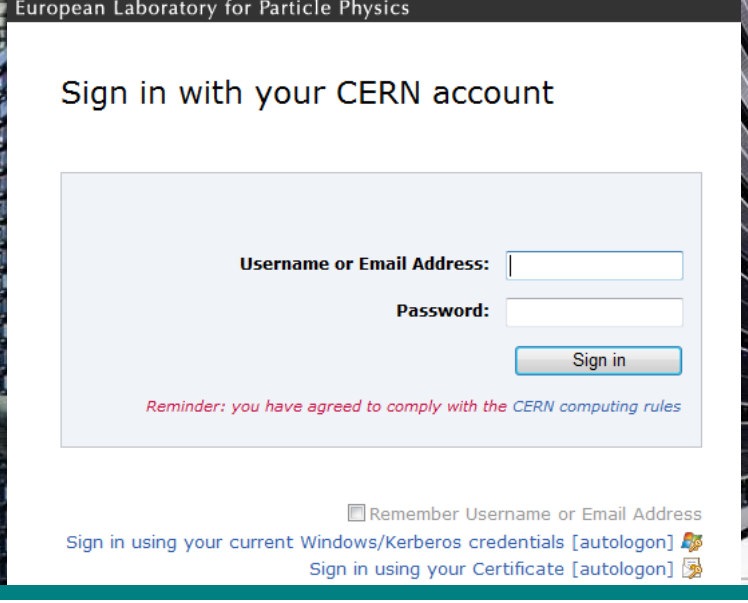
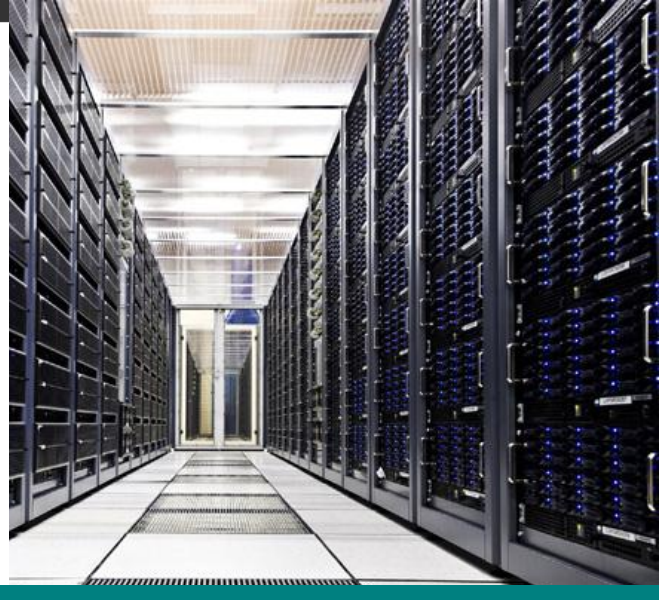




CERN Workshop on Federate ID
Conclusions and Next steps

Dr. Stefan Lüders
CERN Computer Security Officer
Internet2 Fall 2011 Member Meeting, Raleigh (USA)
October 3rd-6th 2011

CERN

EIROforum

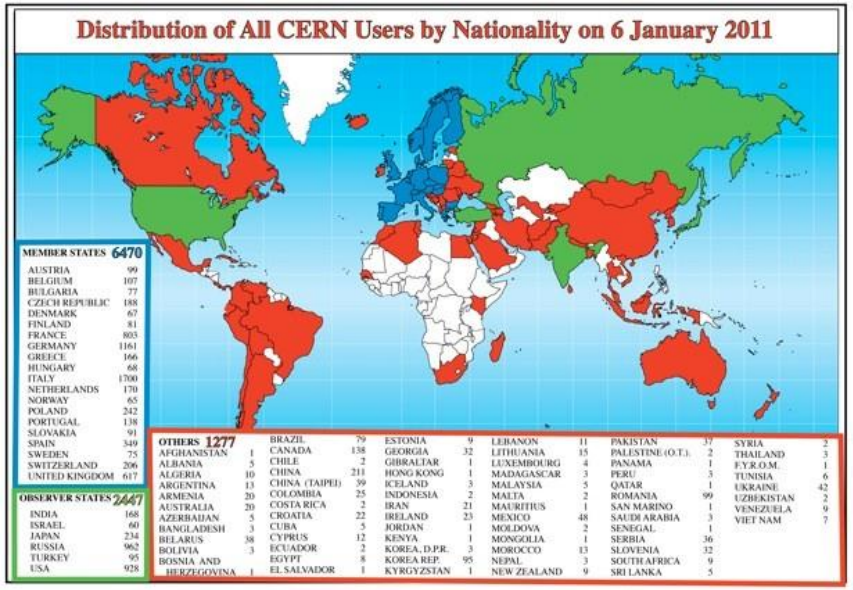
CERN's User Base

CERN's Mission:

- Research: Seeking and finding answers to questions about the Universe
- Technology: Advancing the frontiers of technology
- Collaborating: Bringing nations together through science
- Education: Training the scientists of tomorrow

CERN's Users:

- …from 100s of universities worldwide
- Pupils, students, post-docs, professors, technicians, engineers, physicists, …
- High turn-over (~15k per year)



One CERN Account:

- Everyone with CERN affiliation can get an account (incl. homepage & email)
- Large growth rate of new accounts
- Need for account very diverse (and not always clear)

EIROforum

CERN's User Base

CERN's Mission:

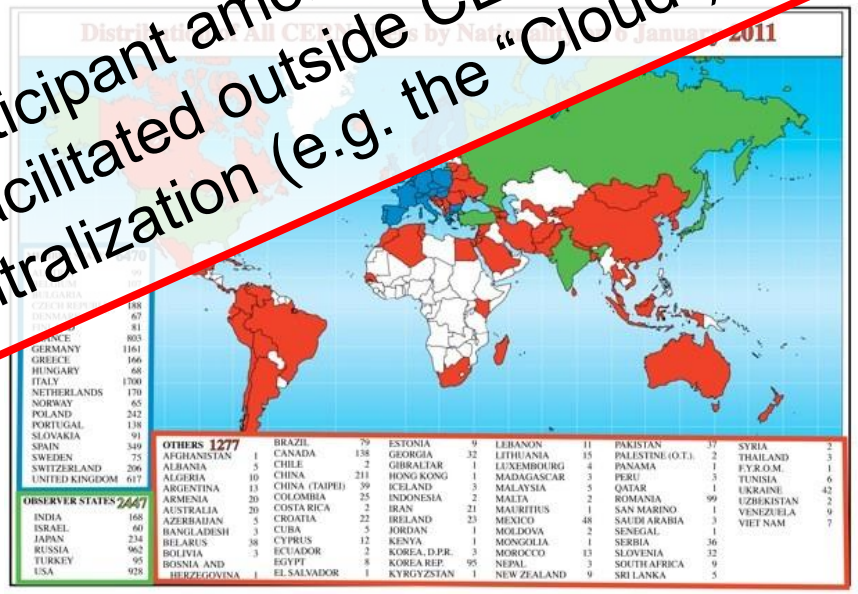
- Research: Seeking and finding answers to questions about the Universe
- Technology: Advancing the frontiers of technology
- Collaborating: Bringing nations together through science
- Education: Training the scientists of tomorrow

CERN's Users:

- …from 100s of universities worldwide
- Pupils, students, post-docs, professors, technicians, engineers, physicists…
- High turnover (~1/3 per year)
- One CERN Account:
  - Everyone with CERN affiliation can get an account (incl. homepage & email)
- Large growth rate of new accounts
- Need for account very diverse (and not always clear)

Shift in focus

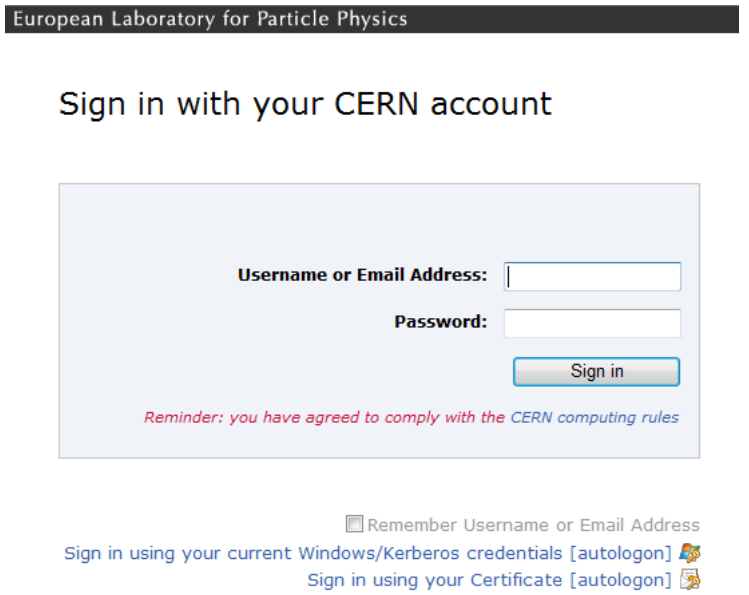
- New projects with CERN as a participant among many
- Collaboration is key (and often facilitated outside CERN)
- Increased externalization/decentralization (e.g. the "Cloud")



CERN SSO

CERN Single Sign On

- 10.000 users p.a.; 20.000 accounts
- One portal for CERN-wide AuthN
- Envisaged for all (web) applications
- From all platforms (Windows, Linux, Mac)
- Microsoft Forefront IM
  AD/LDAP/Shibboleth/Kerberos



E-groups AuthZ/Role Management

- Homegrown solution sync'd with AD/LDAP
- Default access to (more-or-less) all CERN resources
- Fine grained access controls where needed (e.g. controls, admins, …)

Multifactor Authentication

- Currently evaluating SmartChips, Yubikeys, GSMauth

…but also facing demands to join e.g. eduROAM.

CERN

EIROforum

CERN SSO

CERN Single Sign On

- 10.000 users p.a.; 20.000 accounts
- One portal for CERN-wide AuthN
- Envisaged for all (web) applications
- From all platforms (Windows, Linux, Mac)
- Microsoft Forefront IM
  AD/LDAP/Shibboleth/Kerberos

E-groups AuthZ/Role Management

- Homegrown solution synced with AD/LDAP
- Default access to (more-or-less) all CERN resources
- Fine grained access controls where needed (e.g. controls, admins, …)

Multifactor Authentication

- Currently evaluating SmartChips, Yubikeys, GSMauth

This does not scale: Time to step back and review!

- We can't anymore create accounts for everyone and his dog
- We can't force "niche" users to remember another password as they already have one++ in the (HEP) community

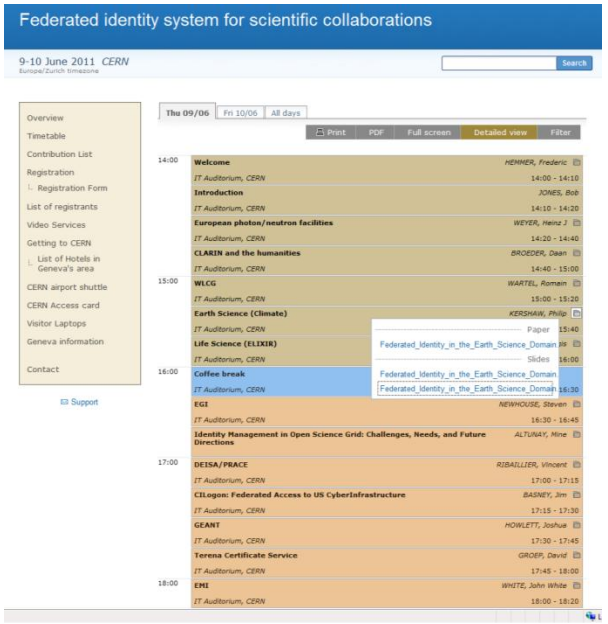
…but also facing demands to join e.g. eduROAM.

FedID for scientific collaborations

Triggered by the EIROforum

(CERN, EFDA-JET, EMBL, ESA, ESO, ESRF, Euro XFEL, ILL)

- "..to explore the requirements for FedID ... compare the functionality, operational constraints and state of deployment of current technologies, and formulate a roadmap for … the future."
- June 9th & 10th 2011
- https://indico.cern.ch/conferenceDisplay.py?confId=129364



85 participants from 44 organizations in 18 countries

- BELNET, CERN, CSC, DANTE, DESY, EGI, GEANT, ICRC, INFN, PSI, SARA, STFC, SURFnet, SWITCH, TERENA, …

Talks from all areas:

- Particle science, social science & humanities, Grid computing, earth science, life science, service providers

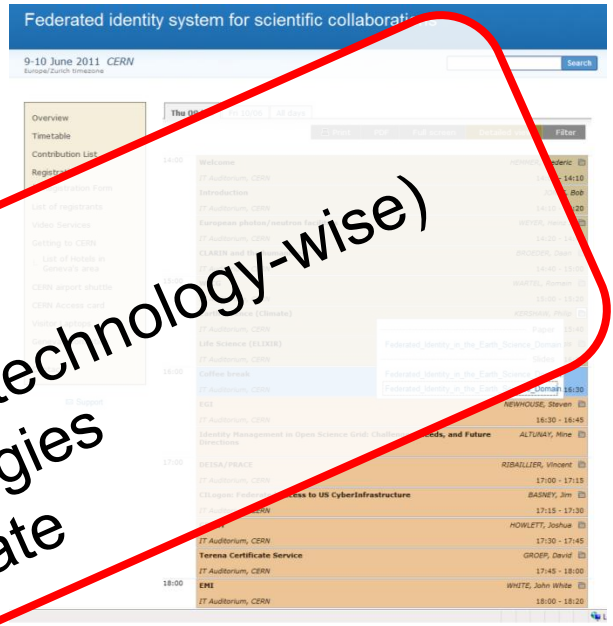
EIROforum

FedID for scientific collaborations

Triggered by the EIROforum

(CERN, EFDA-JET, EMBL, ESA, ESO, ESRF, Euro XFEL, ILL)

- "..to explore the requirements for FedID ... compare the functionality, operational constraints and state of deployment of current technologies, and formulate a roadmap for … the future."
- June 9th & 10th 2011
- https://indico.cern.ch/conferenceDisplay.py?confId=129364



We are not alone!

- Learn what works and what not (policy and technology-wise)
- Identify common areas and potential synergies
- Get guidance where to go/invest/collaborate

85 participants from 44 organizations in 18 countries

- BELNET, CERN, CSC, DANTE, DESY, EGI, GEANT, ICRC, INFN, PSI, SARA, STFC, SURFnet, SWITCH, TERENA, …

Talks from areas:

- Particle science, social science & humanities, Grid computing, earth science, life science, service providers

EIROforum

Comparison

Community	Other projects	# users	Chosen technology	Status	IGTF
ɣ/n Facilities	EUROFEL PanData CRISP	~10 000	Shibboleth/SAML	Umbrella prototype	no
Social Sciences and Humanities	DARIAH CLARIN CESSDAH (DASISH)	O(100) potential for 10 000+	Shibboleth/SAML	CLARIN SP federation (using EduGAIN)	yes
WLCG	WLCG	~5900	x509	Production	yes
Earth Sciences	ESGF GENESI-DEC CMIP5 Metafor IS-ENES	5000+ for CIMP5	OpenID x509 SAML	Production (earth system grid)	not yet but foreseen for EGI integration
Life Sciences	ELIXIR & 10 ESFRI projects	Several millions of user access data via EBI website	not chosen yet	Included in BioMedBridges project workplan	no

Key Findings

Common needs provide scope for agreement:

- Communities focus on data access; existing federations grasp for more
- Trust is the key: IGTF is the source of trust for many existing projects
- SSO wanted, but global SSO much more complex than local SSO
- Make it easier for users (does this rule out x509?)
- But also: risks increase with one single identity. Traceability is a MUST.

Federation policies are well established:

- Delegated down to home institute
- Plans and processes need effort and preparation
- …but how to deal with "homeless" users?

Areas of discussion:

- We need high level collaborative policy, not technological silver bullet
- Identity is only part of the problem:
  What about attributes & group membership across boundaries
- How to guarantee (global) interoperability between federations?

Next Steps

Develop a roadmap we can all agree to

- Identify a few key use cases
- Essential before talking to industry and funding agencies!!!
- How we can learn from our colleagues in the US? Asia? Latin America?

There is no free lunch…

- Need to work in between the workshops – we can't just talk!
- Nominate architect(s) from each community
- Join the CERN email list on FedID!

Follow up workshop rotating between user communities:

- November 2-3, 2011: Rutherford Appleton Lab, Oxford, U.K.
  Spring 2012, Summer 2012, … (volunteers?)

Next Steps

Develop a roadmap we can all agree to

- Identify a few key use cases
- Essential before talking to industry and funding agen
- How we can learn from our colleagues in the US

There is no free lunch…

- Need to work in between the workshops – we c
- Nominate architect(s) from each community
- Join the CERN email list on FedID!

Follow up workshop rotating between user communities:

- November 2-3, 2011: Rutherford Appleton Lab, Oxford, U.K.
- Spring 2012, Summer 2012, … (volunteers?)

Thank you.