Invenio Authentication and Authorization

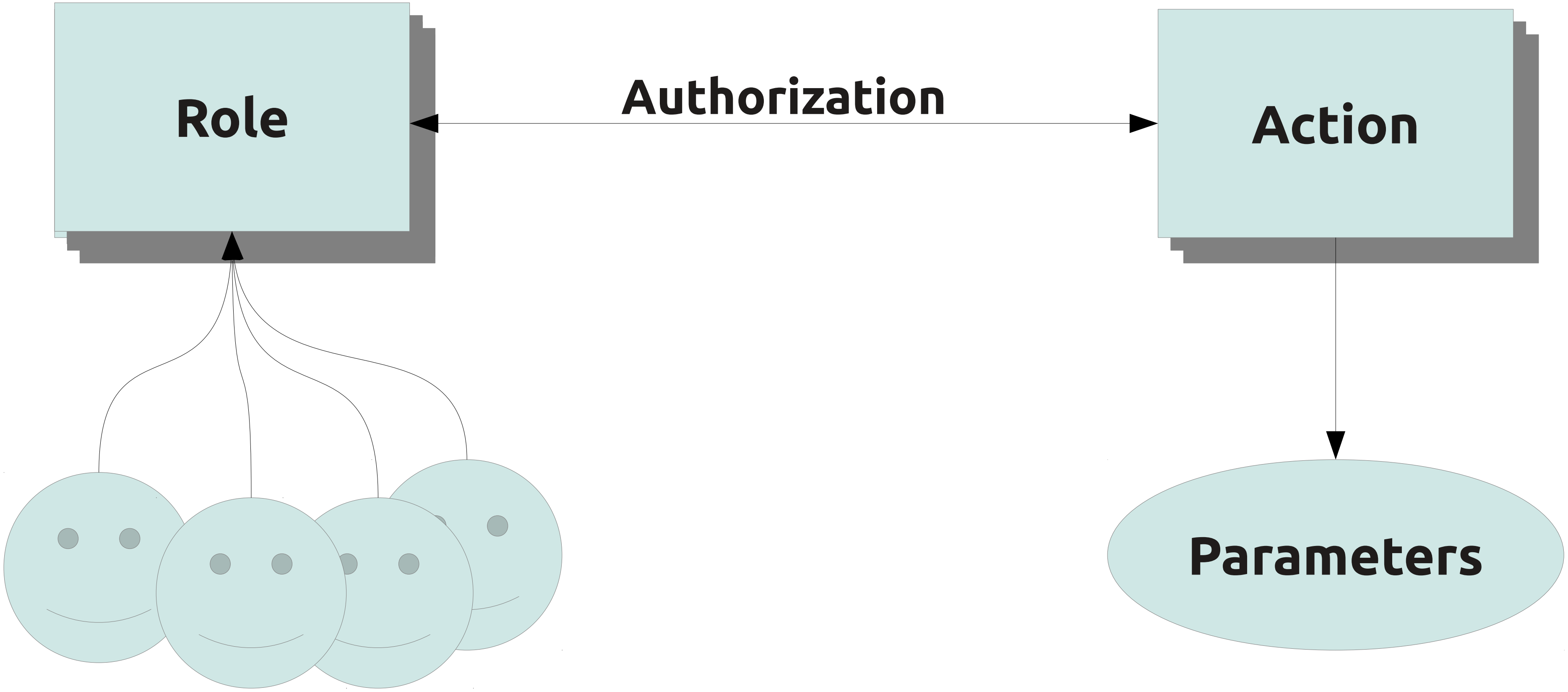
Samuele Kaplun

1st Invenio User Workshop 2012

Authentication

- Local accounts
- **LDAP** (thanks to Greg from EPFL :-))
- Shibboleth Single-Sign-On
- Proprietary Single-Sign-On
- More (plugin based. Feel free to contribute customized solutions)
- **Note:** external method can provide user details such as affiliations, address, group memeberships (see later with FireRole)

Authorization



Roles

- Set of users
  - Explicitly attached (one by one)
  - Implicitly attached (via FireRole)

Roles: FireRole

- Firewall Like Role Definition Language
- Let you attach users implicitly: e.g.
  - By IP address
  - By group membership
  - By other attributes (imported from an external authentication service, e.g. LDAP)

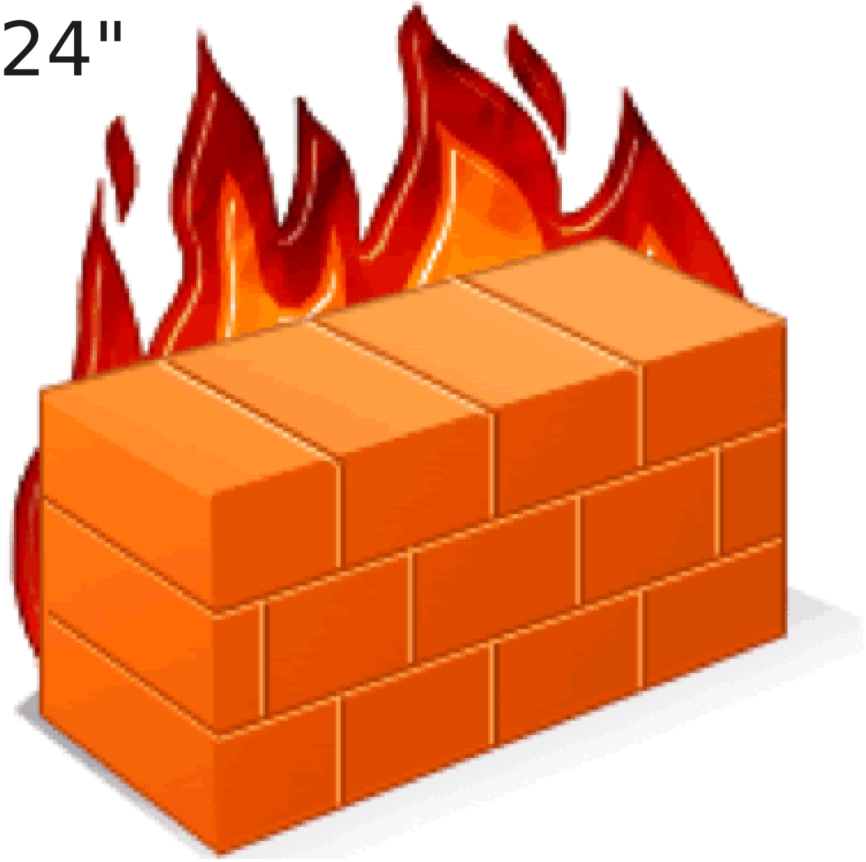
Roles: FireRole

allow not *email* /.*@gmail.com/,/.*@hotmail.com/

deny *group* badguys

allow *remote_ip* "127.0.0.0/24"

deny *until* “2012-06-06”



Actions

- One per admin tool (e.g. *cfgwebsubmit*)
- One per user tool (e.g. *usegroup*)
- Special one:
  - **submit**
  - **viewrestrcoll/viewrestrdoc**

Actions: submit

- **act**: to authorize for a specific action
- **categ**: to authorize for a specific category
- **doctype**: to authorize for a specific document type

*example1: **act**=SBI, **categ**=ARTICLE, **doctype**=DEMOART*

*example2: **act**=MIB, **categ**=*, **doctype**=**

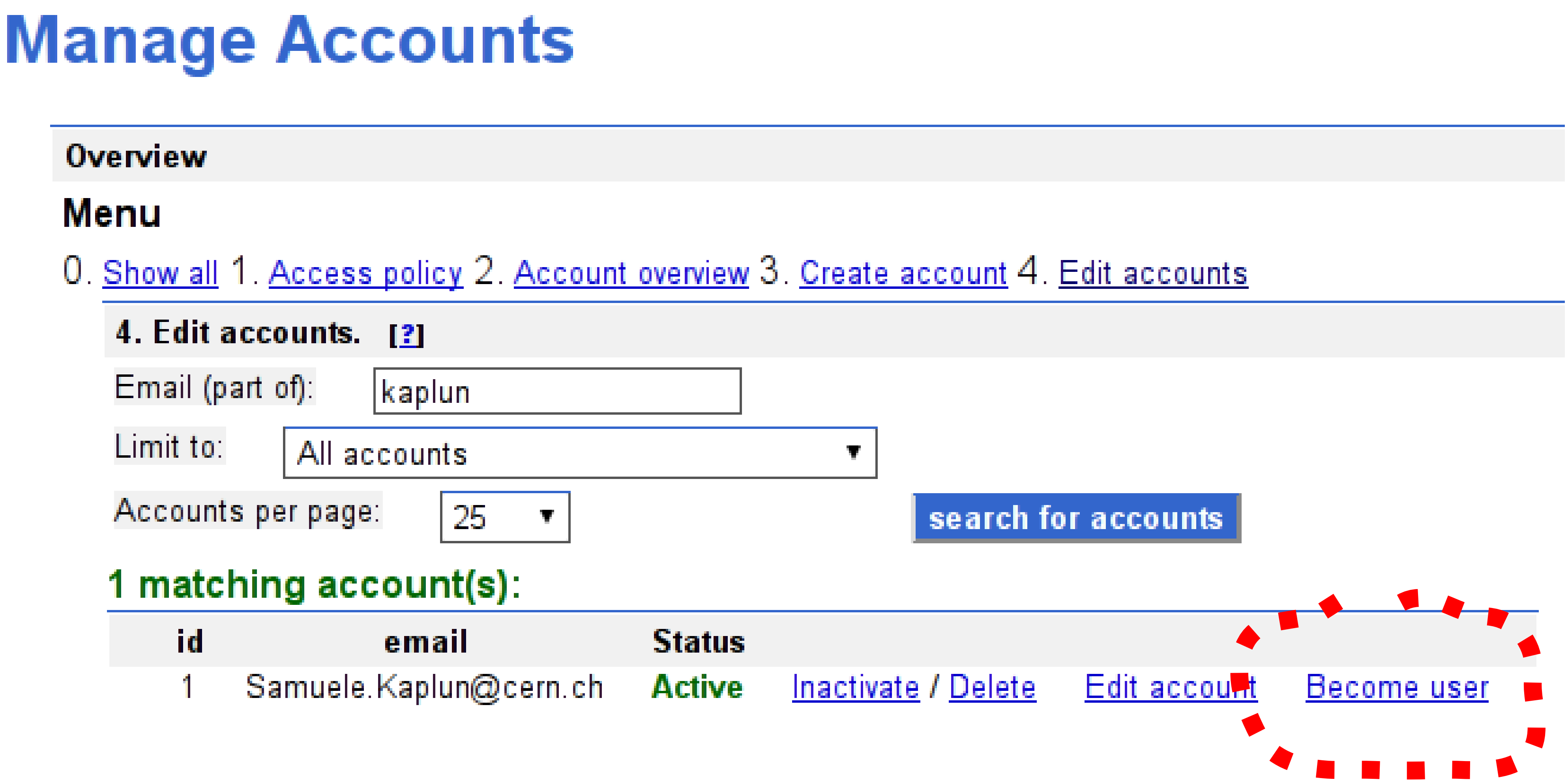
Actions: viewrestrcoll

- **collection**: name of the collection to authorize.
- **Note1:** If a collection is not explicitly mentioned in an authorization, then it's public!
- **Note2:** if a record belongs to many collections, a user must be authorized to **all** the restricted collections to which it belongs (a flag is introduced in 1.1 to choose instead for **any**)
- **Note3:** if a user **owns** a record, then she's authorized
- **Note4:** a new record is restricted to the world until webcoll has associated it to collections

Actions: viewrestrdoc

- **status:** arbitrary string that can be attached to a BibDoc (i.e. a document)
  - Such string should be specified in the *status* param of a bibdoc
  - This string can directly specify: an authorized email, group, role or firerole
  - The owner of a record can see the attached bibdocs regardless of the status

Debugging authorizations



Manage Accounts

Overview

Menu

0. Show all 1. Access policy 2. Account overview 3. Create account 4. Edit accounts

4. Edit accounts. [?]

Email (part of): kaplun

Limit to: All accounts ▼

Accounts per page: 25 ▼

1 matching account(s):

id	email	Status			
1	Samuele.Kaplun@cern.ch	Active	Inactivate / Delete	Edit account	Become user

Tuning WebAccess

- CFG_ACCESS_CONTROL_LEVEL_SITE
- CFG_ACCESS_CONTROL_LEVEL_GUESTS
- CFG_ACCESS_CONTROL_LEVEL_ACCOUNTS

see invenio.conf

Tips & Trick

- When upgrading from a previous version of Invenio, always run
  - *webaccessadmin –add –compile*

  in order to add new actions and default authorizations that have been introduced between two version
- Embargo can be implemented via **FireRole until** syntax

Summary

- Authentication + Authorization
- Role Based Access Control with FireRole
- Embargo