# FIRST INDICO WORKSHOP

27-29 MAY 2013 CERN

## Authentication

Alberto Resco Pérez

# AUTHENTICATION

**What is it:** Authentication is the act of confirming the truth of an attribute of a datum or entity.

Users needs to authenticate to access private resources

Support for different types of authentications

# AUTHENTICATORS

Currently we support 3 authenticators

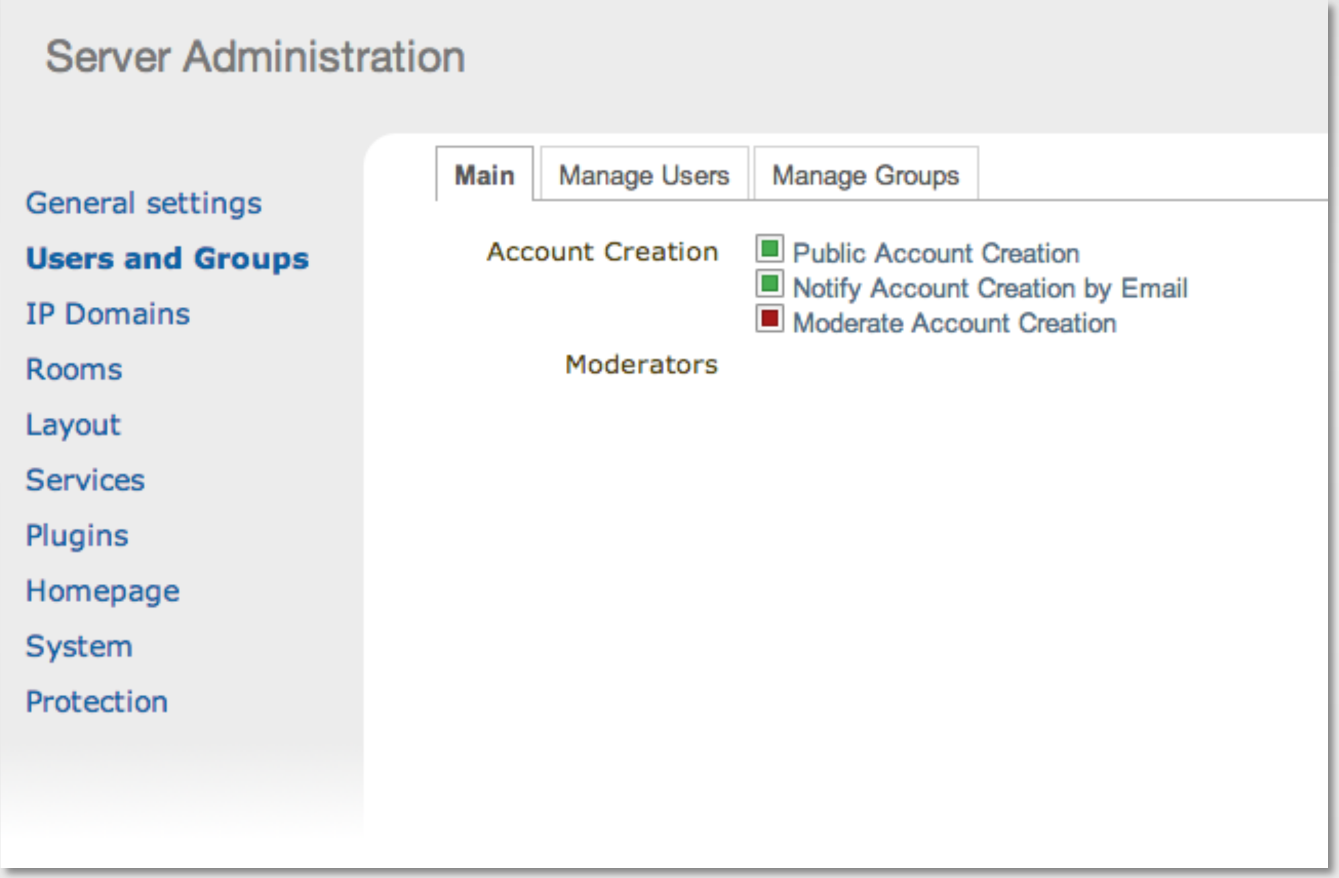
- Local
- NICE → CERN specific
- LDAP (developed by Martin Kuba)

# LOCAL AUTHENTICATOR

## Basic authentication

- Bases in a pair username/password
- Capability to create accounts
- Stored locally

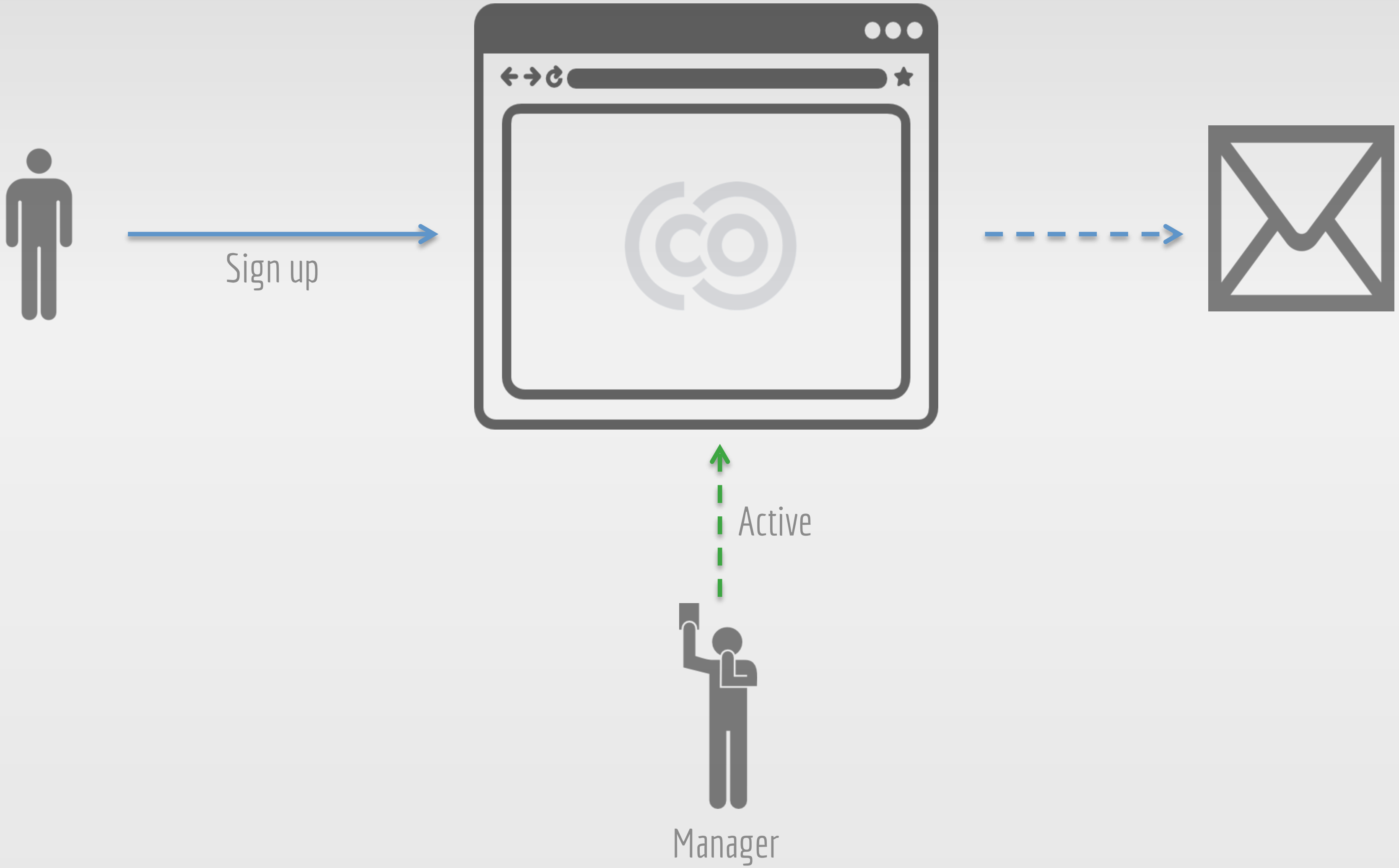
# ADMINISTRATION



Account Creation
- 🟩 Public Account Creation
- 🟩 Notify Account Creation by Email
- 🟥 Moderate Account Creation

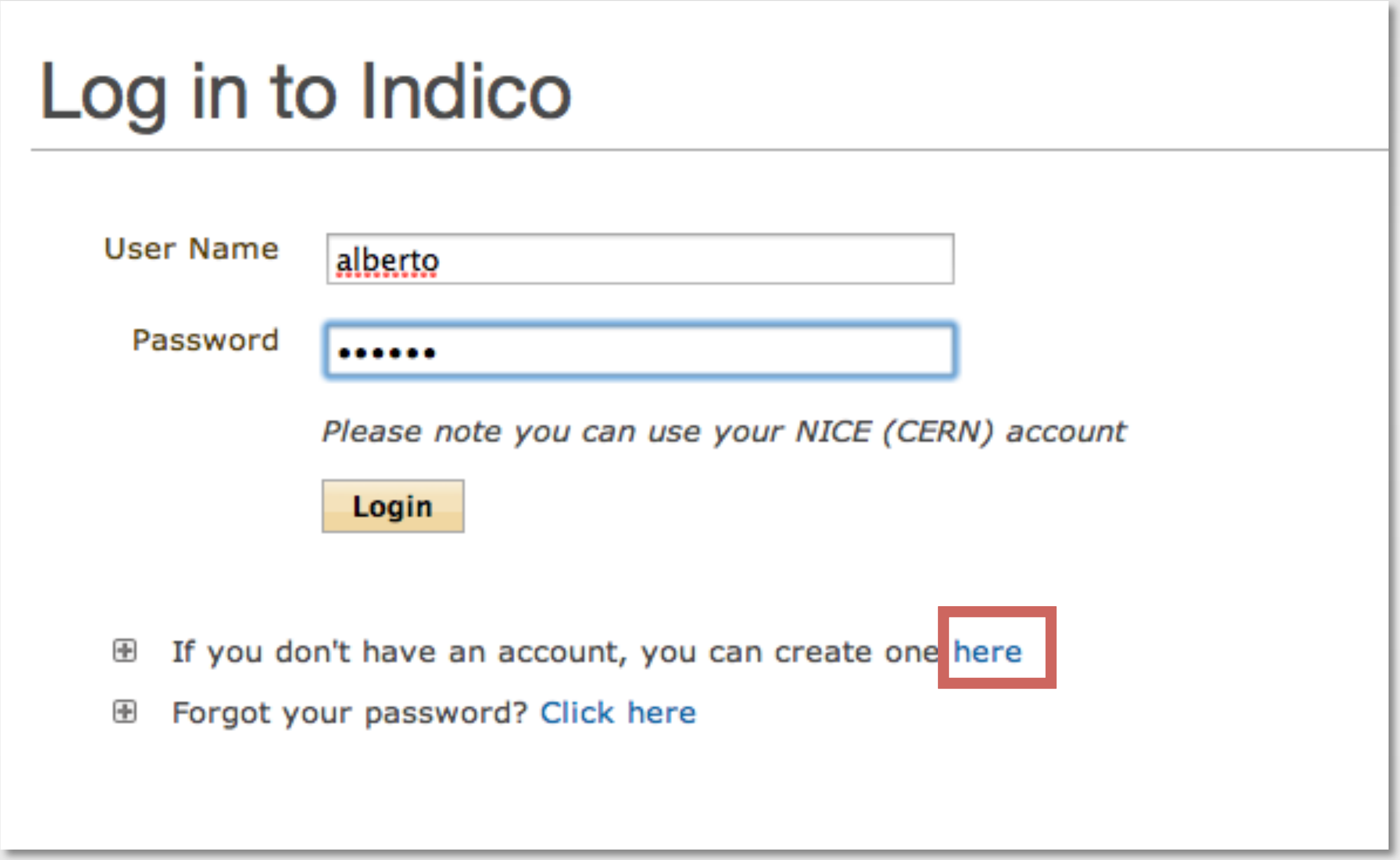
Moderators

# LOCAL



# LOCAL

## Login



### Log in to Indico

User Name: alberto

Password: ••••••

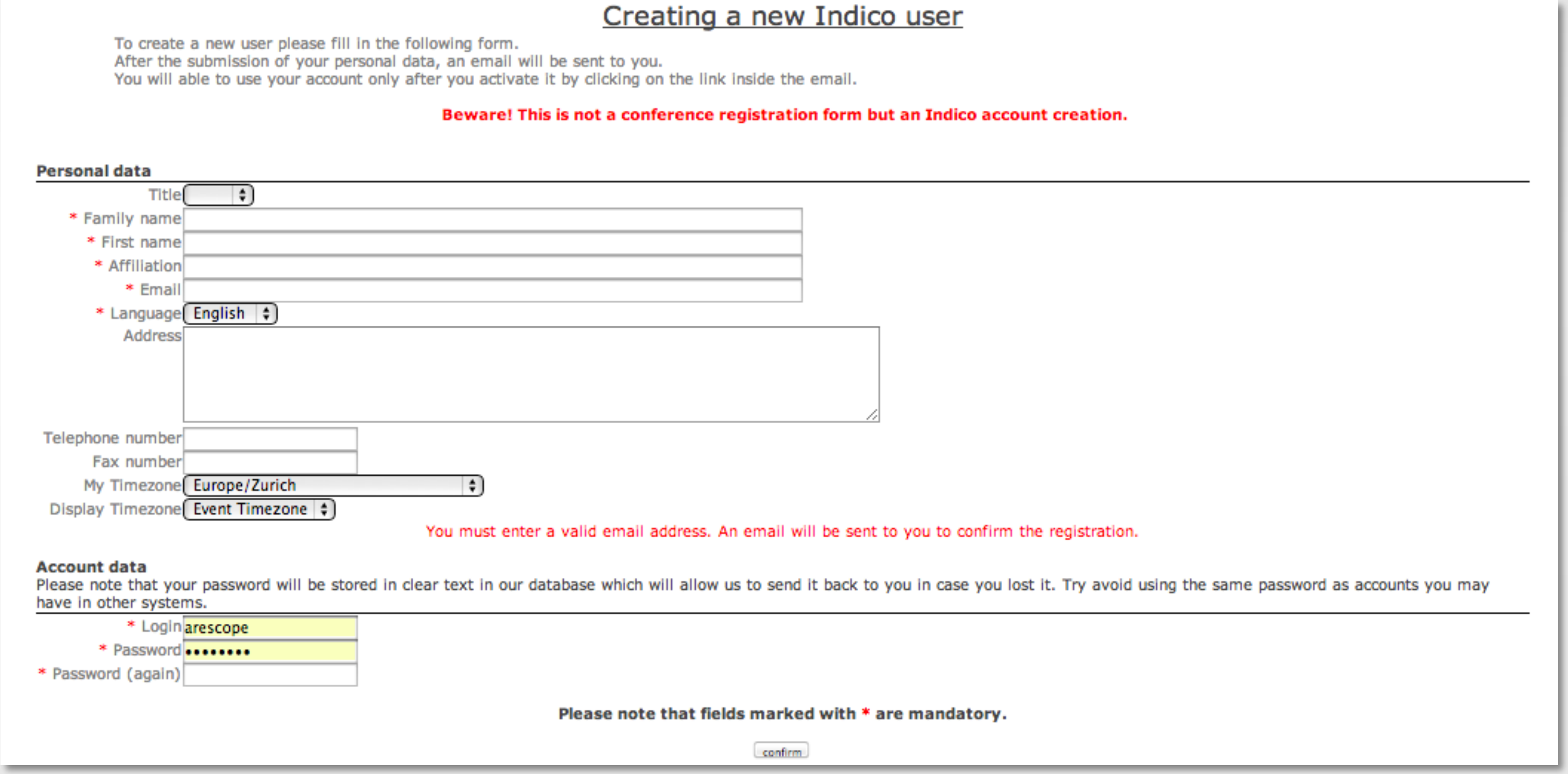
*Please note you can use your NICE (CERN) account*

⊞ If you don't have an account, you can create one here

⊞ Forgot your password? Click here

# LOCAL

## Create an account



### Creating a new Indico user

To create a new user please fill in the following form.
After the submission of your personal data, an email will be sent to you.
You will able to use your account only after you activate it by clicking on the link inside the email.

**Beware! This is not a conference registration form but an Indico account creation.**

**Personal data**

Title
* Family name
* First name
* Affiliation
* Email
* Language English
Address
Telephone number
Fax number
My Timezone Europe/Zurich
Display Timezone Event Timezone

You must enter a valid email address. An email will be sent to you to confirm the registration.

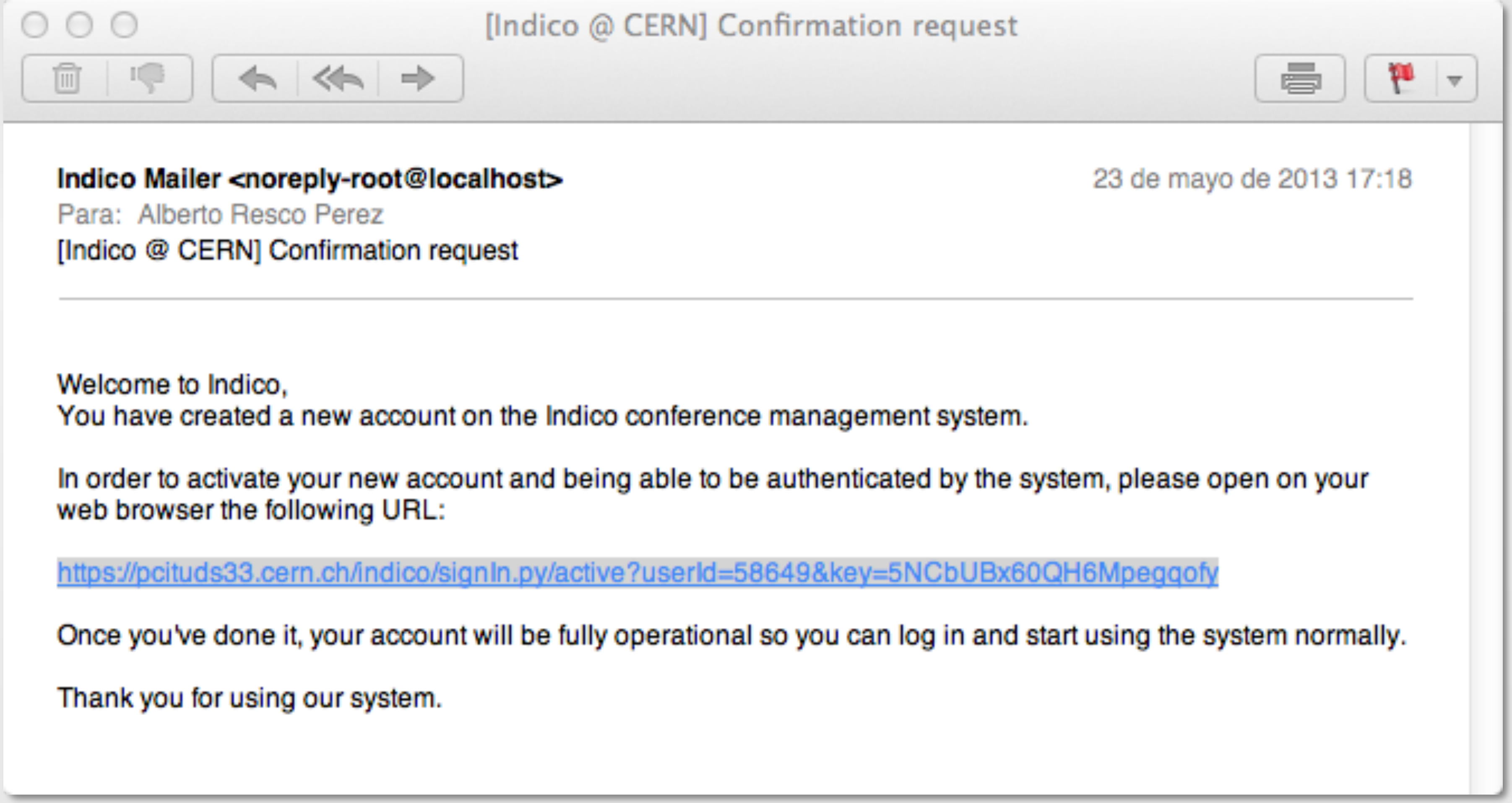
**Account data**
Please note that your password will be stored in clear text in our database which will allow us to send it back to you in case you lost it. Try avoid using the same password as accounts you may have in other systems.

* Login arescope
* Password ••••••••
* Password (again)

**Please note that fields marked with * are mandatory.**

# LOCAL

## Email confirmation



**Indico Mailer <noreply-root@localhost>** 23 de mayo de 2013 17:18

Para: Alberto Resco Perez

[Indico @ CERN] Confirmation request

Welcome to Indico,
You have created a new account on the Indico conference management system.

In order to activate your new account and being able to be authenticated by the system, please open on your web browser the following URL:

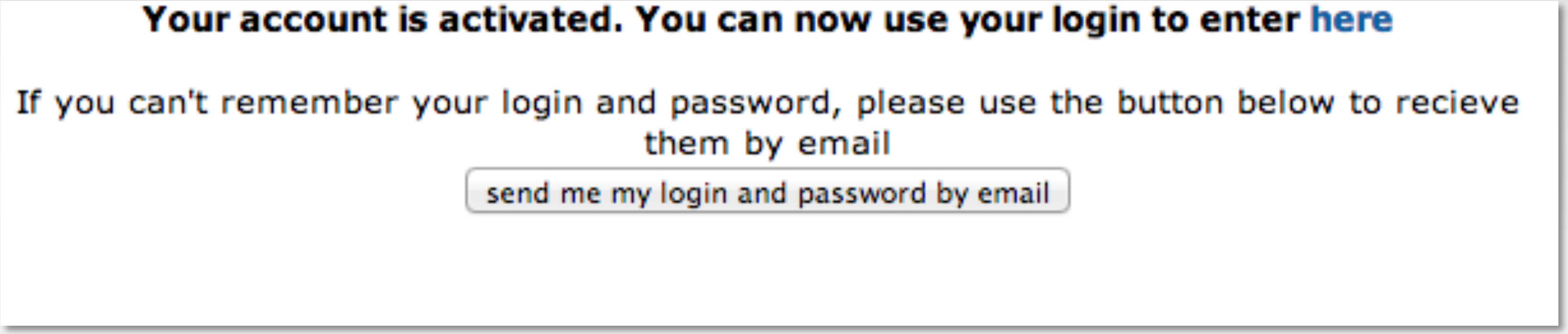
https://pcituds33.cern.ch/indico/signIn.py/active?userId=58649&key=5NCbUBx60QH6Mpeggofy

Once you've done it, your account will be fully operational so you can log in and start using the system normally.

Thank you for using our system.

# LOCAL

## Activation confirmation

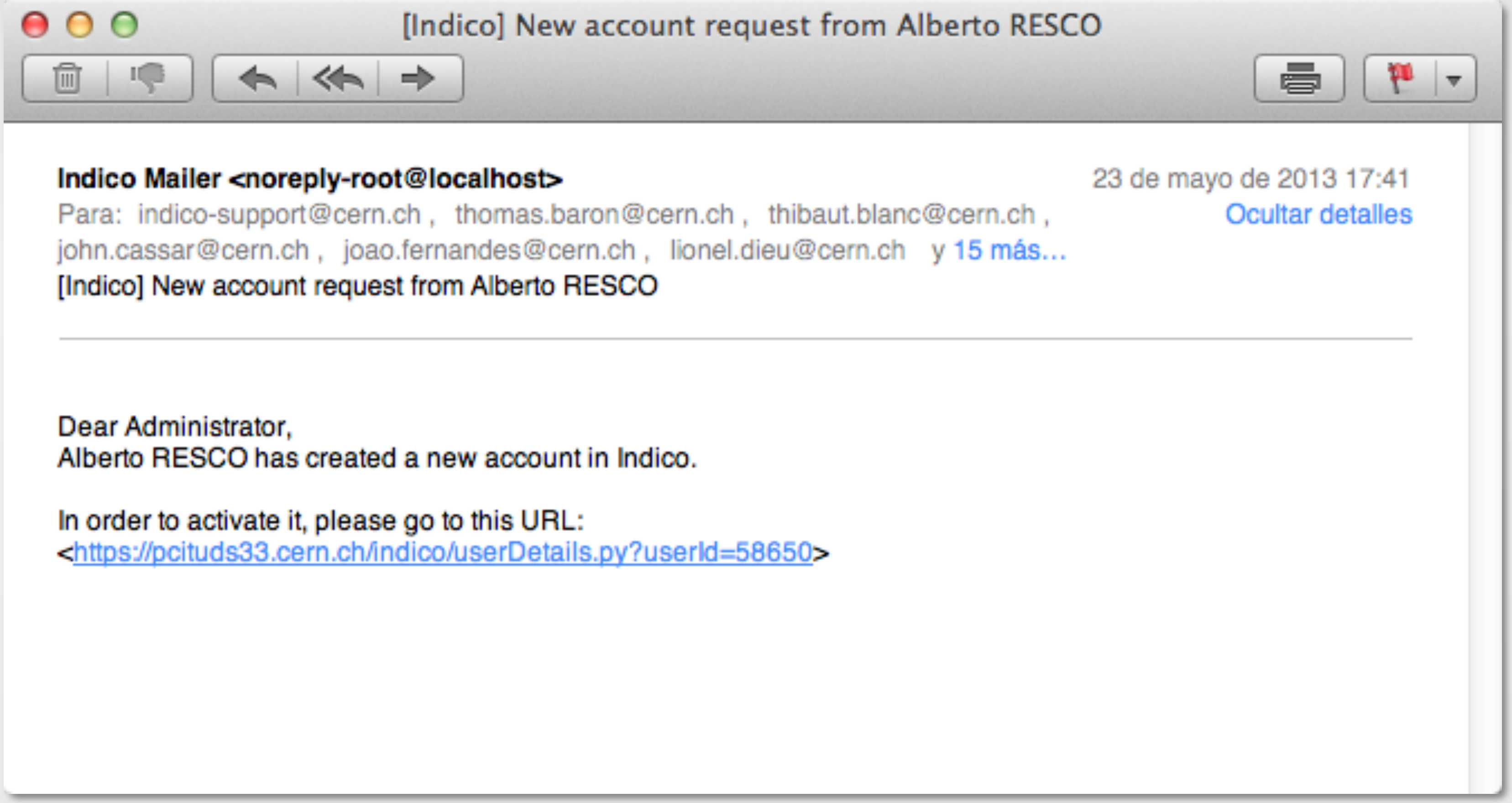


**Your account is activated. You can now use your login to enter here**

If you can't remember your login and password, please use the button below to recieve them by email

# LOCAL

## Account moderation



[Indico] New account request from Alberto RESCO

**Indico Mailer <noreply-root@localhost>**

23 de mayo de 2013 17:41

Para: indico-support@cern.ch , thomas.baron@cern.ch , thibaut.blanc@cern.ch , john.cassar@cern.ch , joao.fernandes@cern.ch , lionel.dieu@cern.ch y 15 más…

Ocultar detalles

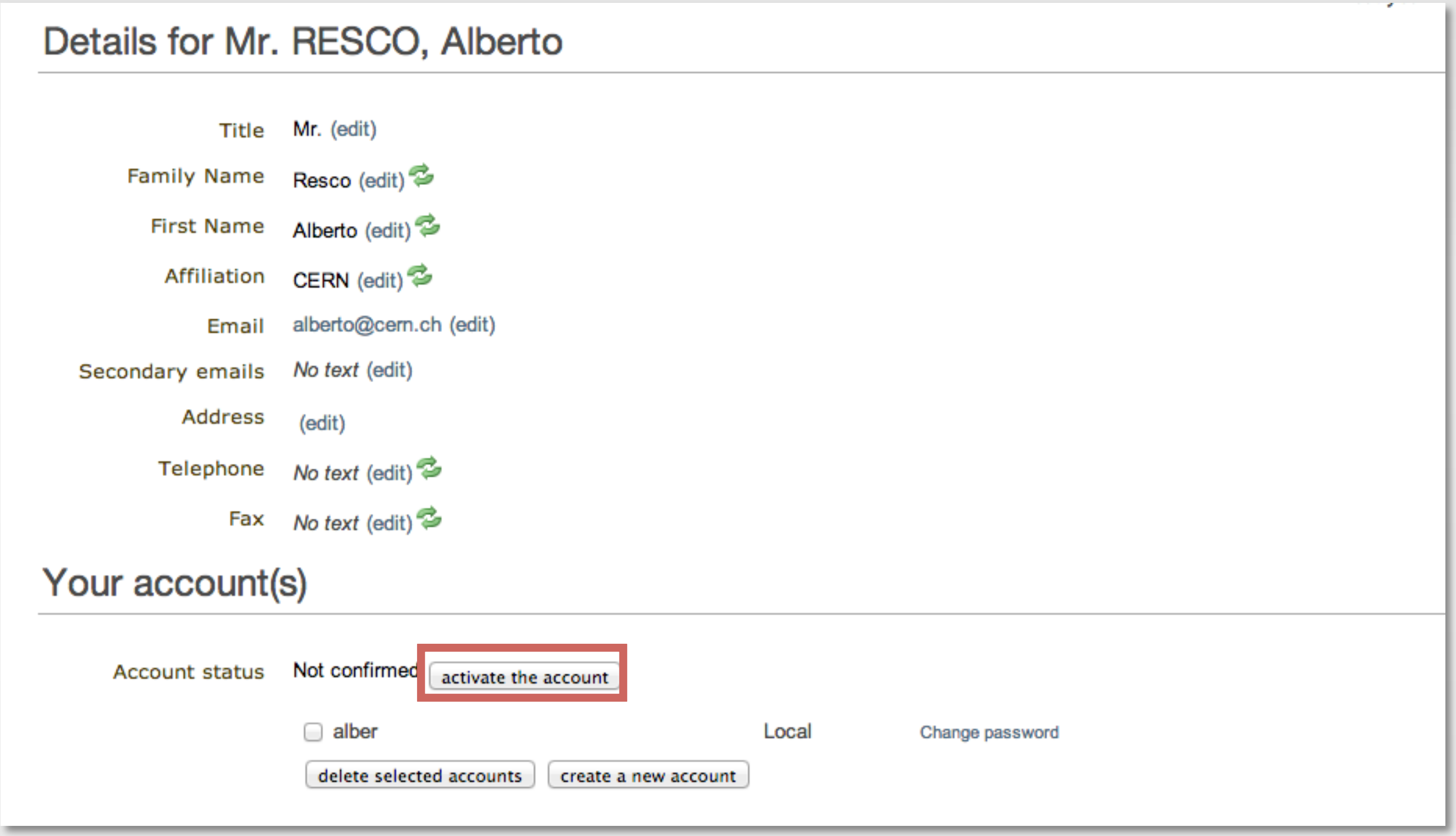
[Indico] New account request from Alberto RESCO

Dear Administrator,
Alberto RESCO has created a new account in Indico.

In order to activate it, please go to this URL:
<https://pcituds33.cern.ch/indico/userDetails.py?userId=58650>

# LOCAL

## Activate account



### Details for Mr. RESCO, Alberto

| | |
|---|---|
| Title | Mr. (edit) |
| Family Name | Resco (edit) |
| First Name | Alberto (edit) |
| Affiliation | CERN (edit) |
| Email | alberto@cern.ch (edit) |
| Secondary emails | *No text* (edit) |
| Address | (edit) |
| Telephone | *No text* (edit) |
| Fax | *No text* (edit) |

### Your account(s)

| | | | |
|---|---|---|---|
| Account status | Not confirmed | | |
| | □ alber | Local | Change password |

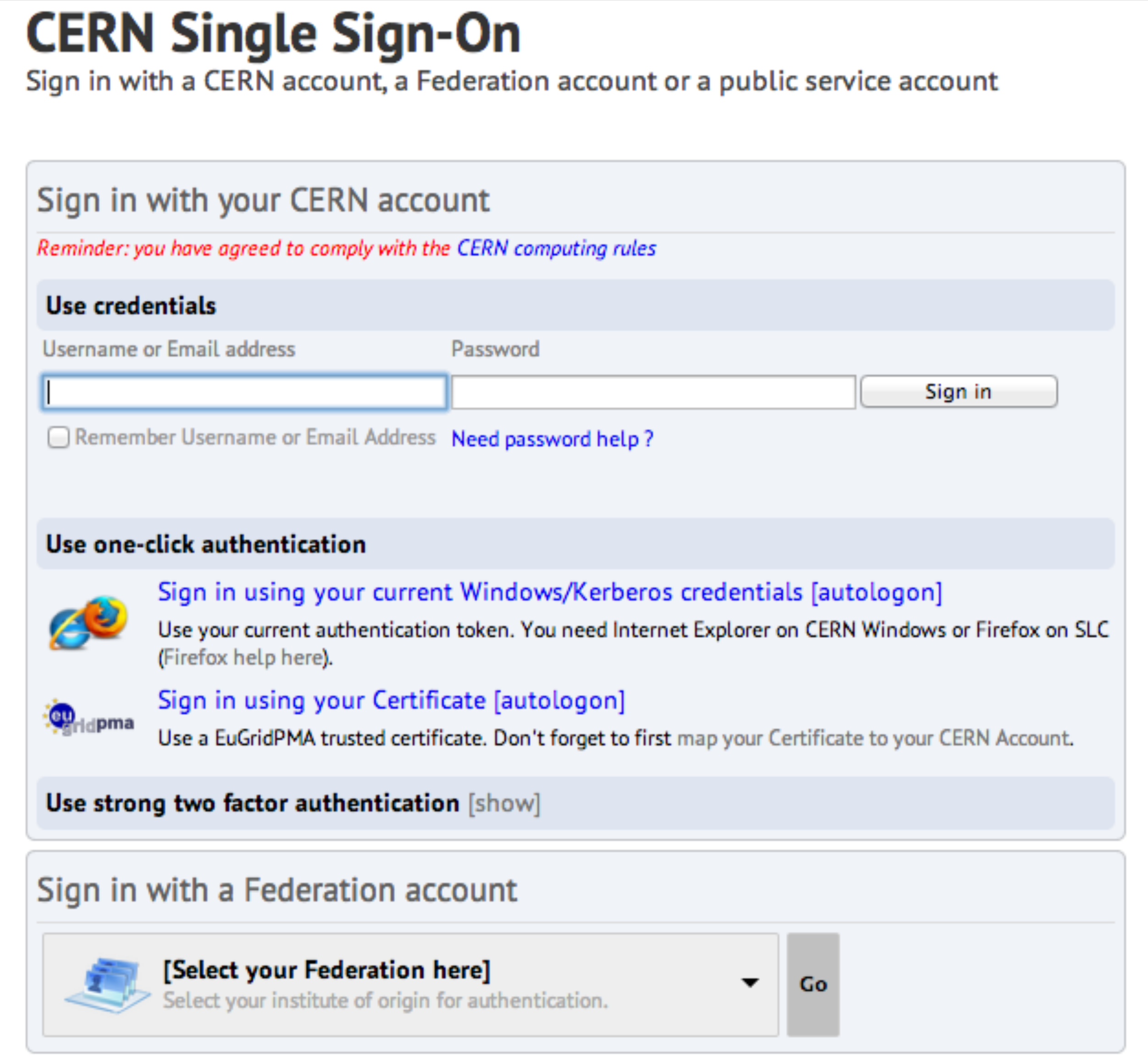
# NICE

## CERN Specific

- Web services to lookup for users and groups
- Single Sign On to login
- Sometimes very slow

# NICE

## Authentic



# CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

## Sign in with your CERN account

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

### Use credentials

Username or Email address

Password

□ Remember Username or Email Address

Need password help ?

### Use one-click authentication

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

Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC (Firefox help here).

Sign in using your Certificate [autologon]

Use a EuGridPMA trusted certificate. Don't forget to first map your Certificate to your CERN Account.

### Use strong two factor authentication [show]

## Sign in with a Federation account

**[Select your Federation here]**

Select your institute of origin for authentication.

# LDAP

LDAP is an application protocol for accessing and maintaining distributed directory information services

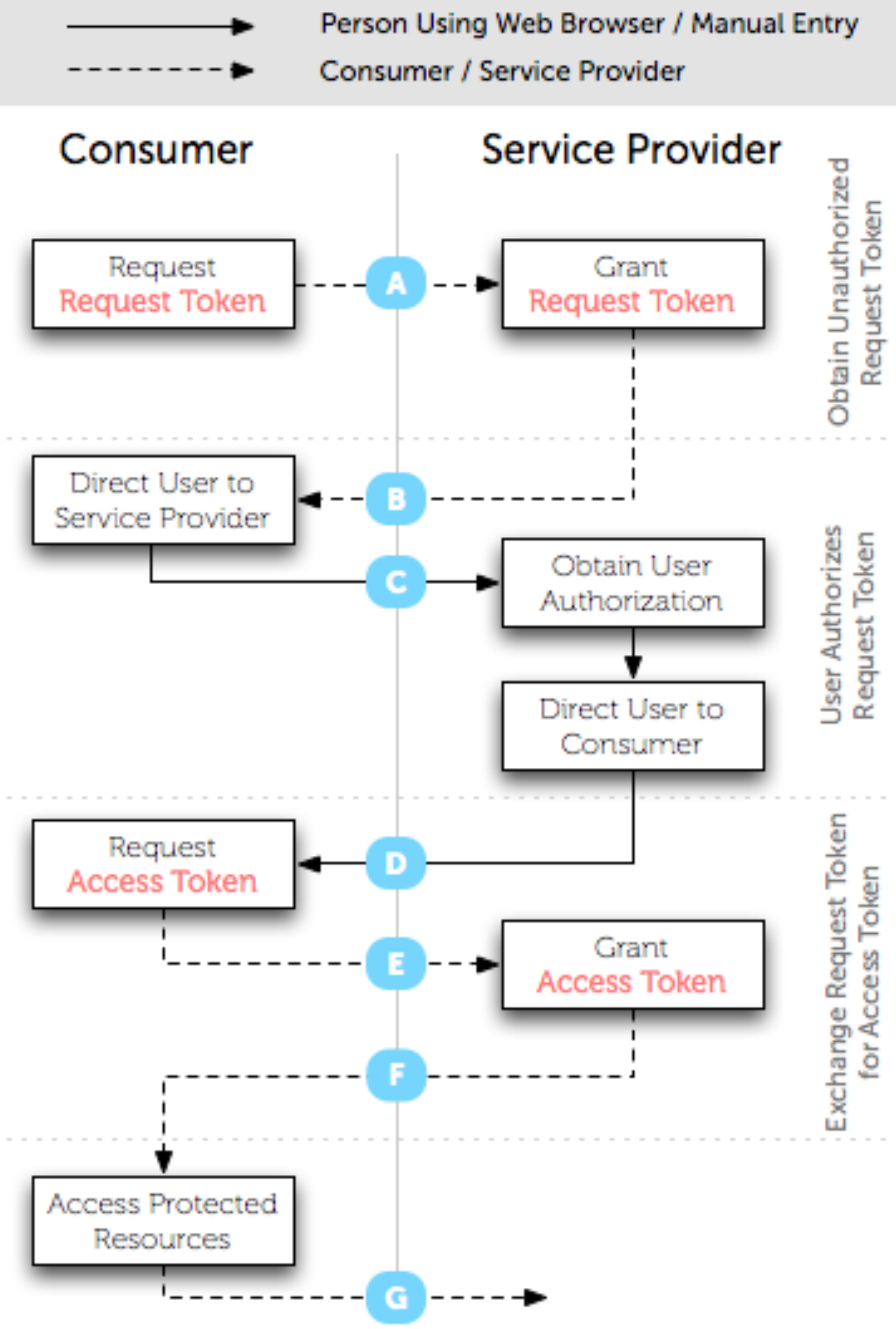
- Developed by Martin Kuba
- Benefit from a centralized directory you may have in your institution
- Indico@CERN: We can get rid of the webservices

# OAUTH

## Introduced in v1.1. Support for Oauth v1.0

- OAuth is an open standard for authorization.
- OAuth provides a method for clients to access server resources on behalf of a resource owner (such as a different client or an end-user).
- It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials (

# OAUTH AUTHENTICATION FLOW v1.0a



Person Using Web Browser / Manual Entry

Consumer / Service Provider

Consumer

Service Provider

Request Request Token

A

Grant Request Token

Obtain Unauthorized Request Token

Direct User to Service Provider

B

C

Obtain User Authorization

Direct User to Consumer

User Authorizes Request Token

Request Access Token

D

E

Grant Access Token

F

Exchange Request Token for Access Token

Access Protected Resources

G

### A Consumer Requests Request Token

Request includes
oauth_consumer_key
oauth_signature_method
oauth_signature
oauth_timestamp
oauth_nonce
oauth_version (optional)
oauth_callback

### B Service Provider Grants Request Token

Response includes
oauth_token
oauth_token_secret
oauth_callback_confirmed

### C Consumer Directs User to Service Provider

Request includes
oauth_token (optional)

### D Service Provider Directs User to Consumer

Request includes
oauth_token
oauth_verifier

### E Consumer Requests Access Token

Request includes
oauth_consumer_key
oauth_token
oauth_signature_method
oauth_signature
oauth_timestamp
oauth_nonce
oauth_version (optional)
oauth_verifier

### F Service Provider Grants Access Token

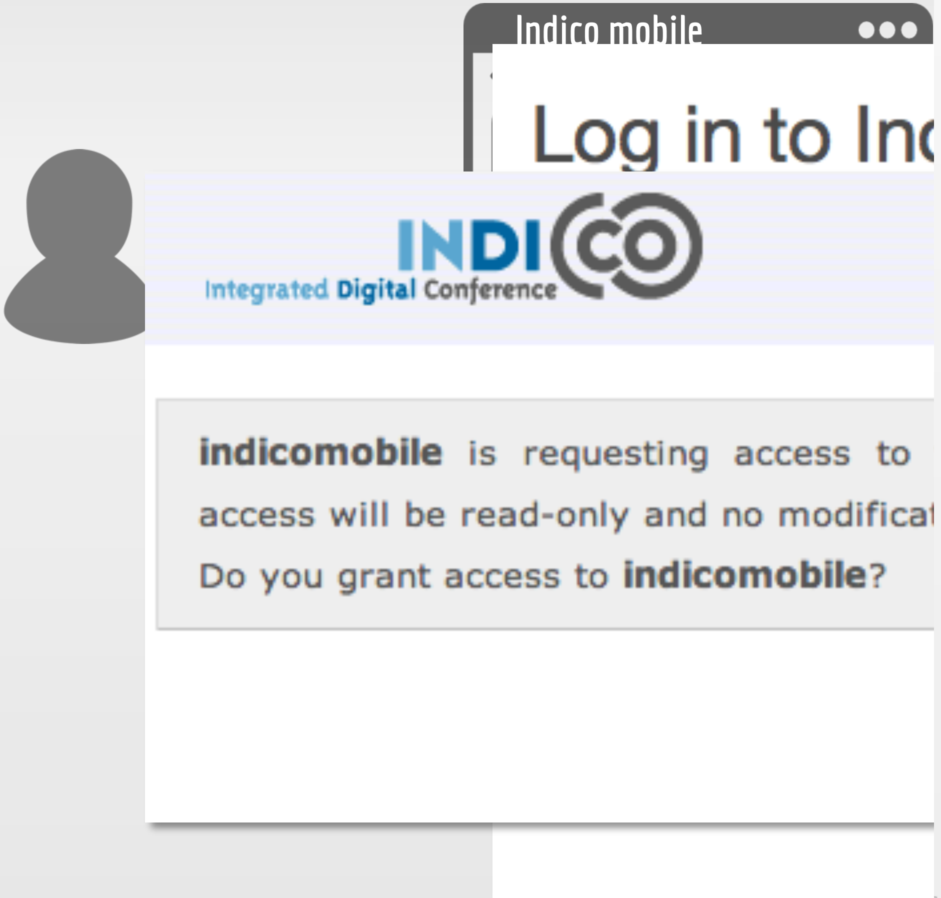
Response includes
oauth_token
oauth_token_secret

### G Consumer Accesses Protected Resources

Request includes
oauth_consumer_key
oauth_token
oauth_signature_method
oauth_signature
oauth_timestamp
oauth_nonce
oauth_version (optional)

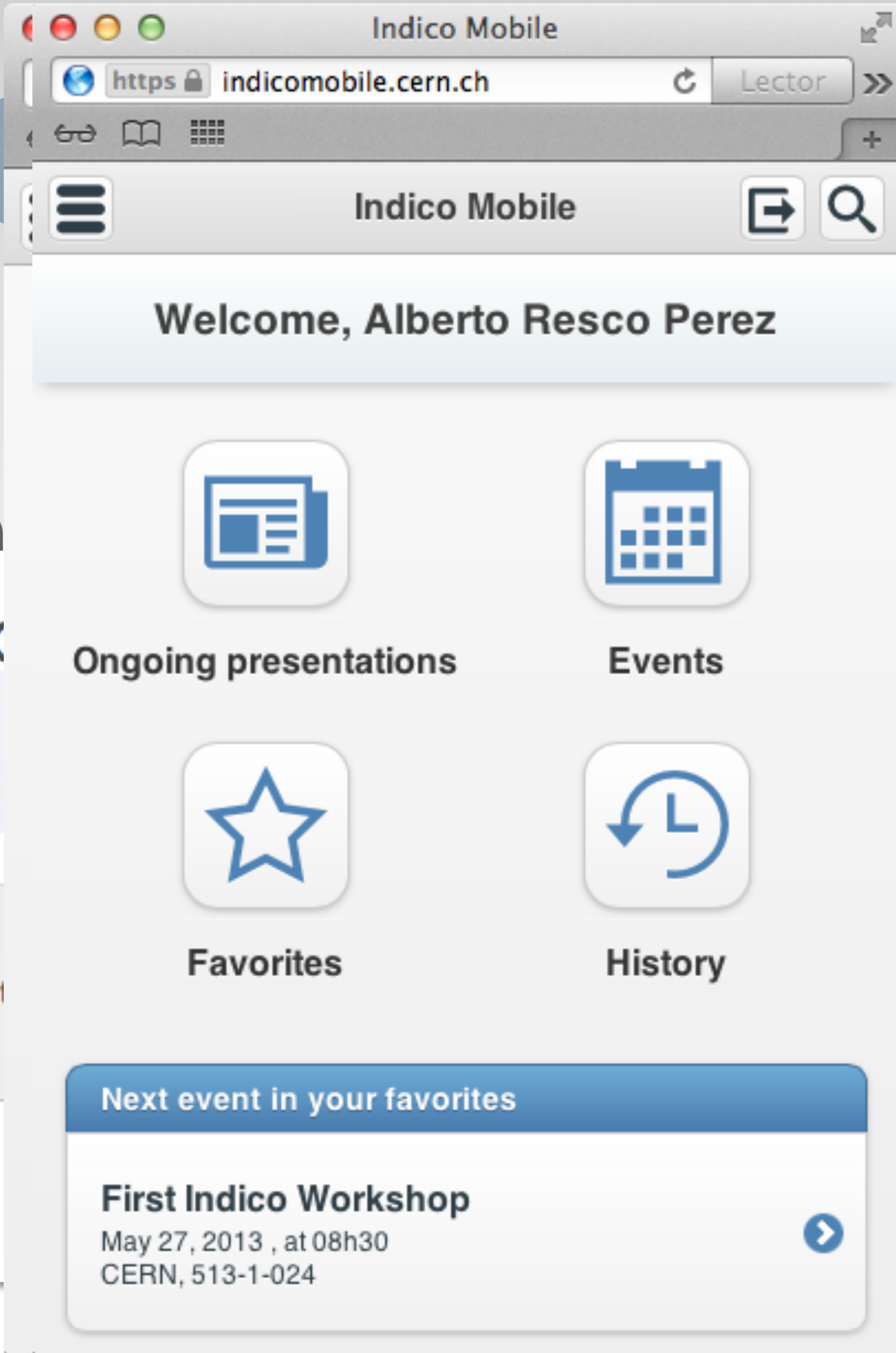
# INDICO MOBILE WO

## Authentication Workflow



Log in to Inc

**indicomobile** is requesting access to
access will be read-only and no modificat
Do you grant access to **indicomobile**?



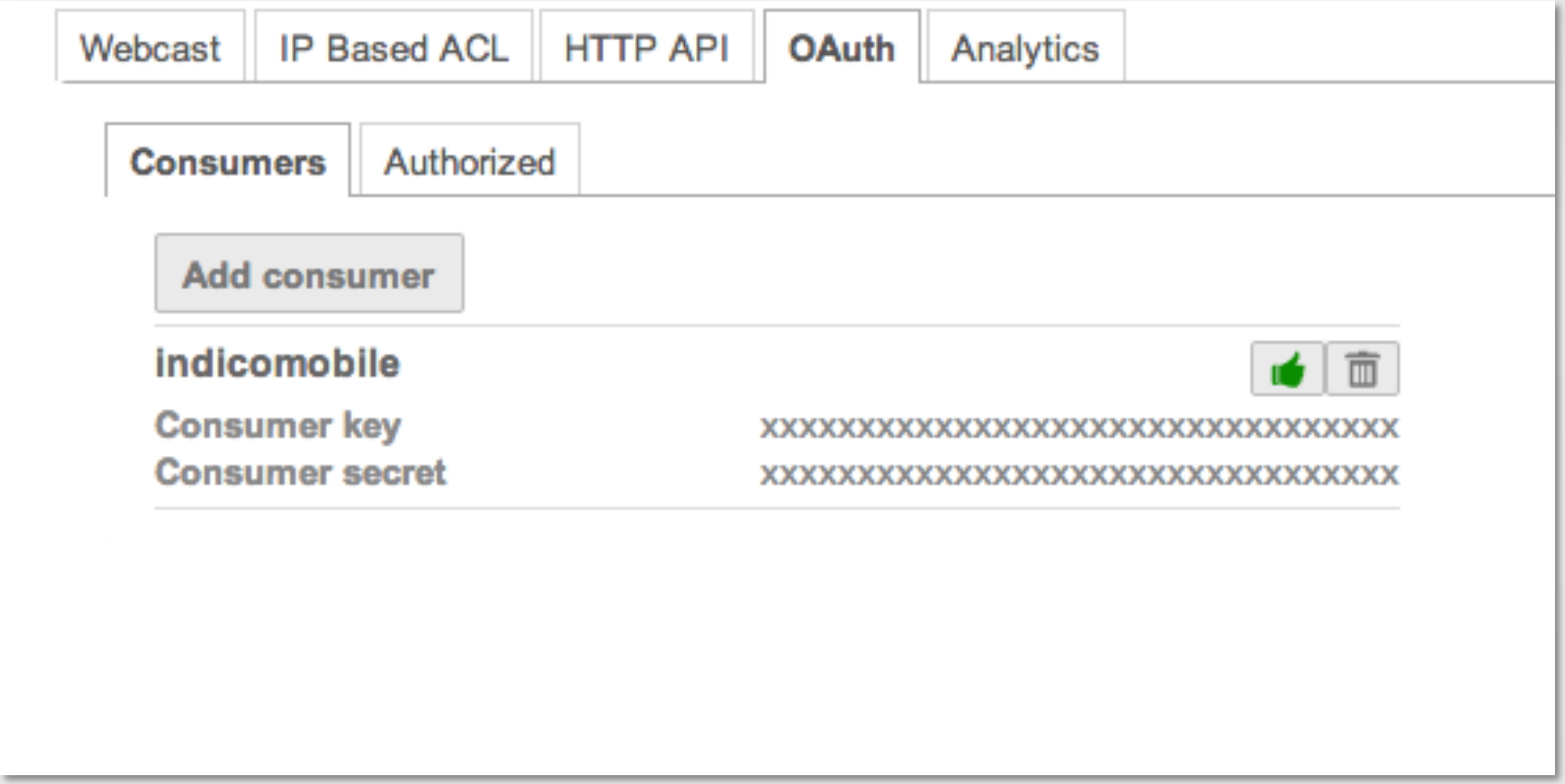
Welcome, Alberto Resco Perez

Next event in your favorites

**First Indico Workshop**
May 27, 2013 , at 08h30
CERN, 513-1-024

# OAUTH: ADMINISTRATION

## List of consumers

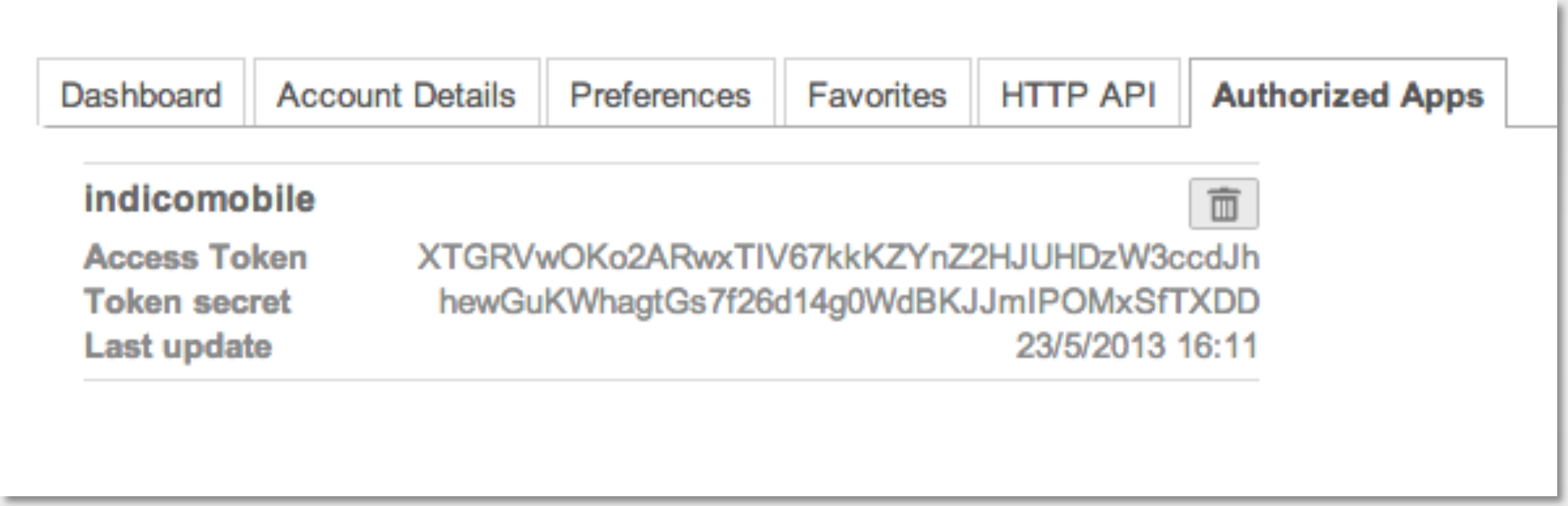


**indicomobile**

Consumer key xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Consumer secret xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

# OAUTH: USER APPLICATIONS

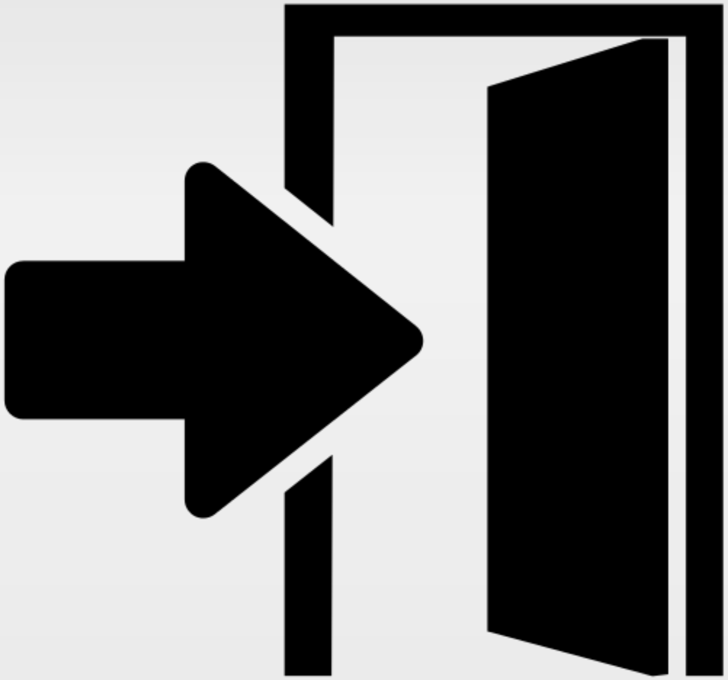
List of applications authorized



**indicomobile**

| | |
|---|---|
| **Access Token** | XTGRVwOKo2ARwxTIV67kkKZYnZ2HJUHDzW3ccdJh |
| **Token secret** | hewGuKWhagtGs7f26d14g0WdBKJJmIPOMxSfTXDD |
| **Last update** | 23/5/2013 16:11 |

# NEW AUTH SYSTEM



# NEW SYSTEM

## To be released in v1.2*

- Refactor of the code
- Get rid of NICE Authenticator
    - Easy to add new authenticators
    - Faster, cache
- SSO capabilities: it would only be a matter of configuration

# BASIC CONFIG

```
# etc/indico.conf

AuthenticatorList = [(’Local’, {})]
```

# CONFIGURE LDAP

```
# etc/indico.conf

AuthenticatorList = [(’LDAP',
   { 'host': 'cerndc.cern.ch',
     'useTLS': False,
     'peopleDNQuery': ('cn={0}’,'OU=Users,OU=Organic Units,DC=cern,DC=ch'),
     'groupDNQuery': ('cn={0}', 'OU=Workgroups,DC=cern,DC=ch'),
     'groupStyle': 'SLAPD’,
     'accessCredentials': ('CN=indico,OU=Users,OU=Organic
Units,DC=cern,DC=ch',’XXXXXXX’)})]
```

# ENABLE SSO

```
AuthenticatorList = [('MyAuthSystem',
                   { 'SSOActive': True,
                     'LogoutCallbackURL': 'https://example.com/wsignout’,
                     'SSOMapping' = {'email': 'ADFS_EMAIL',
                                      'login': 'ADFS_LOGIN',
                                      'personId': 'ADFS_PERSONID’,
                                      'phone': 'ADFS_PHONENUMBER’,
                                      'fax': 'ADFS_FAXNUMBER',
                                      'lastname': 'ADFS_LASTNAME’,
                                      'firstname': 'ADFS_FIRSTNAME’,
                                      'institute': 'ADFS_HOMEINSTITUTE’}
})]
```

# DEMO LOGIN LDAP

# QUESTIONS?

## ALBERTO RESCO

http://github.com/arescope

🐦 @arescope

arescope@cern.ch