Greek Research and Technology Network

Authentication & Authorization Infrastructure

Faidon Liambotis
faidon@grnet.gr

February 22nd, 2011

Who am I?

- Servers & Services Engineer,
  Network Operations Center,
  Greek Research and Technology Network
- One of the “AAI people”
  (not exactly network, not exactly ops, but…)

grnet
Networking Research and Education

Greek Research and Technology Network

- aka GRNET
- The Greek NREN
- Public company providing Internet & computing services to the academic, research and educational community
- Part of the pan-European GÉANT network
- Part of the pan-European TERENA association
- Long history (10+ years) of cooperating with SEE countries
  - Networks: SEEREN, SEE-FIRE, SEE-LIGHT
  - Grid/HPC: SEE-GRID, HP-SEE, …

grnet
Networking Research and Education

Part I
about AAI

Why AAI?

- Not just AAI but *federated* AAI
- Single-Sign-On (SSO)
- Centralized point of policy enforcement
- User privacy/consent
- Transport security
- Eases service provisioning
- Facilitates *personalized* services

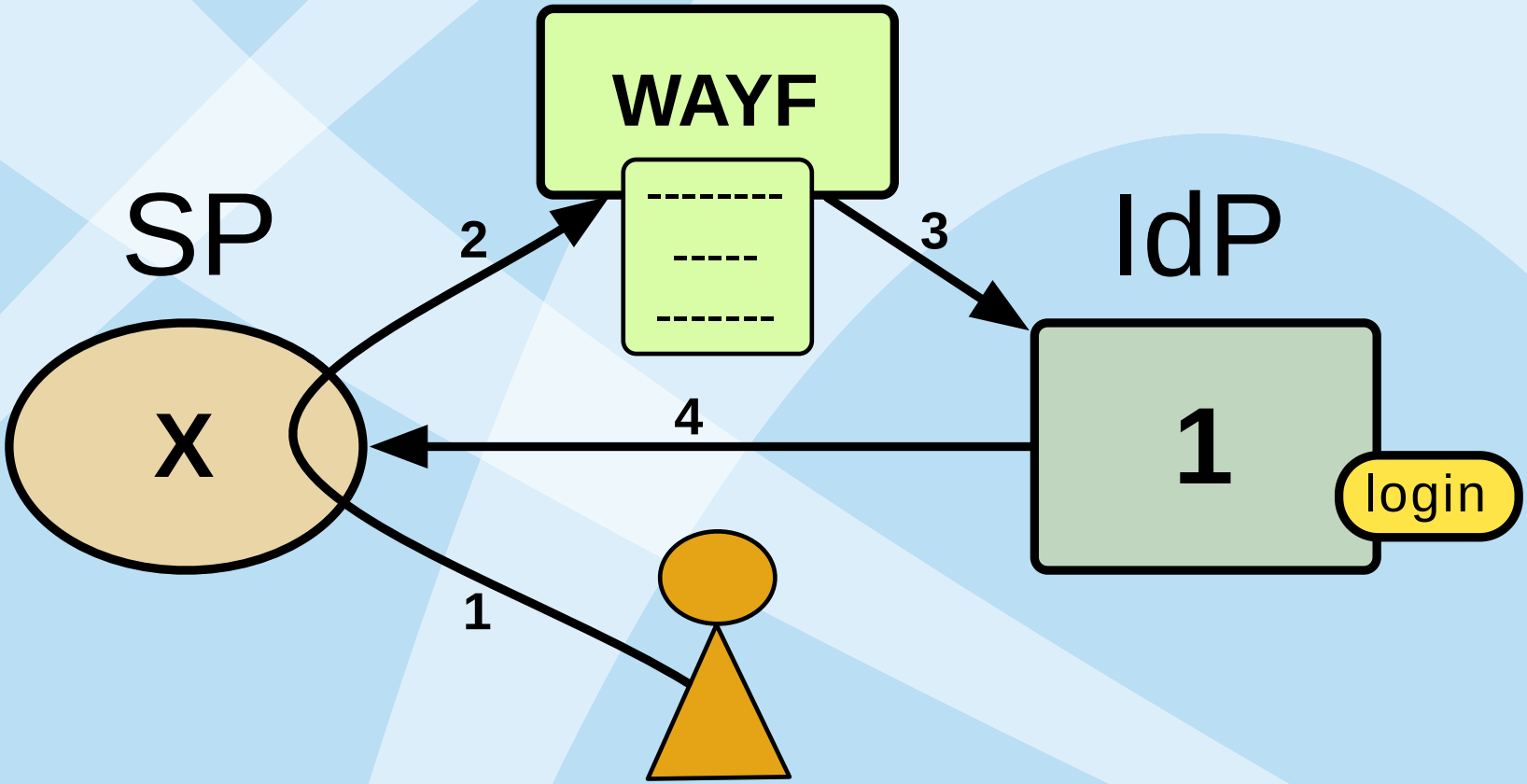
grnet
Networking Research and Education

The technology

- *The* standard in academic identity federations: **SAML** (Security Assertion Markup Language)
- An OASIS standard
- Used by Internet2 (USA), European NRENs, …
- Well into the commercial world too (Google, Microsoft ADFS, Oracle IdM etc.)
- Heavily tied to LDAP
  - Heavily recommended, almost a prerequisite

grnet
Networking Research and Education

Terminology



The software

- Shibboleth
  - The most popular one (by far)
  - http://shibboleth.internet2.edu/
  - Created by Internet2 (U.S.)
  - IdP: Java, needs Tomcat
  - SP: C++, Apache module
- SimpleSAMLphp
  - http://simplesamlphp.org/
  - Created by UNINETT (Norway)
  - Both IdP and SP
  - written, well¸ in PHP
- Others, too…

grnet
Networking Research and Education

Bootstrapping a federation

- I won't lie to you…
- AAI has a steep learning curve
- Complex and **hard** to deploy (properly)
- Also depends on proper IdM and hence operational *procedures*
- Non-trivial amount of time
- ~~It was a lot worse!~~
  It's getting better!

grnet
Networking Research and Education

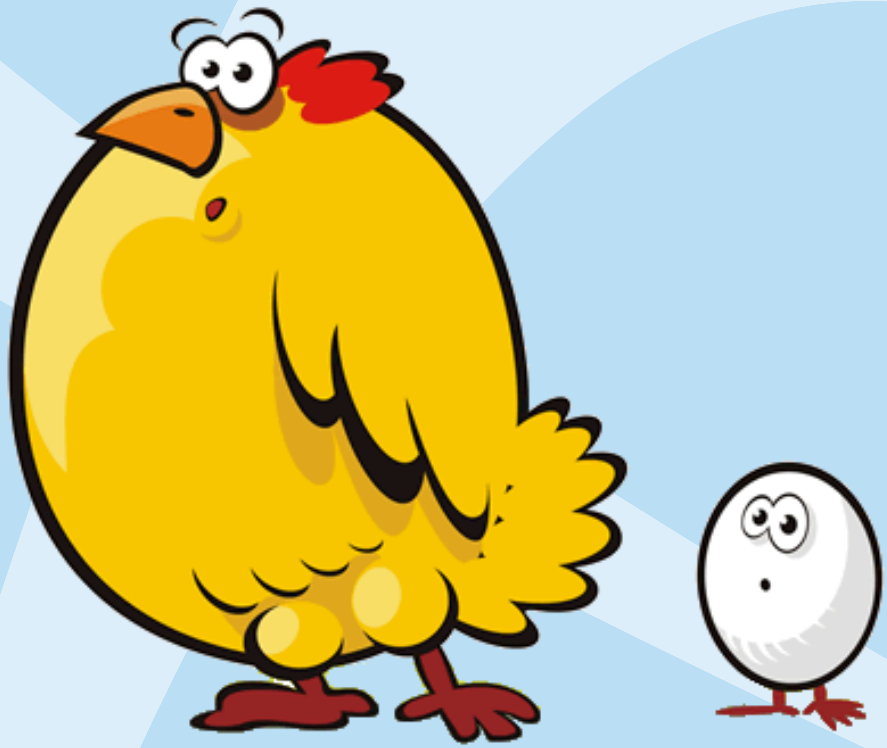
The problem

- IdPs have no incentive to spend that time without services
- SPs have no incentive to join without IdPs

grnet
Networking Research and Education

The problem

- IdPs have no incentive to spend that time without services
- SPs have no incentive to join without IdPs



grnet
Networking Research and Education

Solving the problem

- It's in everyone's interest (users & admins)
- Be proactive
  - You will do the work at some point anyway…
- Create demand
  - Federate existing services
  - Provide attractive new services *exclusively* federated
- Create a community
  - i.e. talk with each other :)
  - most of the issues will be common anyway

grnet
Networking Research and Education

Identity Management

- AAI pushes IdM to IdPs
  - that's a *good* thing!
- User identity life-cycle management
  - Provide users with a login when they enroll (automagically)
  - Expire old users
  - Implement password policies
  - Deal with identity theft
  - Deal with unique identifiers
  - …
- Synchronize with data sources (student offices etc.)

grnet
Networking Research and Education

It's *all* about IdM

grnet
Networking Research and Education

Settling on a schema

- The way you **encode** user information
  - givenName, sn, cn, displayName, mail, …
  - affiliation, user status, student ID, …
- You build services based on that
  - it can't be easily changed!
- SAML “schema” can be different than LDAP schema
- Internet2/EDUCAUSE's eduPerson
- TERENA's SCHAC *(SCHema for ACademia)*
- Usually not enough
  - e.g. student branch information is missing

grnet
Networking Research and Education

Part II
our experience

grnet
Networking Research and Education

GRNET as a service provider…

- …used to provide services to users *indirectly**
  - Mostly as an ISP
  - The rest were the universities' “domain”
- But: shifting to end-user services
  - Following the trend
  - It's all about “the Cloud”
- AAI is crucial to that goal!

grnet
Networking Research and Education

A bit of history

- Initial pilot by VNOC: late 2004
- SAML 1.1, Shibboleth 1.2
- Descendant of the “Directory Service” (LDAP)
- In production by 2005
- Very few initial members (largest universities)
- Even fewer services

grnet
Networking Research and Education

2006-2009: trying to break the loop…

- Idea no. 1: Document, have workshops, marketing
- Idea no. 2: the “Service Box Project”
  - Turn-key LDAP, RADIUS, Shibboleth IdP, demo SP
  - 1U servers, bought and operated by GRNET
  - More of a workaround than a solution
  - Gradually deployed 20 of them across Greece
- Idea no. 3: **“50GB free for everyone!”**

grnet
Networking Research and Education

2006-2009 cont'd

- Quickly expanded the federation to about 20 IdPs (≈30%)
- But…
  - No identity management (IdM) procedures
  - Very heterogeneous userbase
  - Problems were not being detected nor solved

grnet
Networking Research and Education

The 2010 expansion

- Ministry of Education project for textbook distribution (as in: *physical* distribution of paper textbooks)
- Participation is mandatory for **all** universities
- GRNET was chosen to implement the project
- We chose to leverage our AAI (naturally)
- Put pressure on everyone
  - Including us!
  - Chance of backfiring…
- But also got us funding :)

grnet
Networking Research and Education

The 2010 expansion cont'd

- From 30% to **100%** university coverage in **3** months!
- **Massive** cleanup of cruft
- Switched to SAML 2.0 exclusively
- Started using SCHAC and created grEduPerson
- Written a detailed Policy & Procedures document
- Established communication channels;
  Issues are found and resolved promptly

grnet
Networking Research and Education

The 2010 expansion cont'd

- From 30% to **100%** university coverage in **3** months!
- **Massive** cleanup of cruft
- Switched to SAML 2.0 exclusively
- Started using SCHAC and created grEduPerson
- Written a detailed Policy & Procedures document
- Established communication channels;
  Issues are found and resolved promptly
- **Huge** success!

grnet
Networking Research and Education

Current status

- **51** IdPs
- **44** higher education institutes/universities
- **6** research institutes
- **100%** of all undergraduate students (≈270.000)
- **10** federated services
  - …plus academic library providers

grnet
Networking Research and Education

Setup

- A loosely-coupled federation (vs. a hub-and-spoke one)
- …but with a central WAYF (developed in-house)
- IdPs: Shibboleth 2.x, all of them
- SPs:
  - most run Shibboleth 2.x
  - lately a couple of SimpleSAMLphp
  - plus some legacy Shibboleth 1.3

grnet
Networking Research and Education

Part III
our services

grnet
Networking Research and Education

Services

- Not a whole lot of them
- Mostly developed by GRNET
- Expecting more of them
  - We *just* broke the loop!
- *Developing* more of them
- Core part of the company's strategy

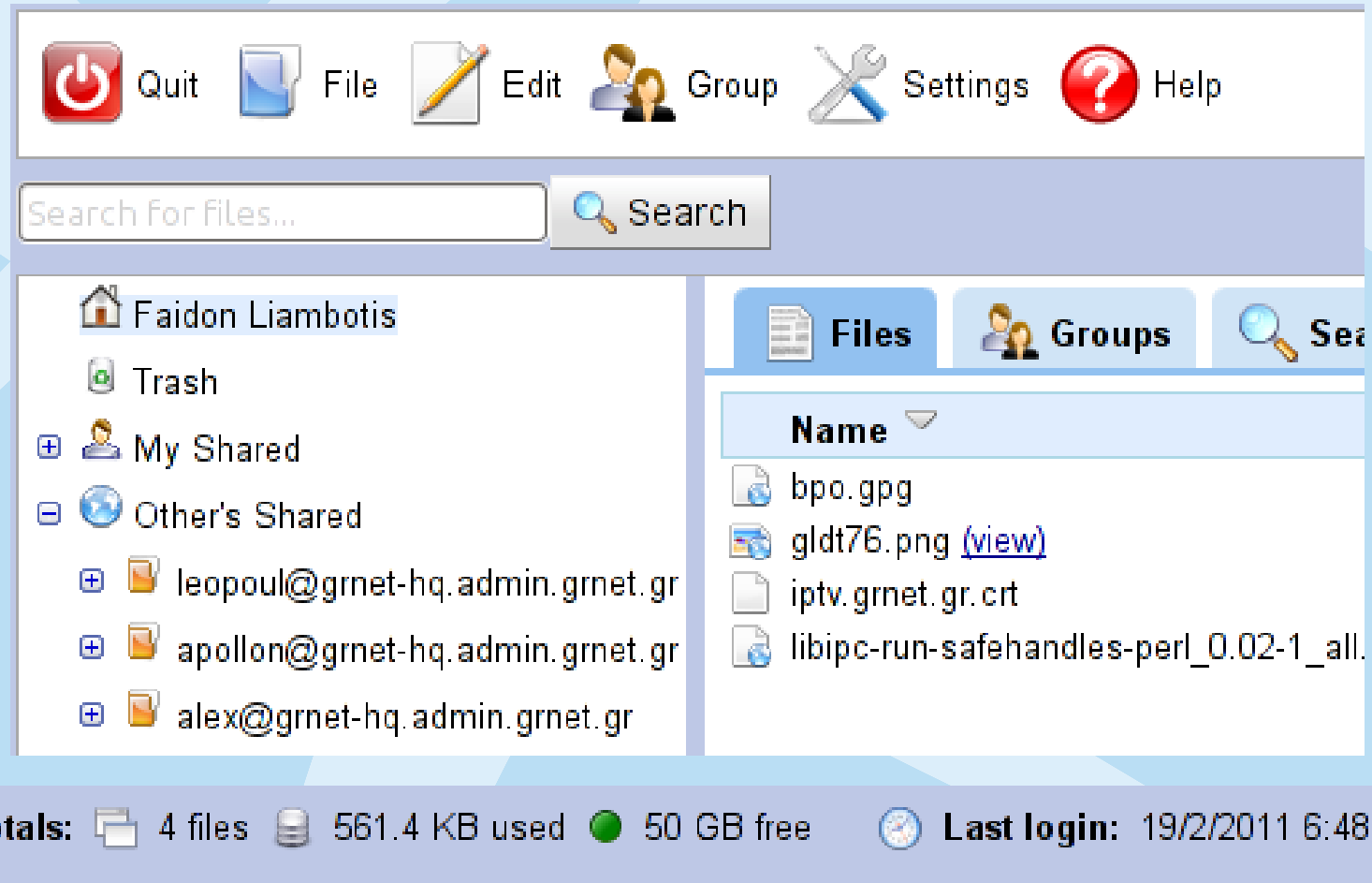
grnet
Networking Research and Education

Services: Pithos

- Storage-as-a-service
- Web GUI, RESTful API, WebDAV
- 50GB free for everyone
- Users can *share* files with each other
- Using the federation exclusively
- Open-source software, developed in-house
  http://code.google.com/p/gss/

grnet
Networking Research and Education

Services: Pithos



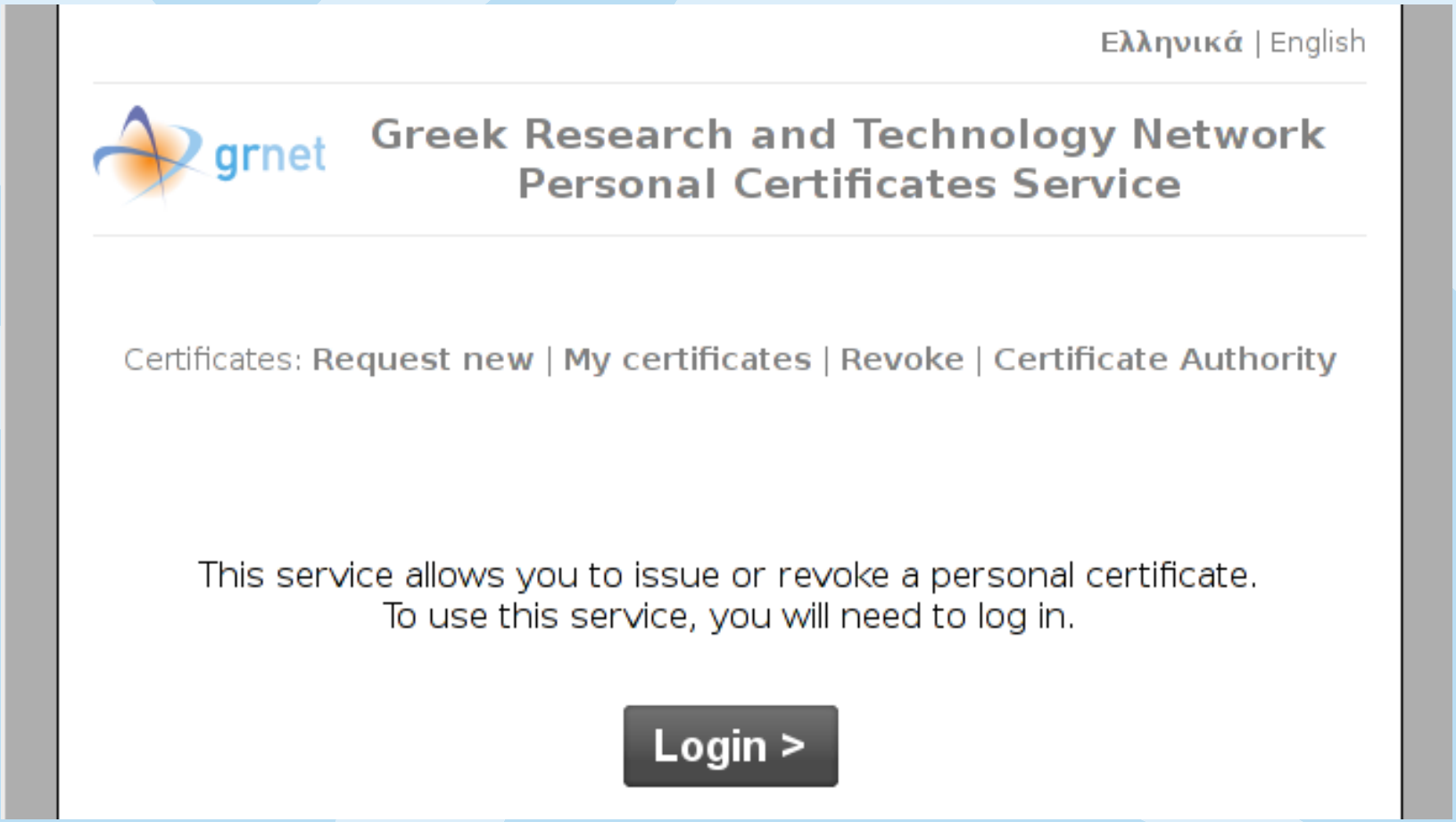
grnet
Networking Research and Education

Services: TCS

- TERENA's digital certificate service
- Flat-fee X.509 commercial certificates for everyone
- Three types of certificates:
  1. Server certificates
  2. Personal certificates
  3. Code-signing certificates
- For **(2)**, AAI is mandatory (literally written in the CPS)
- We use a heavily customized Confusa

grnet
Networking Research and Education

Services: TCS



grnet
Networking Research and Education

Services: TCS

Info About You

This is information we have received from your home organization Identity Provider (Greek Research and Technology Network)

Name:	Faidon Liambotis
E-mail address:	faidon@admin.grnet.gr
Entitlement:	admin, user
Unique ID	faidon@grnet-hq.admin.grnet.gr
Home Organization	Greek Research and Technology Network
Country	GR
Domain:	grnet.gr
Full-DN:	/C=GR/O=Greek Research and Technology Network/CN=Faidon Liambotis/unstructuredName=faidon@grnet-hq.admin.grnet.gr

grnet
Networking Research and Education

Services: Anafandon

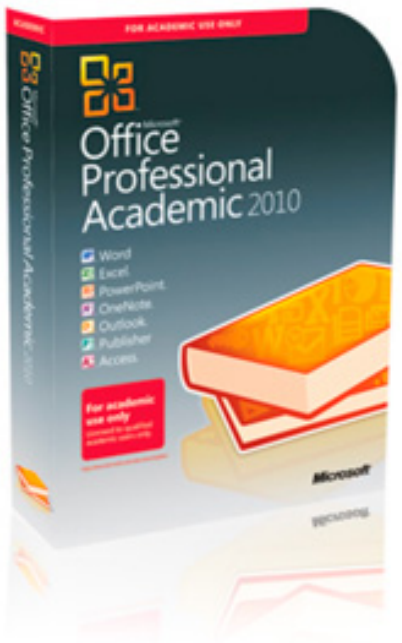
- Distribution of commercially available software
- In cooperation with vendors
- mostly Microsoft
  - MSDNAA
  - eAcademy
  - Dreamspark
- Oracle
- Forrester

grnet
Networking Research and Education

Services: Anafandon

Ελέγξτε αν είστε δικαιούχος και παραγγείλετε ένα από τα διαθέσιμα προϊόντα.

Αγοράστε τώρα



ΜΟΝΟ
ΓΙΑ ΦΟΙΤΗΤΕΣ

από ~~720,00€~~

μόνο 64,99€

ΕΚΠΤΩΣΗ 91%

*διαθέσιμο στην ελληνική
και στην αγγλική έκδοση

grnet
Networking Research and Education

Services: IPTV

- Experimental IPTV broadcasting
- Special rules for distribution of content apply
- Targetting our community: (multicast || AAI)

grnet
Networking Research and Education

Collaborating

- We collaborate on *networks*
- Can we collaborate on *services*, too?
- GÉANT has eduGAIN for inter-federation services
- Can we have a closer, SEE, collaboration?
- We're willing to drive this!
- **Is there interest?**

grnet
Networking Research and Education

More...

- GRNET AAI
  http://aai.grnet.gr/ (English too!)
- Mail me!
  faidon@grnet.gr

grnet
Networking Research and Education

Questions?

grnet
Networking Research and Education