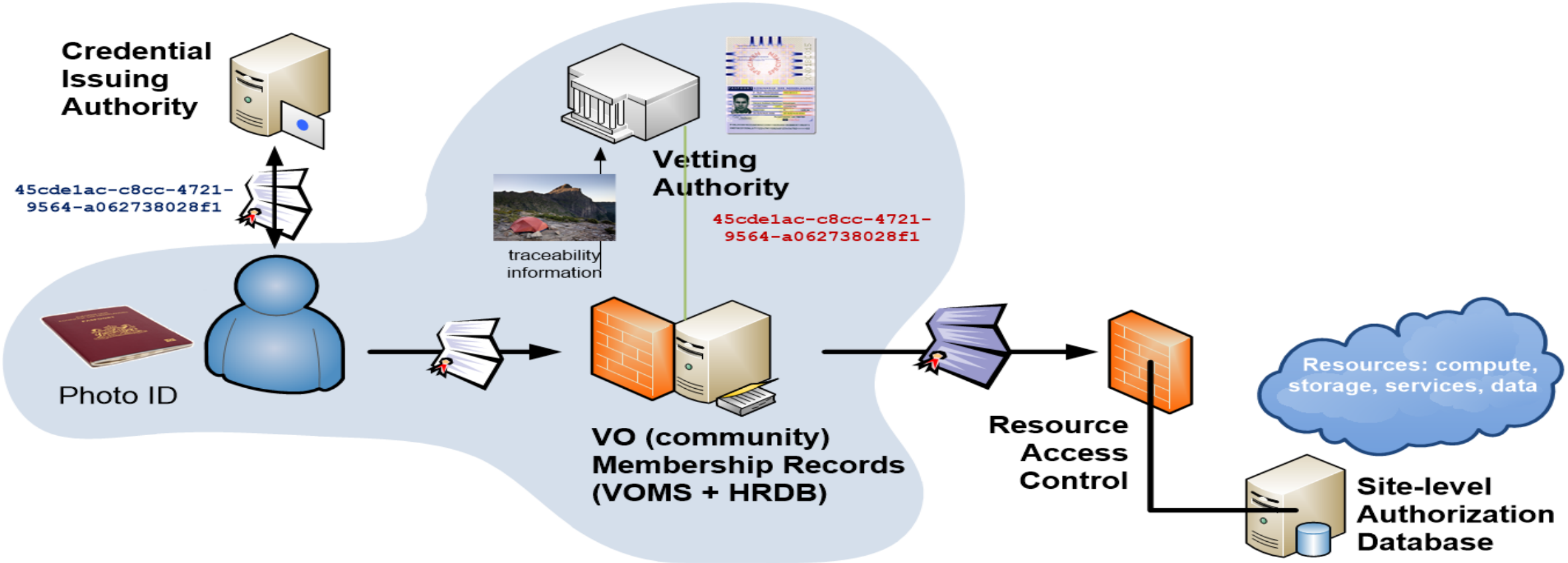
… so who can absorb the responsibility?

- The resource centres – and go back to 1995 with per-site vetting ☹
- The Infrastructure or funding agencies, through a rigorous registration process – PRACE ‘home sites’, or XSEDE registration + NSF granting
- EGI UMP – that’s what’s happening partially in the LToS service
- Or the communities?

Distributed Responsibilities I: Trusted Third Party



Distributed Responsibilities II: Collaborative Assurance & Traceability

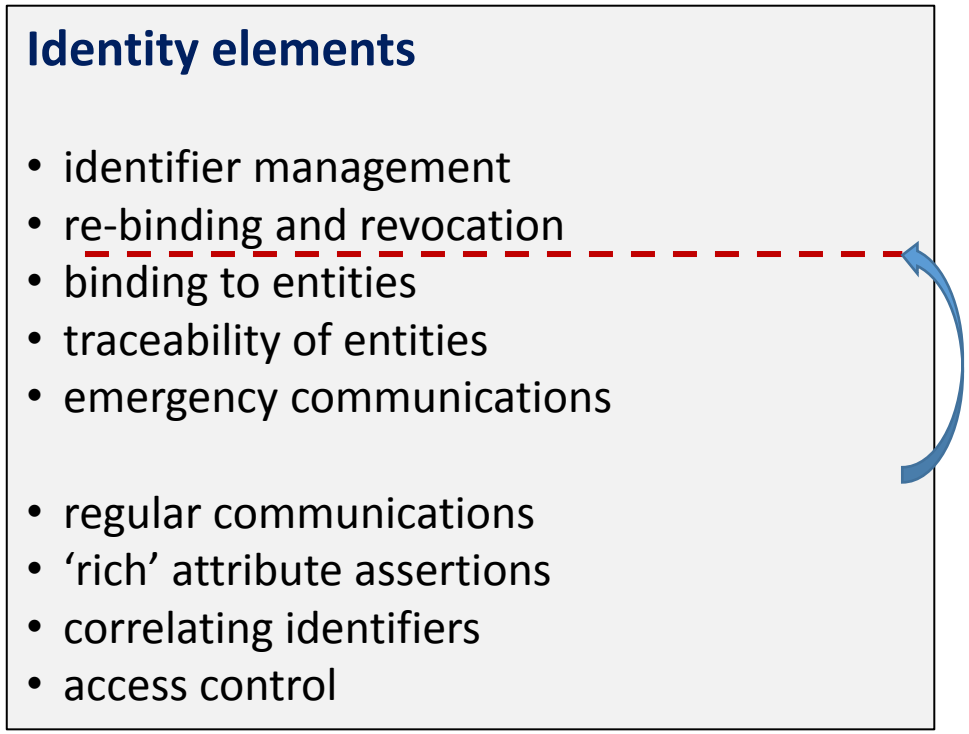


Moving the bar towards differentiated assurance

http://igtf.net/ap/iota *(part of http://igtf.net/ap/loa)*

- IOTA AP assurance level ‘DOGWOOD’ *is* different, and remainder of the elements ***must*** be taken up by somebody else – the VO or the sites

- Only thing you get is an opaque ID
- Consider questions about
  - Real names and pseudonyms
  - Enrolling users in a community
  - Keeping audit records
  - Auditability and tracing
  - Incident response



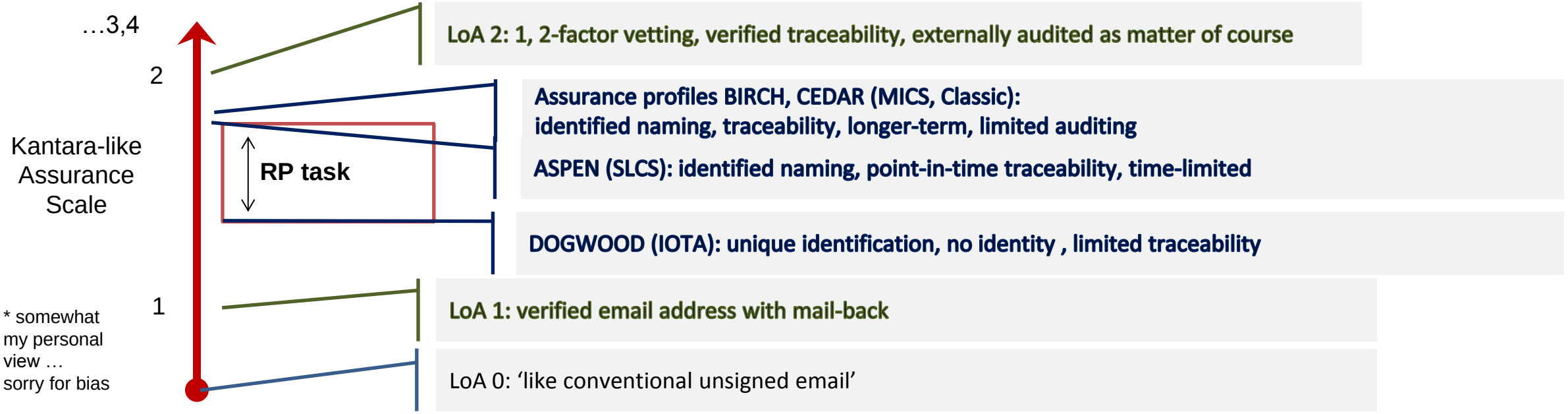
Assurance profiles as charted by the IGTF

So many production federations and IdPs are pretty good, but …

- they are **all different**, and the lowest common denominator is quite low

… so IGTF for ‘conventional’ assurances requires **additional per-user controls**

… and the (‘uniqueified’) AP ‘DOGWOOD’ (IOTA) leaves an assurance gap



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’ – the CERN LCG IOTA CA

- 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

*) https://documents.egi.eu/document/79

Can you combine two policies within the same infrastructure?

- Can been done if new policy does not negatively affect the other one

- Which *in this case* is OK, since the specific new CERN IOTA CA
  - In itself implements all the policy requirements of a traditional CA by insisting on LHC membership
  - the same requirement that already governs the Classic CERN CA

- But note that is **does not generally hold** for arbitrary IOTA CAs
- Have to wait for “VO+CA-authZ” before adding e.g. InCommon Basic

- Technically it is a relatively easy change

Software support for DiffLoA

What is needed it for the infrastructures (resource centres) to differentiate between ‘light-weight VOs’ and ‘heavily-managed VOs’

- Preferably on a per-VO basis
- Allowing IdPs with a lower assurance profile to be used for heavily-managed VOs’
- Whilst ensuring light-weight VOs can continue to enjoy airiness since they’re combined with higher-assurance IdPs (CAs)

Logic foreseen for such a decision

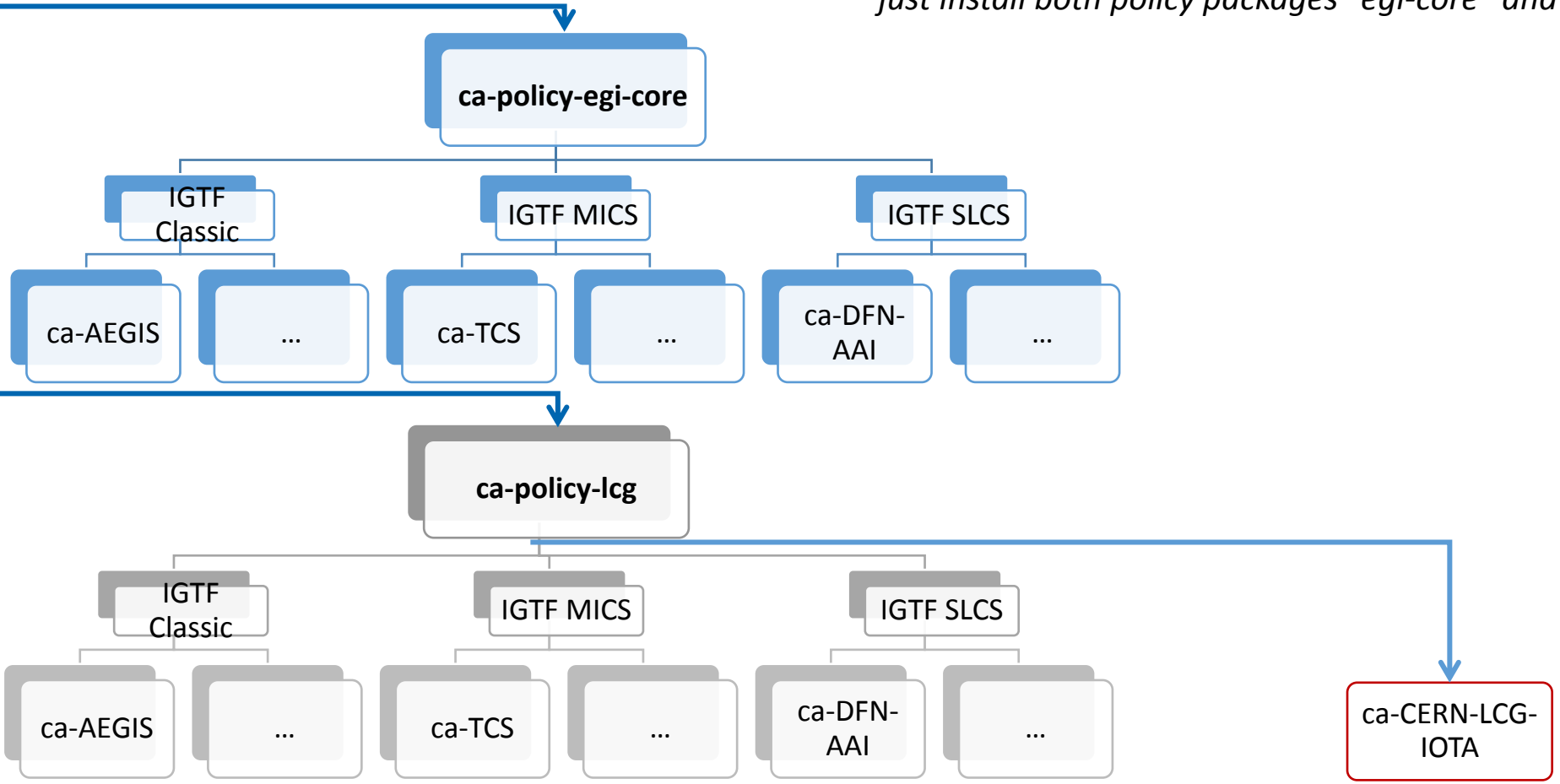
```
( VO:/pvier && CA:IGTF-Classic,IGTF-MICS,”NL-eInfra-Zero-CA” ) ||
( VO:/atlas && CA:IGTF-Classic,IGTF-MICS,IGTF-SLCS,IGTF-IOTA ) ||
( VO:/*     && CA:IGTF-Classic,IGTF-MICS,IGTF-SLCS )
```

Dependencies in policy installation

'lcg-CA'
or explicit configuration

For EGI-only sites: nothing changes!

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



Translation services – beyond the specific use case

CILogon Service

NCSA (IL,USA) operated service and project

InCommon backed MICS and IOTA

Generic ‘opaque’ certificate in Europe

Helps with PII data protection and integration with ESFRIs and e-Infrastructure

CERN wLCG IOTA CA

eduGAIN backed with added CERN HR DB controls

GÉANT

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

AARC operational pre-pilot: bridging R&E federations with non-web & PKI

Proposal-identified pre-pilot: certificate-less access to existing services with “CILogon for Europe”

- Aligned with the EGI “JRA1” activity around the evolution of the AAI technology (ChristosK)
- Using actual use cases from EGI competence centres and AARC communities

“It’s always a challenge to pilot something with a real community – the expectations are usually much higher than what can be provided in a pilot …”

- AARC *will not operate* any long-term services (that’s for GEANT, EGI, PRACE, EUDAT …)
- But *will pilot* actual technology combinations that are useful to (research) communities

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.)

Pre-pilot work, so based on pre-AARC 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, …
- Try to fit first in the existing policy framework: Approved Robots (and “PUSPs”), Trusted Credential Stores, PKP Guidelines, IGTF ‘DOGWOOD’ – unless the pilot runs aground …

Desired feature set

- Certificate or proxy retrieval possible for federatively-authenticated end-user inside a community (VO) portal or science gateway
- Work with the existing (SAML2) R&E federations
- Credential repository feature: manage credentials on behalf of the user
- Provide – on the user's request – delegated credentials to science gateways
- Make end-user facing science gateways *really* light-weight: VOs should not need to know about protecting long-term secrets (and need a way to authenticate users)
- Support both certificate and non-certificate science gateway use cases in the same way
- Provide simple way for users to obtain 'opaque' CLI credentials (proxies) on their own system

Constraints:

- No new software components (only limited glue)
- Deployable in a scalable way – with a sustainability model behind it
- As few CAs as possible (preferably: just one)

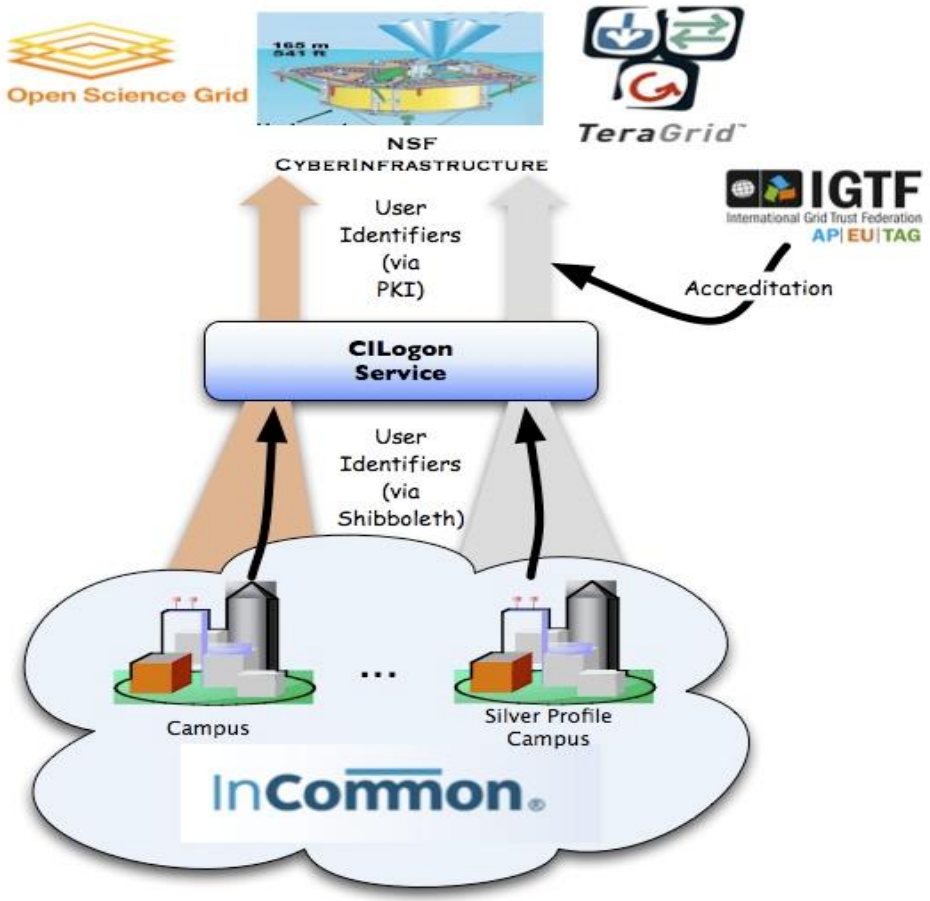
CILogon service and project (Jim Basney et al.)

CILogon Service

- 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

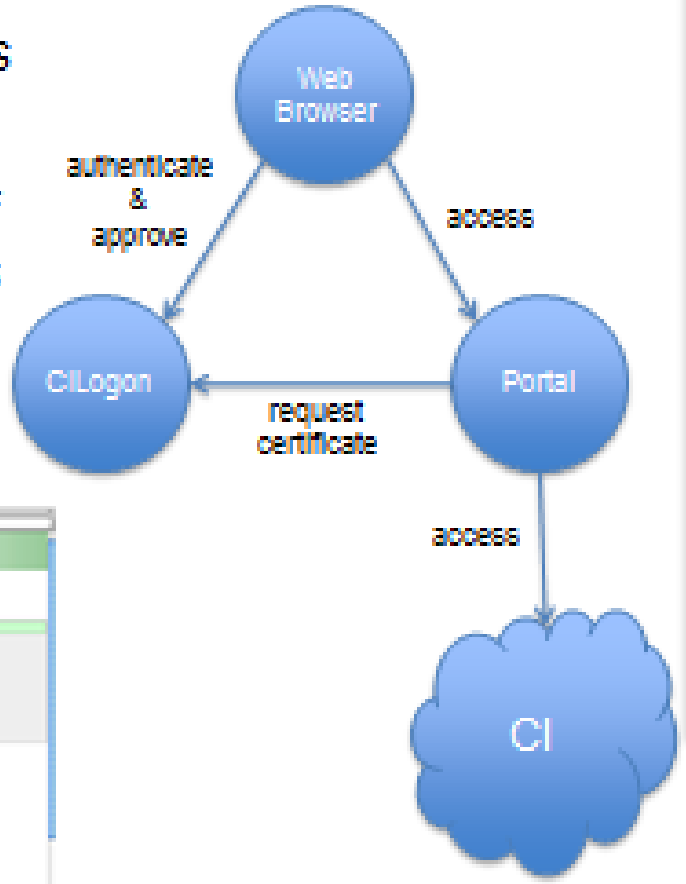
- SAML/OpenID Web Browser SSO
  - PKCS12 certificate download
  - Certificate issuance via OAuth
  - OpenID Connect token issuance
  - SAML ECP for CLI issuance

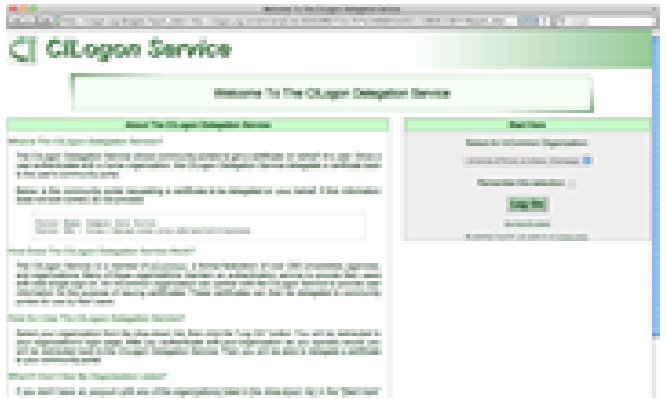


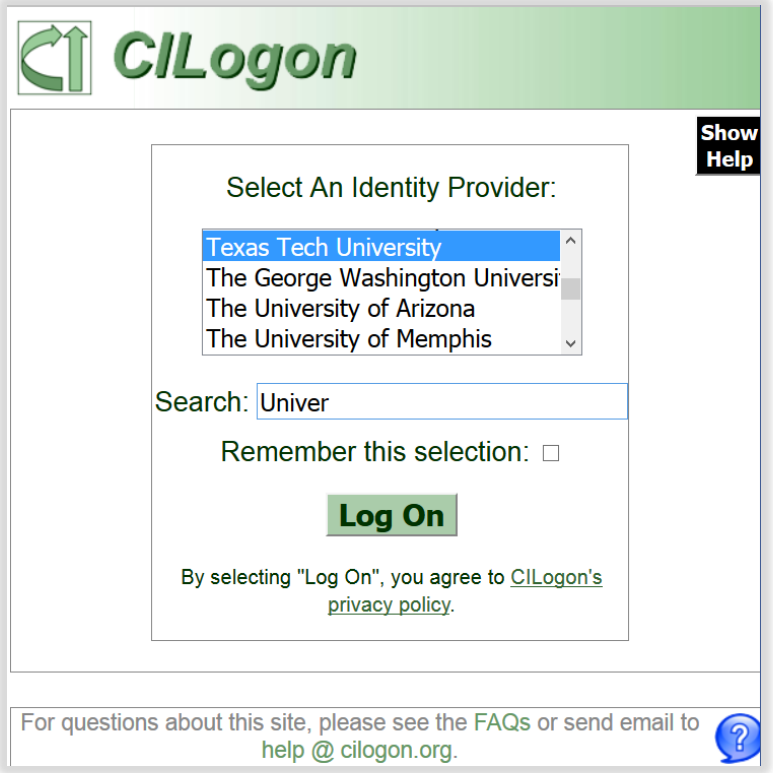
Slide content: Jim Basney, based on http://www.cilogon.org/docs/201106-cilogon-cern.pptx?attredirects=0&d=1 and http://www.cilogon.org/docs/20141030-basney-cilogon.pdf?attredirects=0&d=1

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





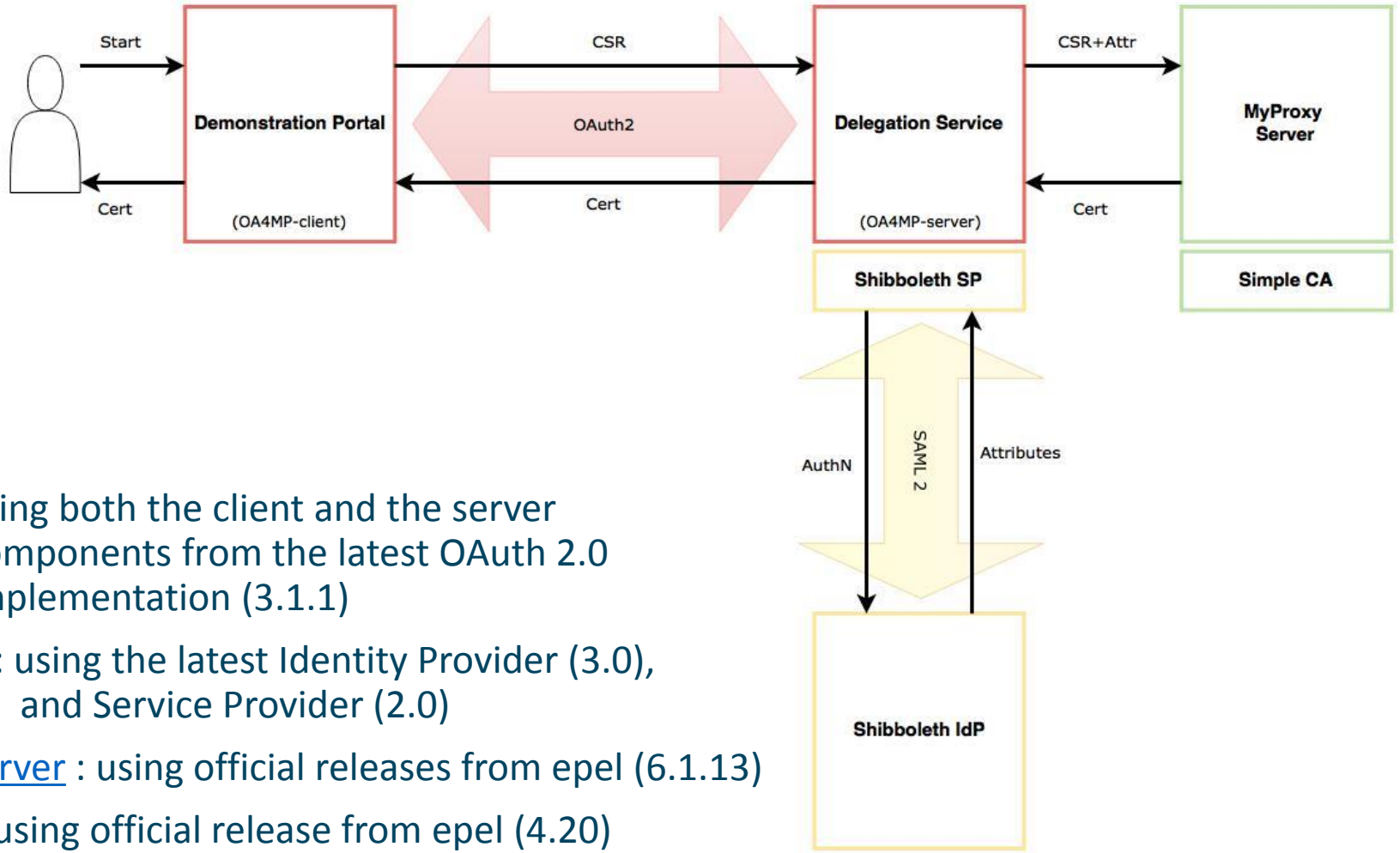


CILogon

www.cilogon.org

Slide: Jim Basney, NCSA and CILogon

CILogon demo portal: Delegation of credentials using OAuth4MyProxy



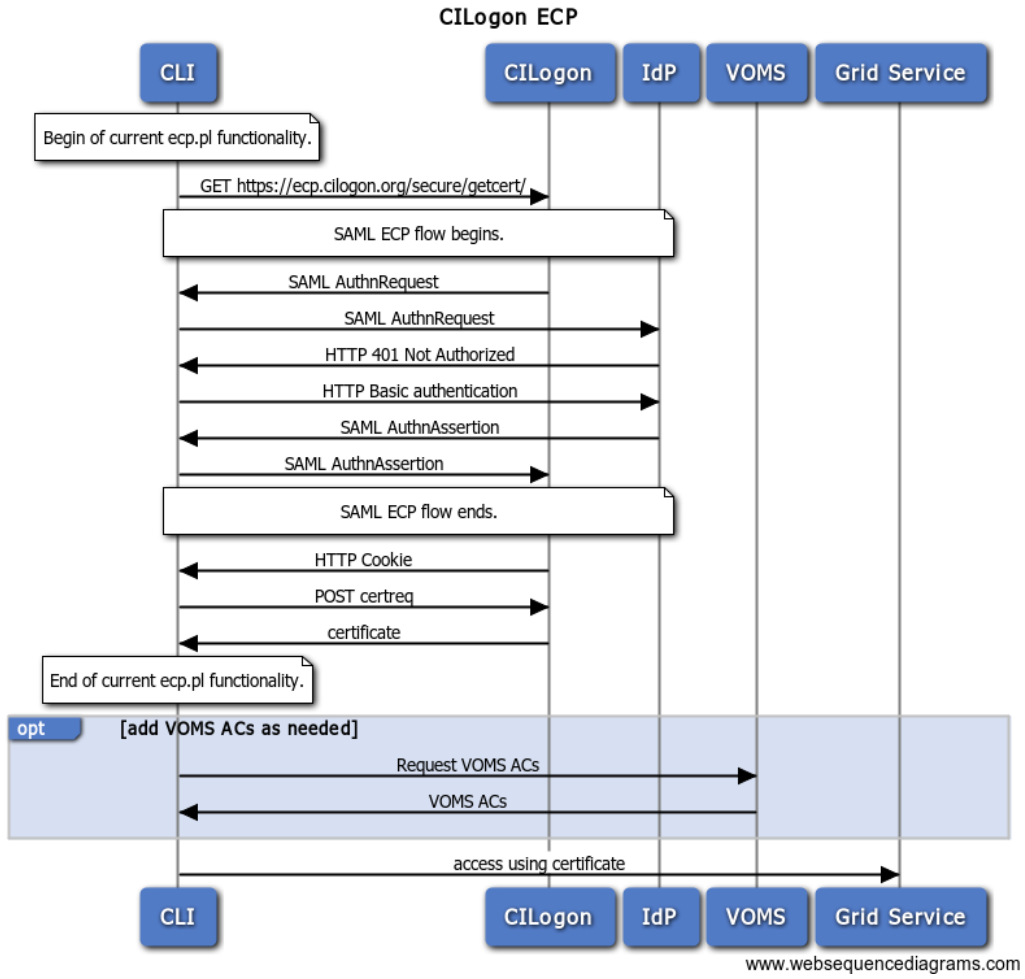
- OA4MP : using both the client and the server components from the latest OAuth 2.0 implementation (3.1.1)
- Shibboleth : using the latest Identity Provider (3.0), and Service Provider (2.0)
- MyProxy Server : using official releases from epel (6.1.13)
- SimpleCA : using official release from epel (4.20)

CILogon and SAML ECP

- SAML federated login via ‘Enhanced Client’ (read: CLI) or ‘Proxy’ (read: brokered access)
- https://wiki.oasis-open.org/security/SAML2EnhancedClientProfile

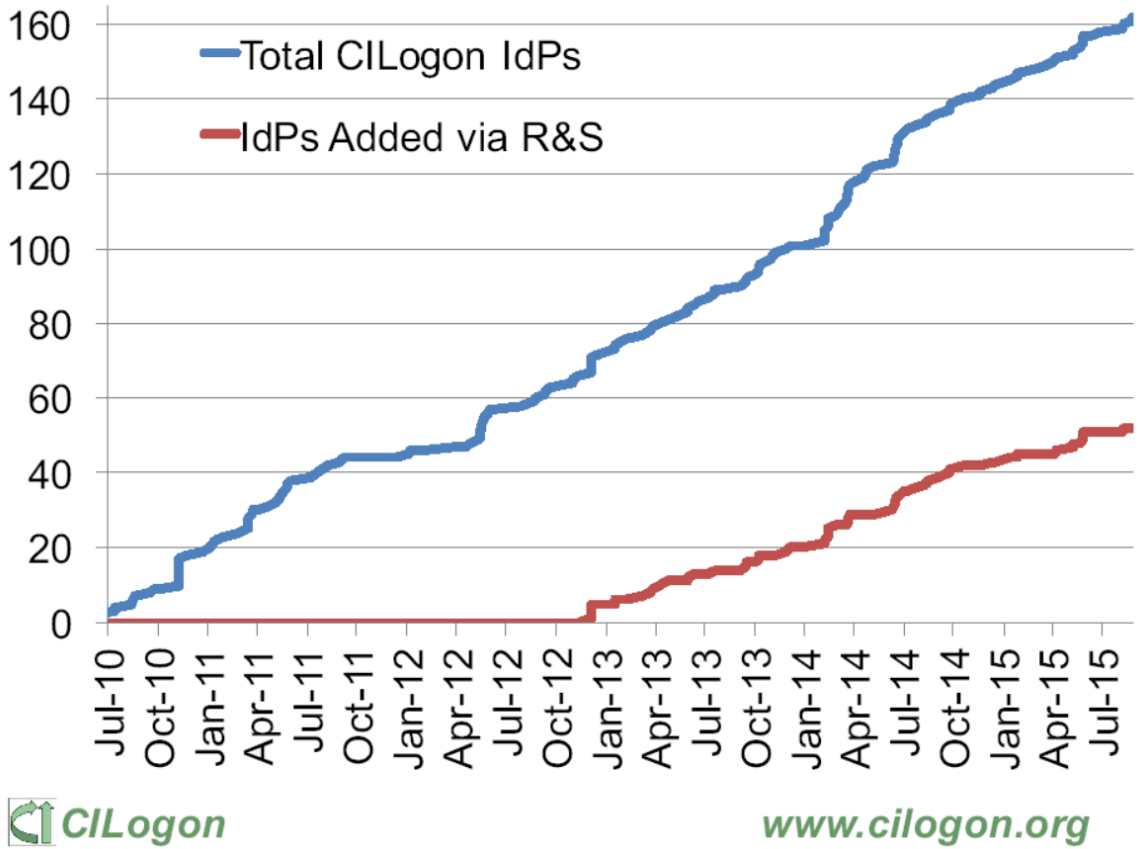
- A heavy (**trusted**) client sends credentials and receives assertions from a specific IdP ECP end-point
- Supports non-web
  … if it were supported by the IdP
- Most prominent use case: Office365
- Limited update & support (only in Shib, and only v3+)

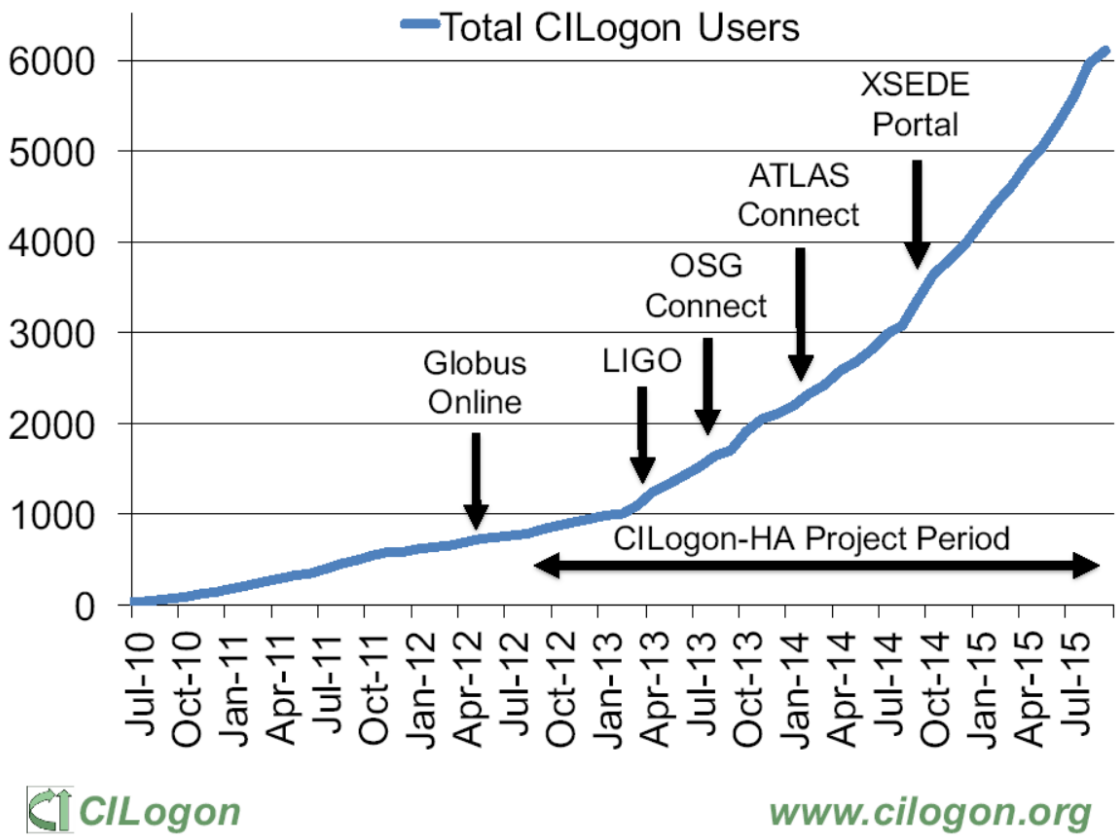
Unlikely to fly in Europe – but there many alternatives like Moonshot, but also a move to OIDC, OAuth2, …



Flowchart: from CILogon

CILogon adoption in the US/InCommon





http://www.cilogon.org/docs/2015-09-cilogon-ha.pdf?attredirects=0&d=1

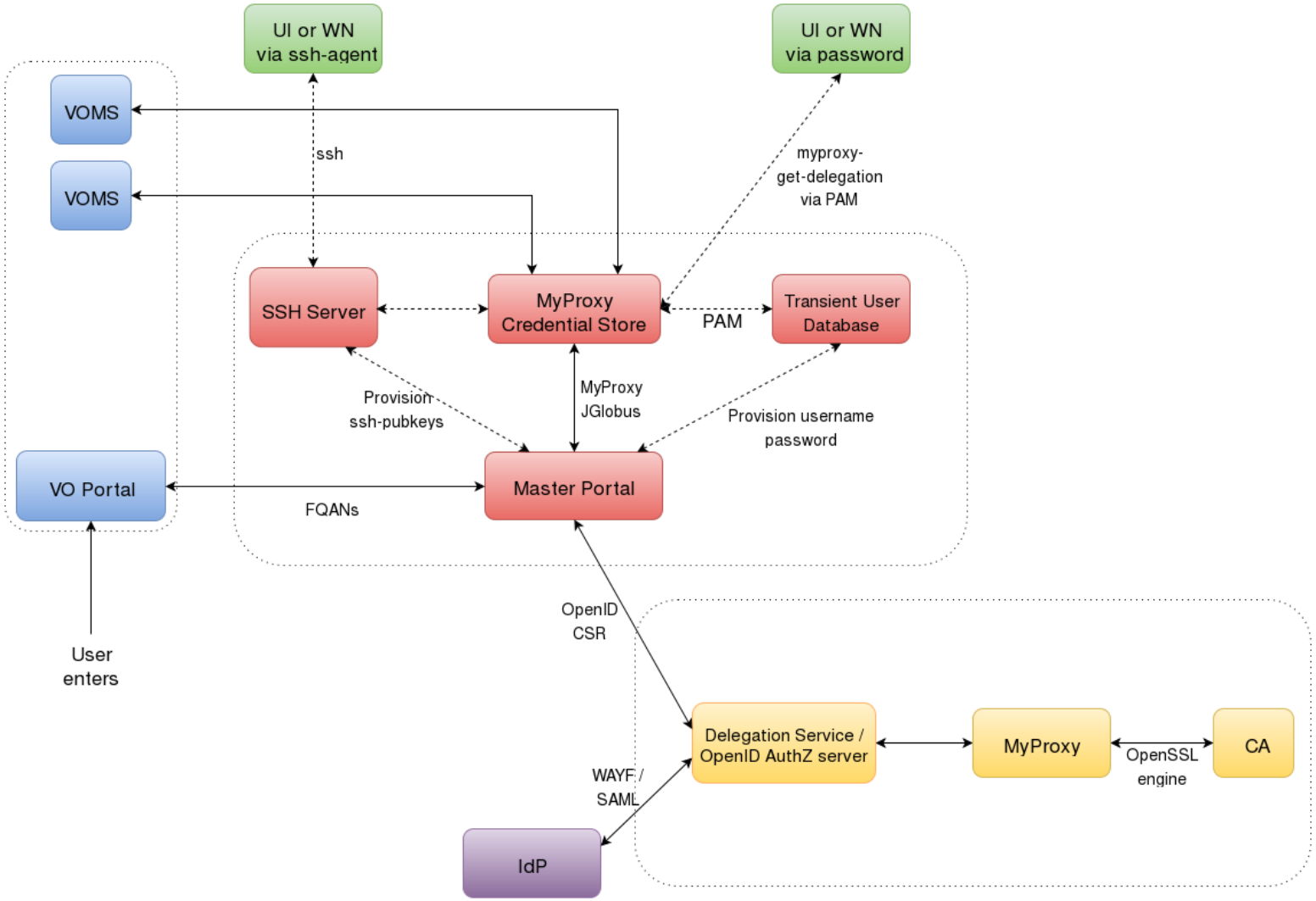
End-user credential hiding in the AARC CILogon-like Pilot

- 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’ (i.e. in a few months work) for a broad audience
- 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*

Components



http://wiki.nikhef.nl/grid/CILogon_Pre-Pilot_Work

Authorization at the VO level

- The VO light-weight portals (gateways) can re-use this system for both AuthN and AuthZ
- Can be used besides a conventional (SAML) login to science gateway when a proxy is needed

Or even …

- *User ability to complete the OIDC login to the VO web portal (each time) does AuthN*
- *Ability of the portal to successfully request VOMS attributes for an AuthZ/membership check*
- *Successful authN and failed AuthZ? Suggest enrolment or auto-enrol members!*

- VO portal must be on a trusted list of the Master Portal
  - Needs to be able to do OIDC in a trusted way
  - Using a VO portal *client ID + client secret* (but there are server certs as well for the web site itself)
  - User must be able to trust that the Master Portal will only relinquish user credentials to intended places
  - OIDC consent mechanism informs the user of where the user credentials are sent

X509 (proxy) certificates as opaque access tokens

- VO or Master Portal can offer user to register user's SSH pubkey with Master Portal
- Master Portal can store (uid, pubkey) pairs in a directory service (e.g. LDAP) associated with the MyProxy user identifier (username)
- SSH Server runs cron job and creates authorized_keys file:
  - Using a single special account, runs a *myproxy-logon* wrapper, similar to what SVN servers do*
- SSH-agent forwarding: central login node, client UI, VDI server, laptop retrieves proxy
- Any script wrapper to save proxy: looks similar to a Kerberos ticket
  - No need for either extra password, ECP, Moonshot etc.
  - Very similar to GitHub, SourceForge, etc.

```
* /usr/local/sbin/mkgroup-sshlpk \
    -c 'command="svnserve -t -r /srv/svn --tunnel-user=@UID@", no-pty' \
    -o ~svn/.ssh/authorized_keys --filter '(authorizedService=ndpfsvn)' nDPFSubversionUsers
... [gives] ...
command="svnserve -t -r /srv/svn --tunnel-user=tsuerink",no-pty ssh-rsa AAAAB3...2w== t@net
```

Distribution of Roles in a Sustainable Model

VO Portal (Science GW)

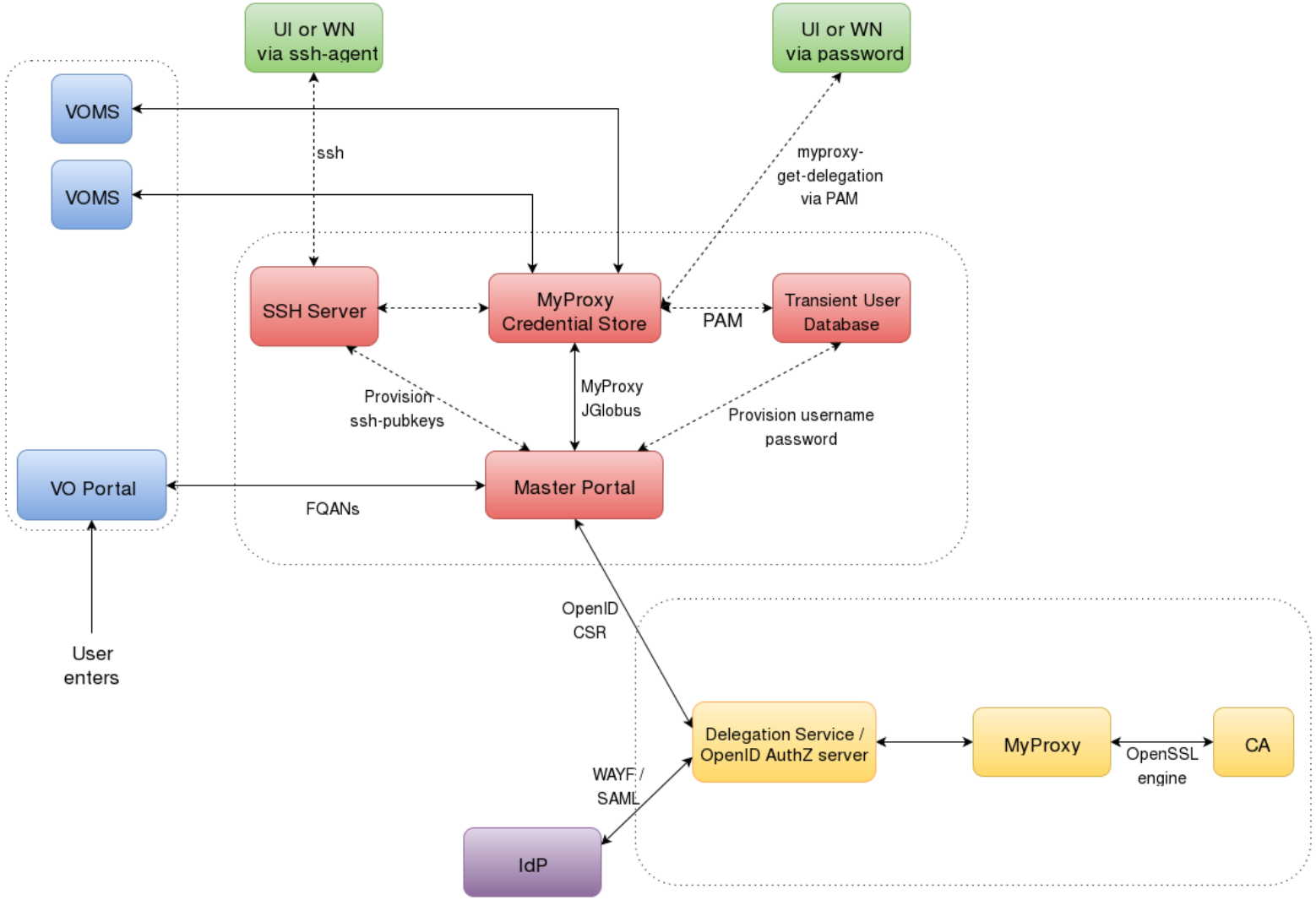
- One per application
- Many deployed throughout
- Reduced policy and compliance burden

Master Portal

- One per country, ESFRI
- Must be well-managed
- Can be managed because there are few

CA and Delegation Service

- As few as possible: just one!



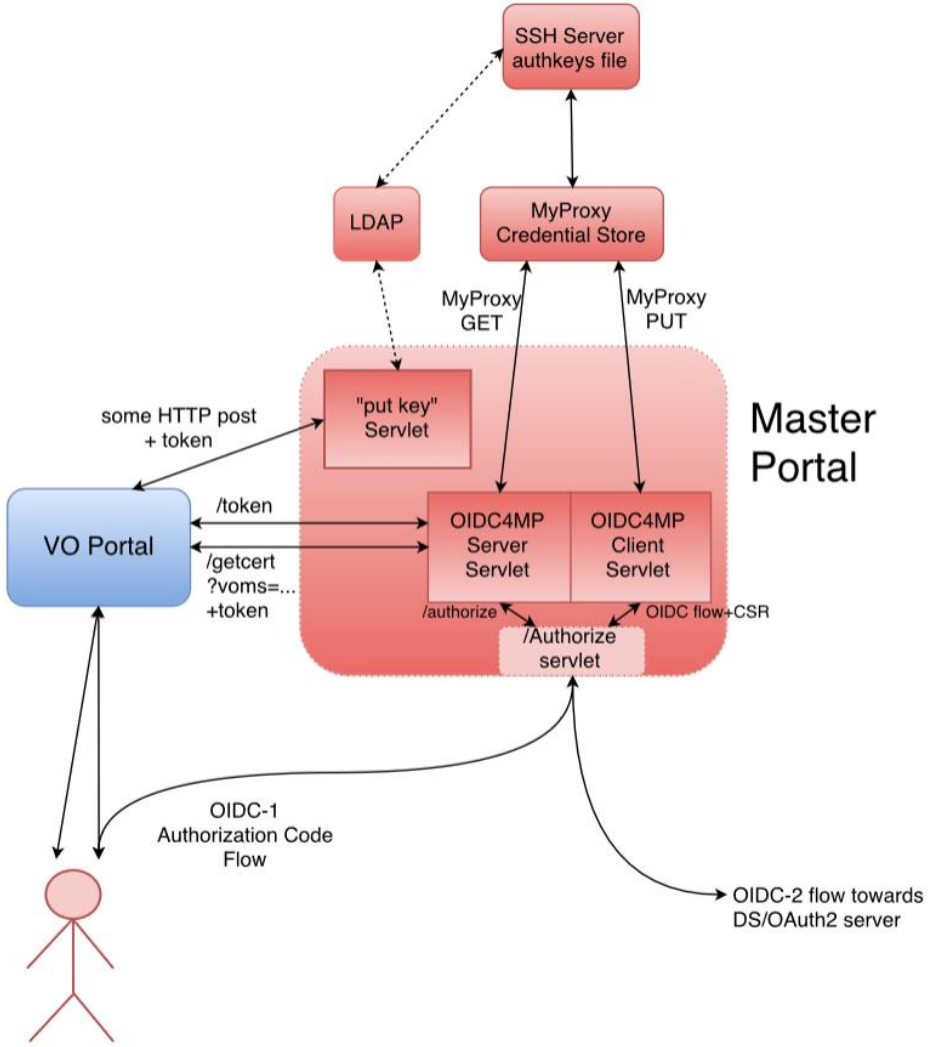
Master portal is a rather critical service

- This is the component that – with a credential store and an (OIDC) authentication interface – takes care of the user credential management

- The back-end CA provides
  - Identifier uniqueness
  - Revocation capability

  but not much more!

- It is a highly trusted component, of which there should not be many
- But it may still be better then end-user managed keys – for *authentication*, that is …



Relevant (IGTF) policies

- IOTA AP: LoA DOGWOOD and PKI Technology Guidelines
  - https://www.igtf.net/ap/iota
  - https://www.igtf.net/ap/loa
  - https://wiki.eugridpma.org/Main/PKITechnologyGuidelines
- PKP Guidelines
  - https://www.eugridpma.org/guidelines/pkp
- Guidelines on the Operation of Credential Stores (draft)
  - https://www.eugridpma.org/guidelines/trustedstores/

Consensus on compliance of a CILogon

- Use proxies and/or EECs with a validity less than 1 Ms (11 days)
- Long-running workflow support (including reminders to the user to refresh credentials) is in the domain of the VO community and not supported by the master portal (needs re-login)
- Align Trusted Credential Store guidelines with PKP – and educate Master Portal Operators
- PKP Guidelines remain as-is. The IOTA CA instance will be an on-line model B CA with L2 HSM + controls

Towards a CILogon CA for Europe

As a first phase, Jim may actually just open up the existing CILogon to 'eduGAIN'

- Once InCommon has also technically joined eduGAIN
- For qualified entities in eduGAIN: **R&S + SirTFi**
- Uniqueness enforced by the CILogon CA itself (as long as there's no true 'ePUniqueID')

Aim for (a single) IOTA CA in Europe (EU/EEA) to back the Master Portals

- This would be a generic IOTA CA, but it can be modeled closely on the existing ones
- Model yet to be worked out (extend CERN's IOTA CA? A new one?)
- Support as many (European) eduGAIN IdP as feasible
- Potentially including qualified *IdPs of last resort* operated by RI/e-Infrastructures, or qualified proxy services like the VOPaaS IdP gateway (with LoA support)
- Having it issue only short-lived credentials would make things like DPCoCo compliance easier

Another alternative: replace the CA with a single Robot & ‘Per-User sub-proxies’ (PUSPs)

- PUSPs are already used by the EGI “Long Tail of Science” gateways
- RFC3820 proxy certificates generated from a single Approved Robot:
  - embedded in the naming is a unique identifier
  - the generator (portal) can associate the identifier with an individual Web User

```
"/C=IT/.../CN=Robot: Catania Science Gateway - Roberto Barbera/CN=user:jdoe" jdoe_localuser
"/C=IT/.../CN=Robot: Catania Science Gateway - Roberto Barbera/CN=*" .portal_users
```

- This can also replace the CA it ‘just’ take the portal setup outside the PKP scope

but … is this the best way to do things??

https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Federated_AAI:per-user_sub-proxy

Access to a CILogon service from ‘all of eduGAIN’ - requirements

eduGAIN is a policy-neutral interfederation exchange mechanism

– so it has no single policy ☹

To make it trustworthy and usable, it is wide to consider requiring e.g.

- R&S attribute release,
  so a service gets *eduPersonPrincipalName*, *mail*, and *(displayName OR (givenName AND sn))*
- gets a non-reassigned identifier
  may be ePPN, could be the (useless but at least unique) *eduPersonTargetedID* or *NameID*
- aligned with the SirTFi Framework
  for IdPs, attribute auhorities and other SPs

SirTFi – 1.0 !

- defines basic security incident response capabilities to which member organizations can **self-assert compliance**
- initial draft intended to be a simplified framework – approved now by REFEDS to stimulate adoption by IdPs and promotion via federations (but the framework is general)
- Based on SCI grouping of capabilities

- Self-assertion is a rather newish concept in conventional R&E federations, but fits the RIs and e-Infrastructures for the prevalent use cases – the IGTF does peer-review supported self-audits
- To scale self-assertion to 10k+ entities (IdPs, SPs, attribute authorities) needs automation
- EWTI working group on the self-assessment tool collected initial requirements (Mikael, Hannah)

https://wiki.refeds.org/display/GROUPS/SIRTFI

SirTFi – assertions and capabilities: OpSec

Managing access to information resources, maintaining their availability and integrity, and maintaining confidentiality of sensitive information is the goal of operational security.

- [OS1] Security patches in operating system and application software are applied in a timely manner.
- [OS2] A process is used to manage vulnerabilities in software operated by the organisation.
- [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats
- [OS4] A user's access rights can be suspended, modified or terminated in a timely manner.
- [OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.
- [OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

SirTFi capabilities: IR

Assertion [OS6] above posits that a security incident response capability exists within the organisation. This section's assertions describe its interactions with other organisations participating in the Sirtfi trust framework.

- [IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs.
- [IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.
- [IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust framework
- [IR4] Follow security incident response procedures established for the organisation.
- [IR5] Respect user privacy as determined by the organisations policies or legal counsel.
- [IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy.

SirTFi Capabilities: TR and PR

To be able to answer the basic questions "who, what, where, and when" concerning a security incident requires retaining relevant system generated information, including accurate timestamps and identifiers of system components and actors, for a period of time.

- [TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.
- [TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices.

All participants (IdPs and SPs) in the federations need to rely on appropriate behavior.

- [PR1] The participant has an Acceptable Use Policy (AUP).
- [PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.

Is this good enough for you, for now?

- IOTA CA backed by ‘all of eduGAIN’ in Europe and beyond, giving a non-reassigned ID
- Traceability only via the home IdPs
  - Follow-up may take a while
  - Service can ban known-bad IdPs (as per policy)
  - But its retroactive banning
  - IdPs-of-last-resort will be there, but filtered on some LoA criteria (community-operated, or otherwise classified with a defined, identifiable, but not necessarily sufficient LoA)
- At least some reasonable attributes that are ‘probably OK’
- Filter on SirTFi self-assertion as an option (how hard would you need that to be?)
- Included for both structured VOs (WLCG, ELIXIR, &c) and looser EGI VOs
- Supported by software that will enable (VO+IdP/CA) decisions?

What did we miss?

Thanks to all AARC folk whose slides and work I used in here –
esp. Mischa Sallé, Tamas Balogh, Jim Basney, Paul van Dijk

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-project.eu

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).