




Sign in with your CERN account


Username or Email Address:

Password:

*Reminder: you have agreed to comply with the CERN computing rules*

Remember Username or Email Address

Sign in using your current Windows/Kerberos credentials [autologon] 

Sign in using your Certificate [autologon] 



# CERN Workshop on Federate ID

## *Conclusions and Next steps*

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



# CERN's User Base

Stefan.Lueders@cern.ch — “CERN Workshop on Federate ID” — Internet2 Fall 2011 Member Meeting

## CERN's Mission:

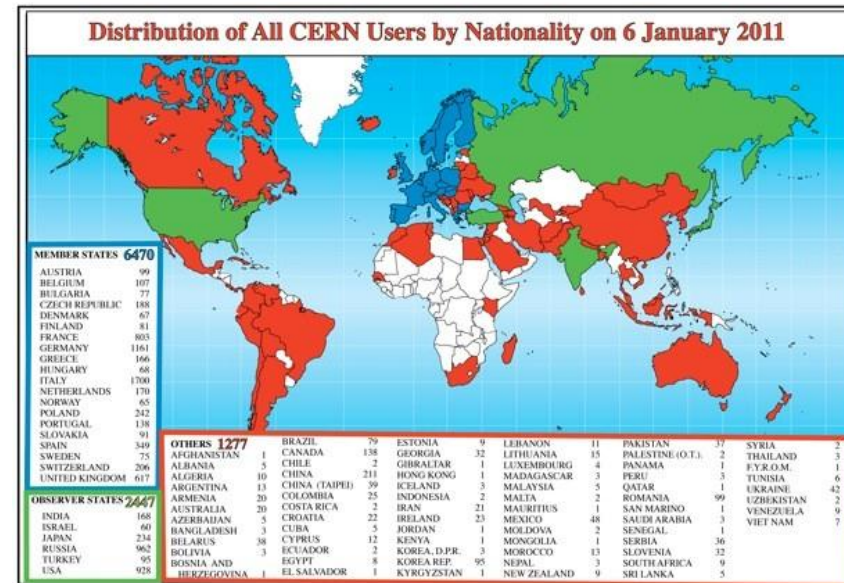
- ▶ Research: Seeking and finding answers to questions about the Universe
- ▶ Technology: Advancing the frontiers of technology
- ▶ Collaborating: Bringing nations together through science
- ▶ Education: Training the scientists of tomorrow

## 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)





# CERN's User Base

Stefan.Lueders@cern.ch — "CERN Workshop on Federate ID" — Internet2 Fall 2011 Member Meeting

## 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 per year)
- ▶ **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")
- ▶ Everyone with CERN affiliation can get an account (home & email)
- ▶ Large growth rate of new accounts
- ▶ Need for account very diverse (and not always clear)



## 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

Sign in with your CERN account


Username or Email Address:

Password:

*Reminder: you have agreed to comply with the CERN computing rules*

Remember Username or Email Address

Sign in using your current Windows/Kerberos credentials [autologon] 

Sign in using your Certificate [autologon] 

## 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 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/Resource Management

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

## Multi-factor Authentication

- ▶ Currently evaluating SmartChips, Yubikeys, GSMauth they already have one++ in the (HEP) community

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

Sign in with your CERN account

Username (CERN ID or email address):

Password:

Sign in

Remember Username or Email Address

Sign in using your current Windows/Kerberos credentials [autologon]

Sign in using your Certificate [autologon]

**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



# FedID for scientific collaborations

Stefan.Lueders@cern.ch — “CERN Workshop on Federate ID” — Internet2 Fall 2011 Member Meeting

## 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 9<sup>th</sup> & 10<sup>th</sup> 2011

- ▶ <https://indico.cern.ch/conferenceDisplay.py?confId=129364>

The screenshot shows the Indico interface for a conference titled "Federated identity system for scientific collaborations". The page is dated "9-10 June 2011" and is hosted by "CERN". The main content area displays a schedule for "The 09/06" (Friday, June 9th, 2011). The schedule includes the following sessions:

- 14:00: Welcome (HENNER, Frederic)
- 14:00 - 14:10: Introduction (JONES, Bob)
- 14:10 - 14:20: European photon/neutron facilities (WEYER, Heinz J)
- 14:20 - 14:40: CLARIN and the humanities (BROEDER, Dean)
- 14:40 - 15:00: WISE (WARTL, Roman)
- 15:00 - 15:20: Earth Science (Climate) (KESSELMAN, Philip)
- 15:20 - 15:40: Life Science (ELIXIR) (Paper)
- 15:40 - 16:00: Federated Identity in the Earth Science Domain (Slides)
- 16:00: Coffee break (Federated Identity in the Earth Science Domain)
- 16:00 - 16:45: EGI (NEWHOUSE, Steven)
- 16:45 - 18:00: Identity Management in Open Science Grid: Challenges, Needs, and Future Directions (ALTUNAY, Mine)
- 17:00 - 17:10: DESA/PRACE (RIBAUILLER, Vincent)
- 17:10 - 17:15: CLlogon: Federated Access to US Cyberinfrastructure (BASNEY, Jim)
- 17:15 - 17:30: GEANT (HOWLETT, Joshua)
- 17:30 - 17:45: Terena Certificate Service (GROPP, David)
- 17:45 - 18:00: EMI (WHITE, John White)

## 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

# FedID for scientific collaborations

Stefan.Lueders@cern.ch — “CERN Workshop on Federate ID” — Internet2 Fall 2011 Member Meeting

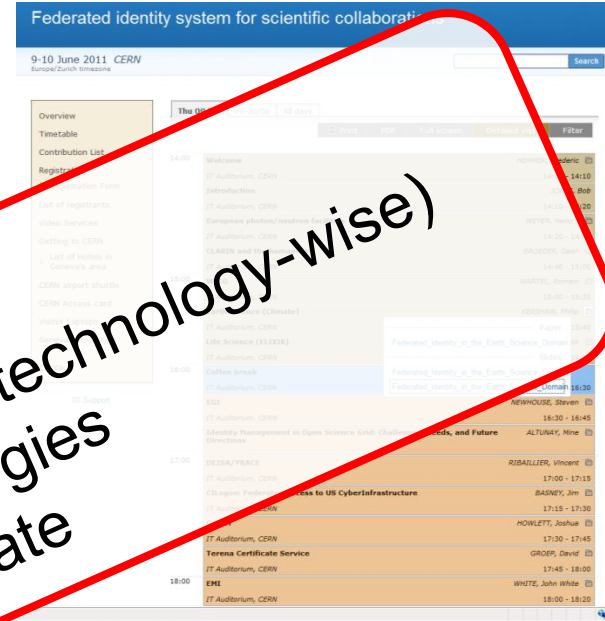
## Triggered by the EIROforum

(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 9<sup>th</sup> & 10<sup>th</sup> 2011

- ▶ <https://indico.cern.ch/conferenceDisplay.py?confId=129364>



**We are not alone!**

**85 participants from 44 organizations in 18 countries**

▶ BELNET, CERN, CSCS, ANTEDES, EGI, GEANT, ICRC, INFN, PSI, TERENA, ...

**Talks from various areas:**

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

# Comparison

Stefan.Lueders@cern.ch — “CERN Workshop on Federate ID” — Internet2 Fall 2011 Member Meeting

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



## 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?

## 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?)

## 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 IIS

## There is no free lunch...

- ▶ Need to work in between the workshops – we can't wait
- ▶ 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: ... (volunteers?)
- ▶ Summer 2012, ... (volunteers?)

**Thank you.**

