Authentication Authorization

Eirini Degkleri

Authentication - Authorization

Authentication: Who is the user?

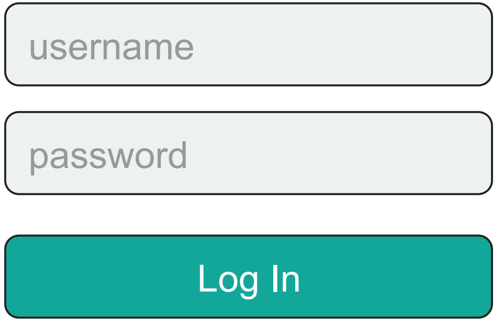
- Allows the user to access a service.

Authorization: What is the role of the user?

- Determines what the user is allowed to do in that service.

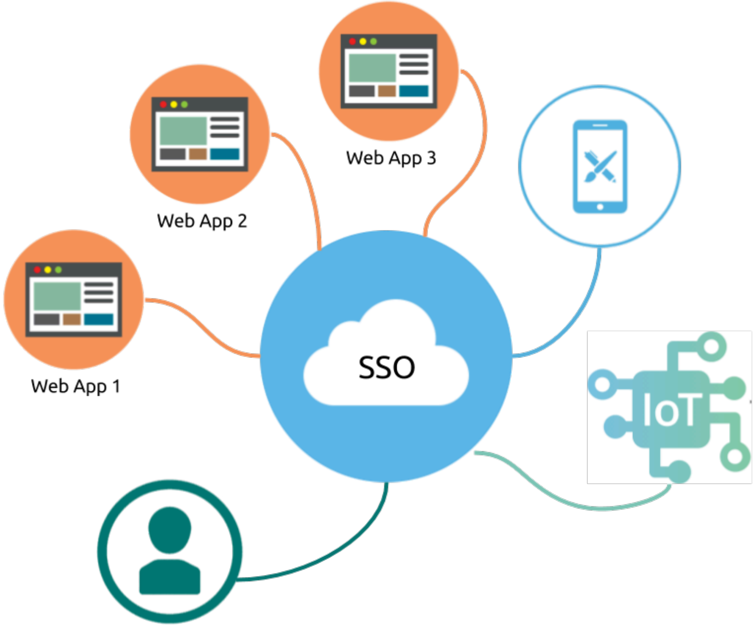
Traditional login

Please login:



How SSO works

User logs in with a single set of credentials to all **connected** applications and services.



Img location: https://insready.com/sites/default/files/SSO%20diagram.png

Known SSO login examples

You can use your institutional credentials to access:

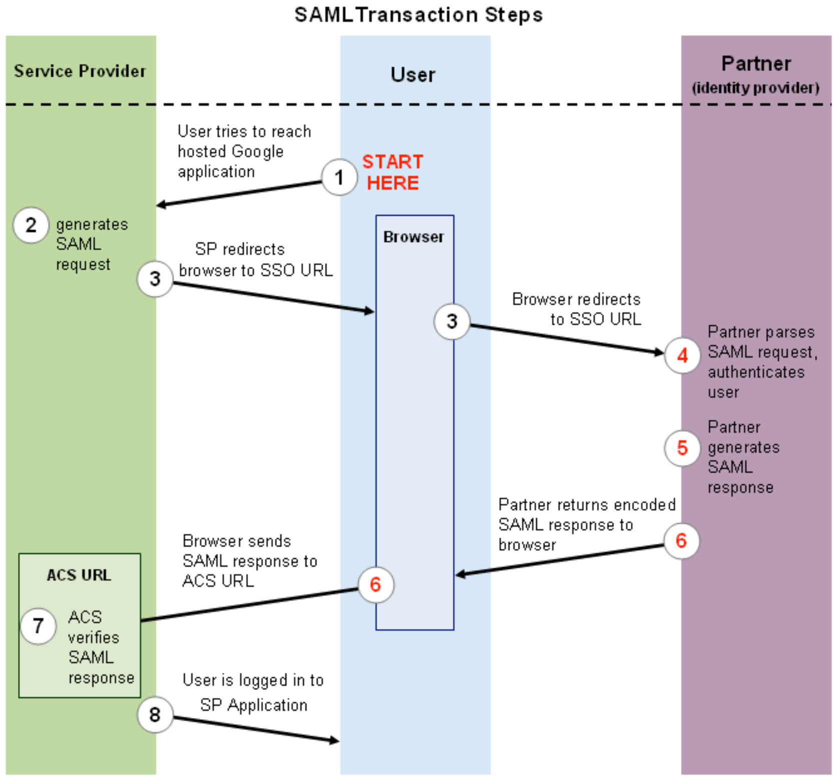
- Eudoxus
- Eduroam
- ~okeanos
- ATLAS (Internship for Greek higher education students)
- …

Components of a SSO system

- The **Identity Provider (IdP)** is responsible for user authentication and providing user information to the Service Provider (SP).
- The **Service Provider (SP)** is responsible for protecting an online resource and consuming information from the Identity Provider (IdP).
- The **Discovery Service (DS)** helps the Service Provider (SP) discover the user's Identity Provider (IdP).

Architecture of a SSO system

Security Assertion Markup Language (SAML) is SSO login standard.


SAMLTransaction Steps
Service Provider
User
Partner
(identity provider)
User tries to reach hosted Google application
1
START HERE
2
generates SAML request
3
SP redirects browser to SSO URL
Browser
3
Browser redirects to SSO URL
4
Partner parses SAML request, authenticates user
5
Partner generates SAML response
Partner returns encoded SAML response to browser
6
Browser sends SAML response to ACS URL
6
ACS URL
7
ACS verifies SAML response
User is logged in to SP Application
8

Img location: https://hungreyweasel.wordpress.com/saml-ssos-shibboleth-sp-reverse-proxy/

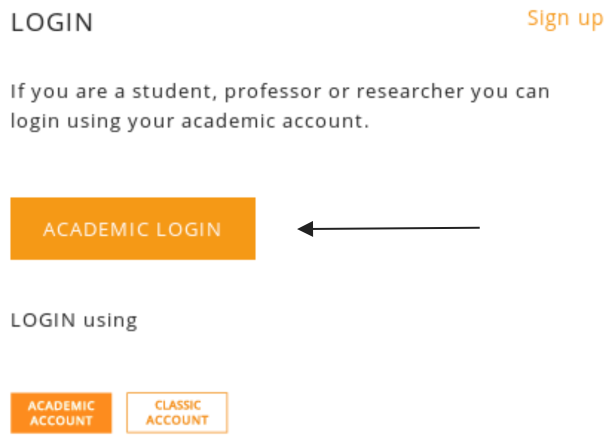
Architecture of a SSO system

okeanos dashboard

In practice:

Step 1:

User tries to access ~okeanos


LOGIN

Sign up

If you are a student, professor or researcher you can login using your academic account.

ACADEMIC LOGIN

LOGIN using

ACADEMIC ACCOUNT

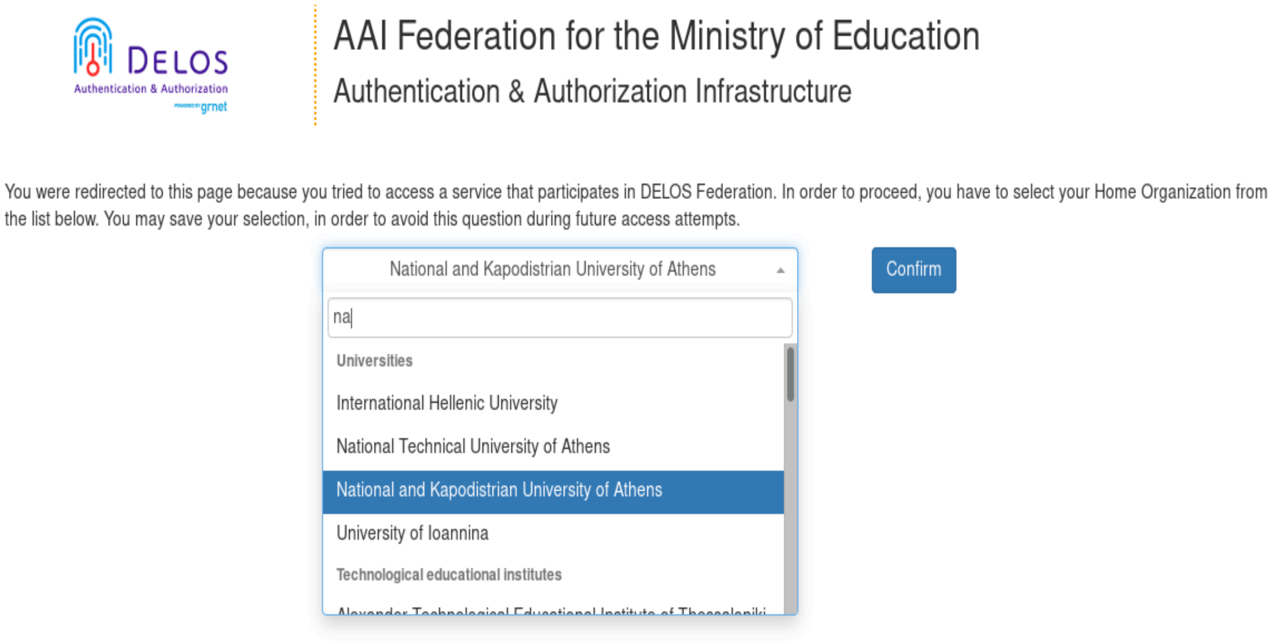
CLASSIC ACCOUNT

Architecture of a SSO system

In practice:

Step 2:

User chooses his home institution



AAI Federation for the Ministry of Education

Authentication & Authorization Infrastructure

You were redirected to this page because you tried to access a service that participates in DELOS Federation. In order to proceed, you have to select your Home Organization from the list below. You may save your selection, in order to avoid this question during future access attempts.

National and Kapodistrian University of Athens

na

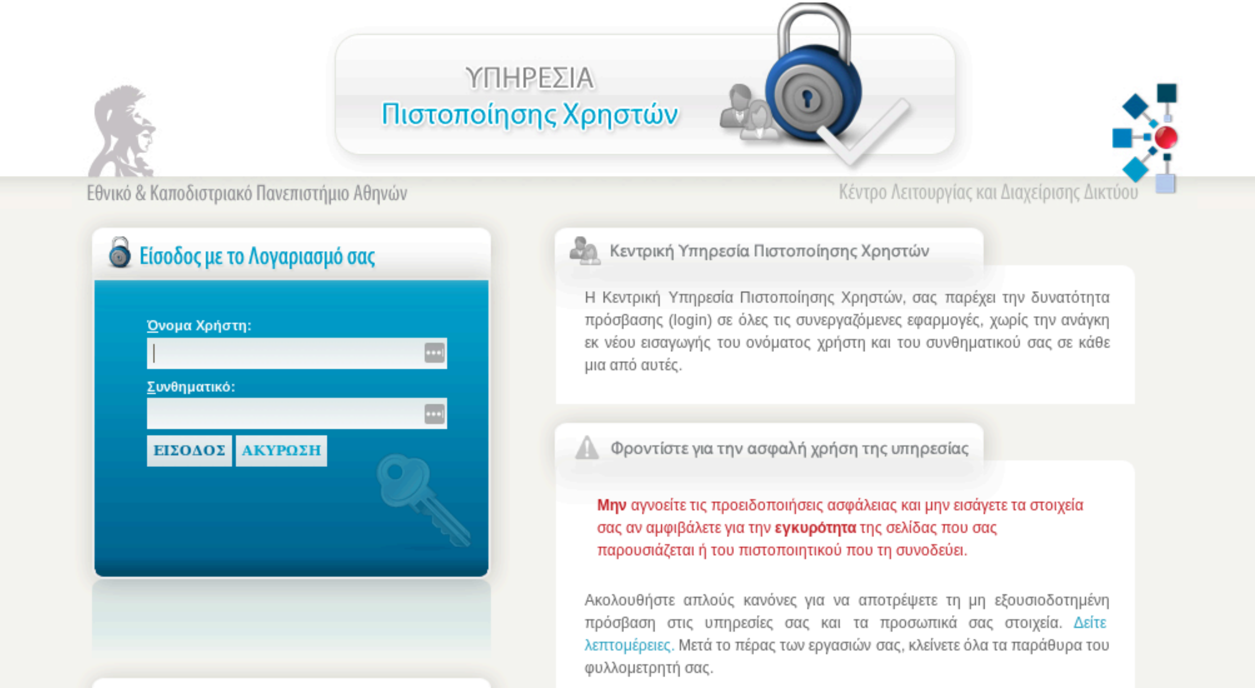
DELOS
Authentication & Authorization
grnet
Confirm
Universities
International Hellenic University
National Technical University of Athens
National and Kapodistrian University of Athens
University of Ioannina
Technological educational institutes
Alexander Technological Educational Institute of Thessaloniki

Architecture of a SSO system

In practice:

Step 3:

User is redirected to his home institution to login



ΥΠΗΡΕΣΙΑ
Πιστοποίησης Χρηστών

Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών

Κέντρο Λειτουργίας και Διαχείρισης Δικτύου

Είσοδος με το Λογαριασμό σας

Όνομα Χρήστη:

Συνθηματικό:

ΕΙΣΟΔΟΣ ΑΚΥΡΩΣΗ

Κεντρική Υπηρεσία Πιστοποίησης Χρηστών

Η Κεντρική Υπηρεσία Πιστοποίησης Χρηστών, σας παρέχει την δυνατότητα πρόσβασης (login) σε όλες τις συνεργαζόμενες εφαρμογές, χωρίς την ανάγκη εκ νέου εισαγωγής του ονόματος χρήστη και του συνθηματικού σας σε κάθε μια από αυτές.

Φροντίστε για την ασφαλή χρήση της υπηρεσίας

Μην αγνοείτε τις προειδοποιήσεις ασφάλειας και μην εισάγετε τα στοιχεία σας αν αμφιβάλετε για την **εγκυρότητα** της σελίδας που σας παρουσιάζεται ή του πιστοποιητικού που τη συνοδεύει.

Ακολουθήστε απλούς κανόνες για να αποτρέψετε τη μη εξουσιοδοτημένη πρόσβαση στις υπηρεσίες σας και τα προσωπικά σας στοιχεία. Δείτε λεπτομέρειες. Μετά το πέρας των εργασιών σας, κλείνετε όλα τα παράθυρα του φυλλομετρητή σας.

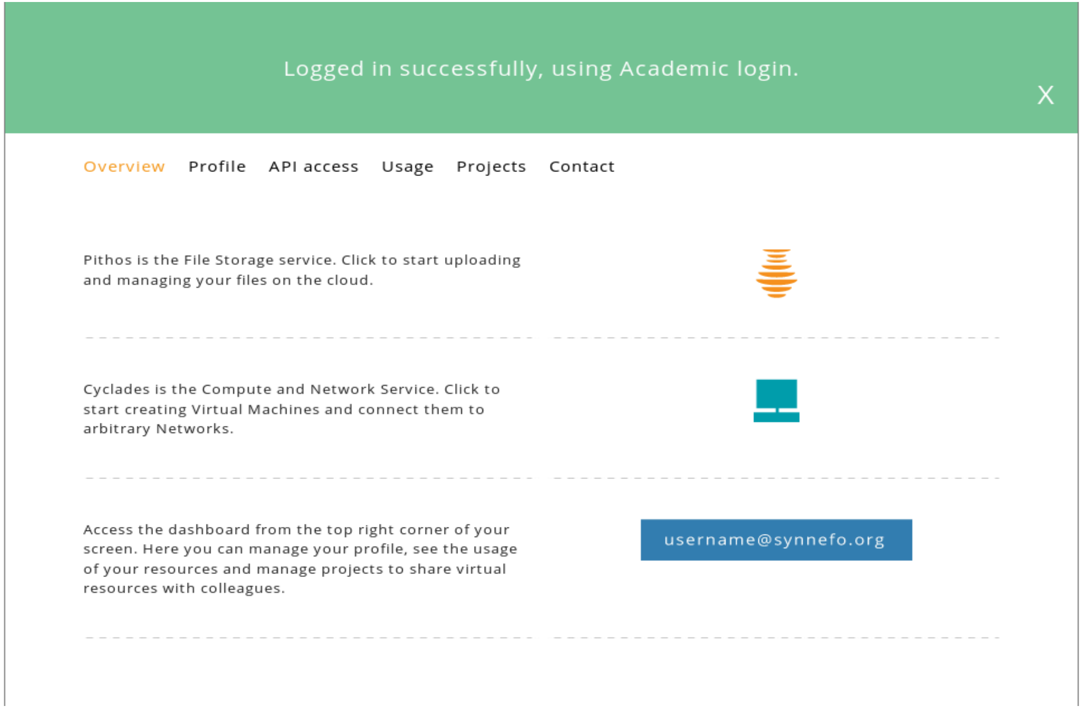
Architecture of a SSO system

In practice:

Step 4:

User is logged in to ~okeanos, with his home institution credentials.

Success!



Logged in successfully, using Academic login.

Pithos is the File Storage service. Click to start uploading and managing your files on the cloud.

Cyclades is the Compute and Network Service. Click to start creating Virtual Machines and connect them to arbitrary Networks.

Access the dashboard from the top right corner of your screen. Here you can manage your profile, see the usage of your resources and manage projects to share virtual resources with colleagues.

What about my role? | Authorization

After login visit: https://accounts.okeanos.grnet.gr/Shibboleth.sso/Session

Miscellaneous

Session Expiration (barring inactivity): 473 minute(s)
SSO Protocol: urn:oasis:names:tc:SAML:2.0:protocol
Identity Provider: https://login.uoc.gr/idp/shibboleth
Authentication Time: 2018-05-23T08:43:11.403Z

Attributes

Shib-EP-Affiliation: Student@uoc.gr
Shib-EP-Entitlement:
Shib-EP-PrimaryAffiliation: Student
Shib-Person-commonName: EIRINI-AIKATERINI DEGKLERI
eppn: <username>@csd.uoc.gr
mail: <username>@csd.uoc.gr

Questions?

Internal Pentesting @ GRNET

Linos Giannopoulos

Some bits of theory

Whitebox Testing:

- Access to internal information about the application (e.g. source code, network architecture)
- Deep and thorough
- Time can be wasted if you don’t know what you’re looking for during code review

Blackbox Testing:

- Performed without any additional information
- Certain scenarios might not be tested
- Simulates a realistic scenario

What should I choose?

- Depends on the scenario we want to test

Some bits of theory

➔ What defines a hacker?

Some bits of theory

Some bits of theory

- What is/defines a hacker?
  - *A computer hacker is any skilled computer expert that uses their technical knowledge to overcome a problem.*
    ....someone who, with their technical knowledge, uses bugs or exploits to break into computer systems ~ Wikipedia
  - *Anyone with enough interest and curiosity in learning how things work, how they can break and helping others fix them*
  - **Ethics**

Internal Penetration Tests

- Tested applications:
  - X: Social media App
  - Y: E-shop
- Whitebox testing
- Lots of interesting findings

Interesting findings - X

- Exposed password hashes and personal data
  - Friends’ information is available when two people like the same “group”
  - The API returned too much information while the UI displayed a fraction of it
- Field injection during User registration
  - The typical User model has several fields (e.g. first_name, age)
  - The backend would take all user-inserted fields and put them in a User object
  - A malicious user could inject fields (e.g. is_verified, user_type) into the final User object
- CSV Injection
  - Administrators can export all users’ data into a CSV file
  - A malicious user can inject CSV formulas instead of valid user data
  - Lack of sanitization leads to exposure to Phishing, Remote Code Execution, Local File Inclusion etc.
    - Depends on the client software and version (e.g. Microsoft Excel, LibreOffice)

Interesting findings - Y

- Stored XSS @ unreachable view
  - A user with low privileges can create a new product with an arbitrary name
  - An XSS payload can also be inserted as the product’s name
  - All of the views that were reachable through the UI were safe due to proper sanitization
  - After reviewing the source code, an unreachable view was found that was vulnerable to XSS
- IP-based rate limiting bypass @ Demo account registration
  - A user can register for a demo account for testing purposes
  - That endpoint must be rate limited, otherwise an Application-level DDoS would be possible
  - Due to improper use of X-Forwarded-For Header, a bypass was found
- CSRF @ Demo account registration
  - Cross-site Request Forgery due to lack of use of CSRF tokens
  - Combined with the above vulnerability, an Application-level DDoS is possible

Questions?