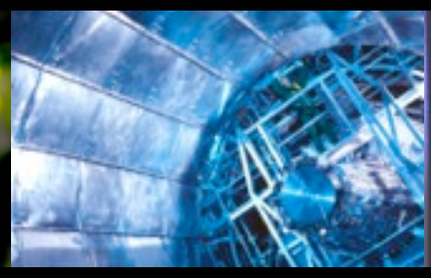
WLCG Group

Identity Federation - HEP/WLCG

FIM4R Meeting PSI Villigen, 20 March 2013, R. Wartel








WLCG Worldwide LHC Computing Grid

Use cases

- Use cases in WLCG are:
  - Web-based (grid portals used for job submission, wikis, etc.)
  - CLI-based (job submission, admin tasks)

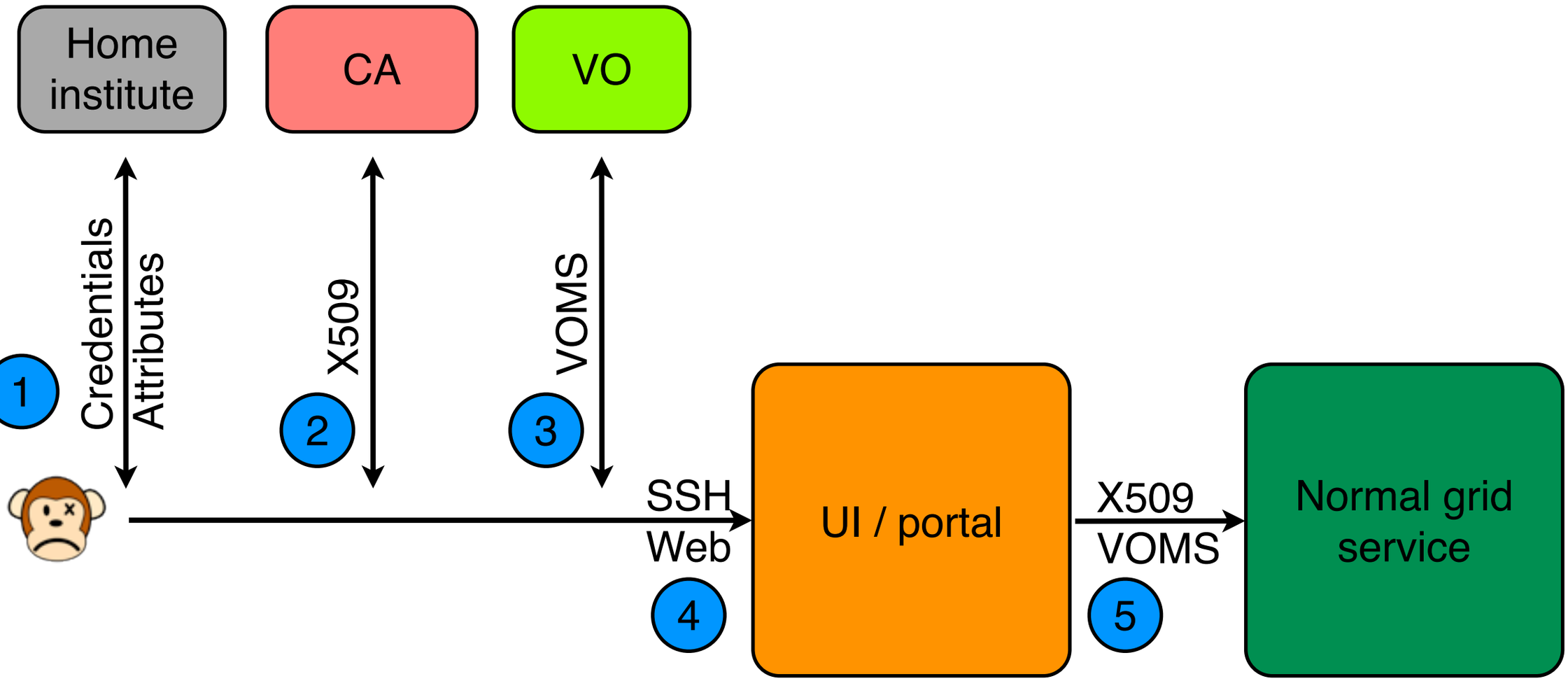
- Use cases foreseen by the experiments for federated identities
  - Alice: Interested - but would rather the work to focus in priority on the Web use case
  - Atlas: Interested in both CLI and Web use case
  - CMS: No immediate adoption foreseen, but supportive of both CLI + Web use cases
  - LHCb: Interested - in particular in a CLI

WLCG CLI pilot

- A working group has been formed in WLCG
  - Proof of concept
  - Architecture design and integration in WLCG
  - Pilot service

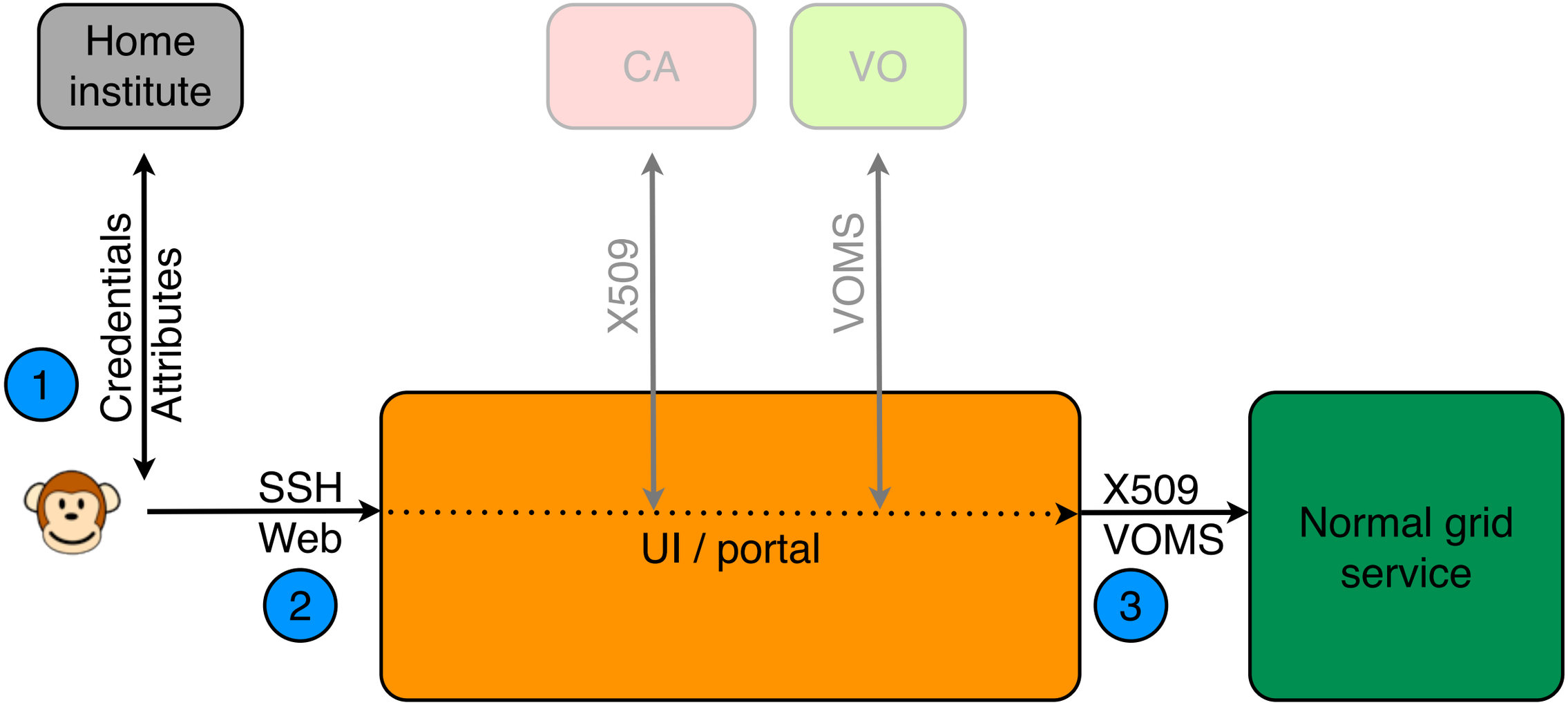
- Pilot service : non-browser based
  - A service enabling access to WLCG resources using home-issued federated credentials
  - CILogon already exists in the US
    - Portal enabling user to obtain a x509 certificate using its standard home institute's credentials
  - Seen as more difficult than the Web use-case
    - Can this work?
    - What would be the costs?
    - How would this interface with the x509-based grid services

A pilot project for WLCG



Traditional access to grid services

A pilot project for WLCG



Federated access to grid services

EMI STS instance at CERN

- A test EMI STS instance has been installed at CERN
  - http://www.eu-emi.eu/security-token
- It can function either with :
  - A test IdP at HIP that supports the ECP profile
  - The WS-Trust endpoint of the CERN ADFS
- A CLI tool has been made available for everyone to test
  - Just works!
  - Promising results

- More information is available at https://twiki.cern.ch/twiki/bin/view/LCG/WLCGFedIdPilot

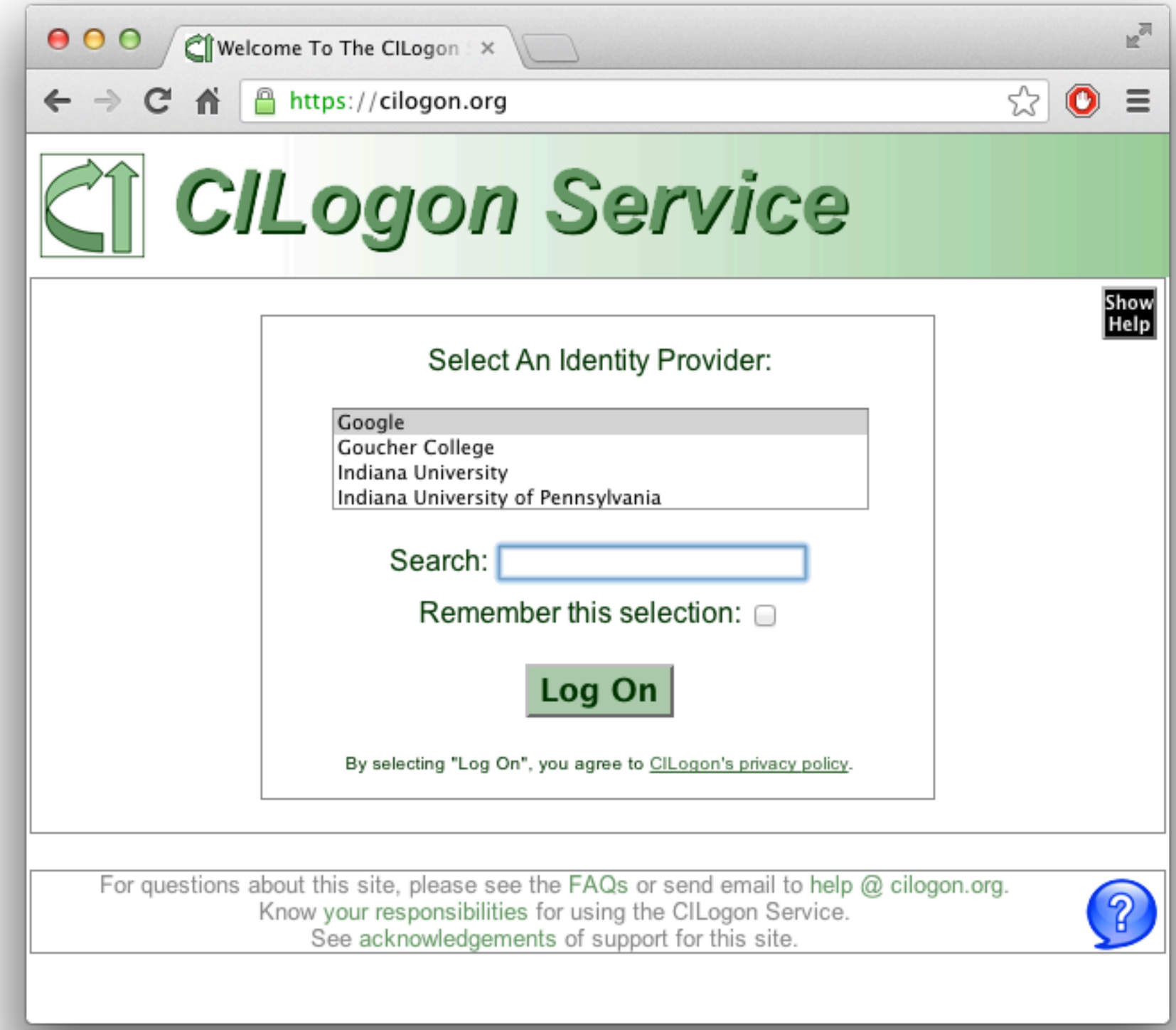
EMI-based CLI pilot

```
[lxadm12] /afs/cern.ch/user/r/rwartel/pilot > ./sts-client.sh -adfs_endpoint https://login-dev.cern.ch:443/adfs/services/trust/13/usernamemixed -v -e https://emi-sts-pilot.cern.ch:8443/sts/wstrust
ADFS Login to address: adfs_endpoint
Creating ADFSCLient
Please enter username: rwartel
Please enter password:
Logging in...
The envelope: <?xml version="1.0" encoding="UTF-8"?>
 [SNIP]
</soap11:Envelope>
[lxadm12] /afs/cern.ch/user/r/rwartel/pilot > ls -l certificate.pem
-rw-r--r-- 1 rwartel c3 1647 Mar 19 14:52 certificate.pem
[lxadm12] /afs/cern.ch/user/r/rwartel/pilot > openssl x509 -in certificate.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            39:0f:cc:80:d6:b0:a0:bb
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=STS WLCG Pilot Test CA, O=EMI, C=CH
        Validity
            Not Before: Mar 19 13:42:39 2013 GMT
            Not After : Mar 29 13:42:39 2013 GMT
        Subject: CN=Romain Wartel, O=WLCG, DC=FedIdentityPilot, C=CH
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
```

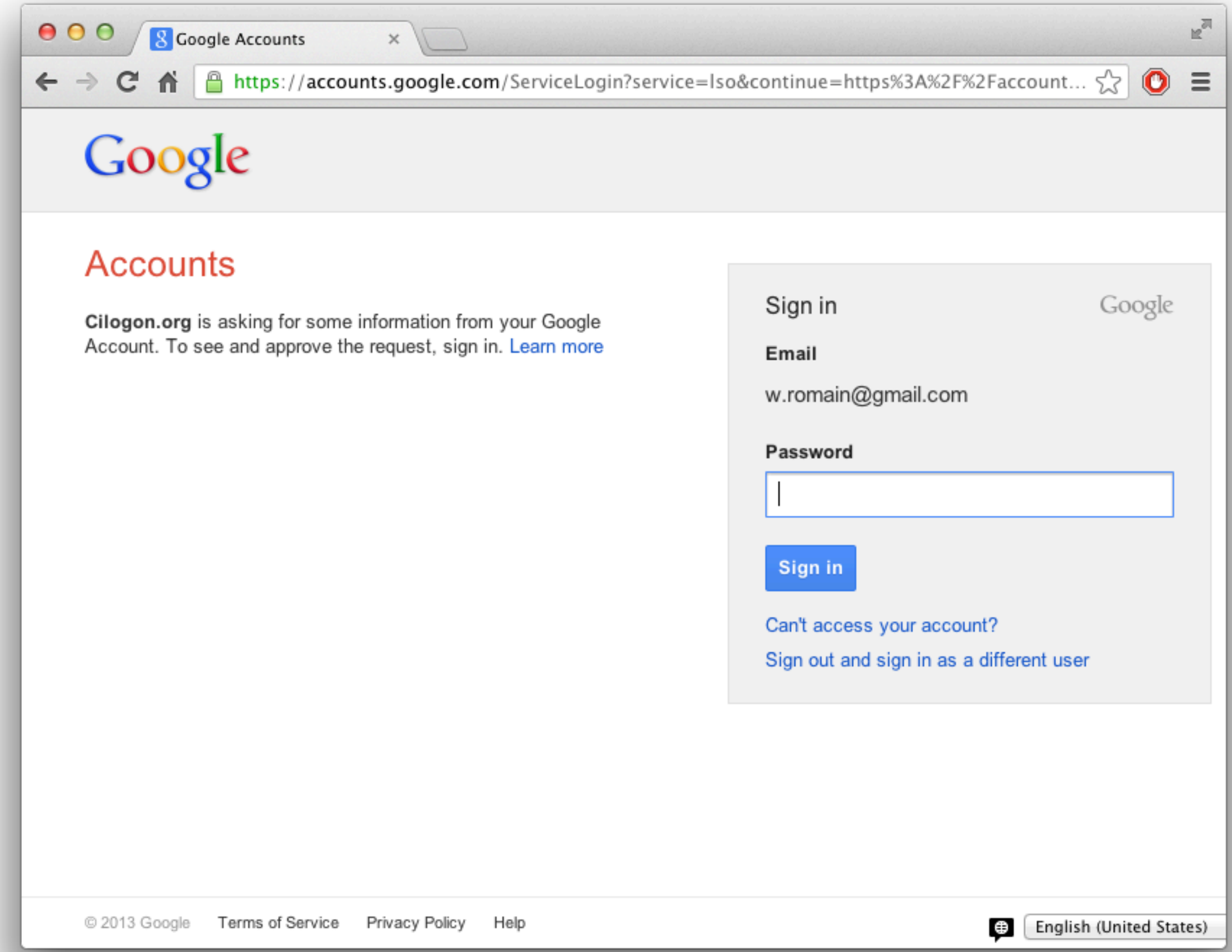
ECP status

- Proof of concept is great, but there is a blocking issue: ECP
- ECP is the standard component need for CLI interaction with IdPs
- Currently, ECP is not deployed, so the CLI pilot is not usable
  - Only very few IdPs support it worldwide
  - Extremely difficult to convince hundreds of IdPs to adopt it, especially when only a small fraction of their users would like to use it
- ECP deployment is may grow, but this is a long term hope
- Solutions without ECP? Significant costs/compromises

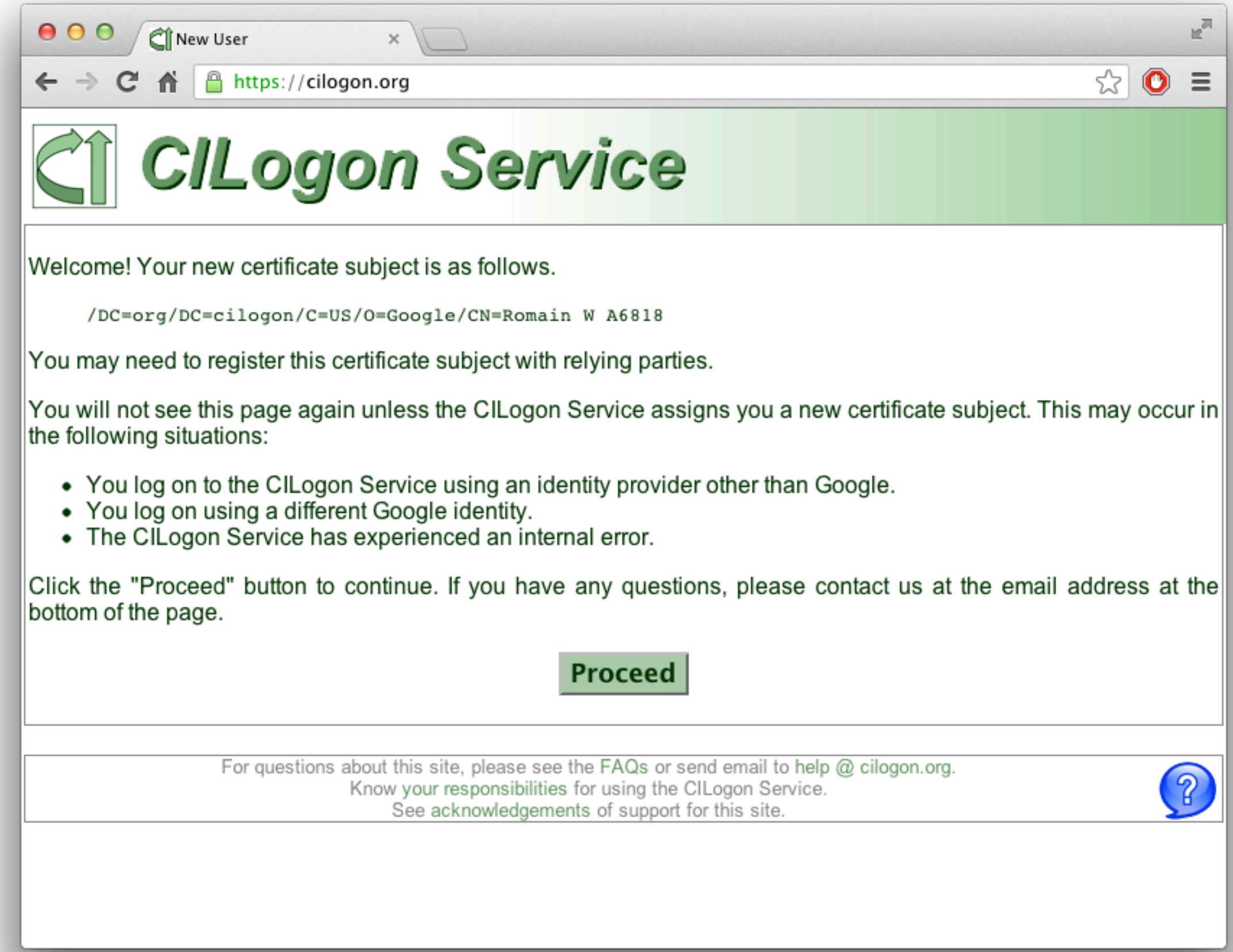
CILogon


Welcome To The CILogon
https://cilogon.org
CILogon Service
Show Help
Select An Identity Provider:
Google
Goucher College
Indiana University
Indiana University of Pennsylvania
Search:
Remember this selection:
Log On
By selecting "Log On", you agree to CILogon's privacy policy.
For questions about this site, please see the FAQs or send email to help @ cilogon.org.
Know your responsibilities for using the CILogon Service.
See acknowledgements of support for this site.

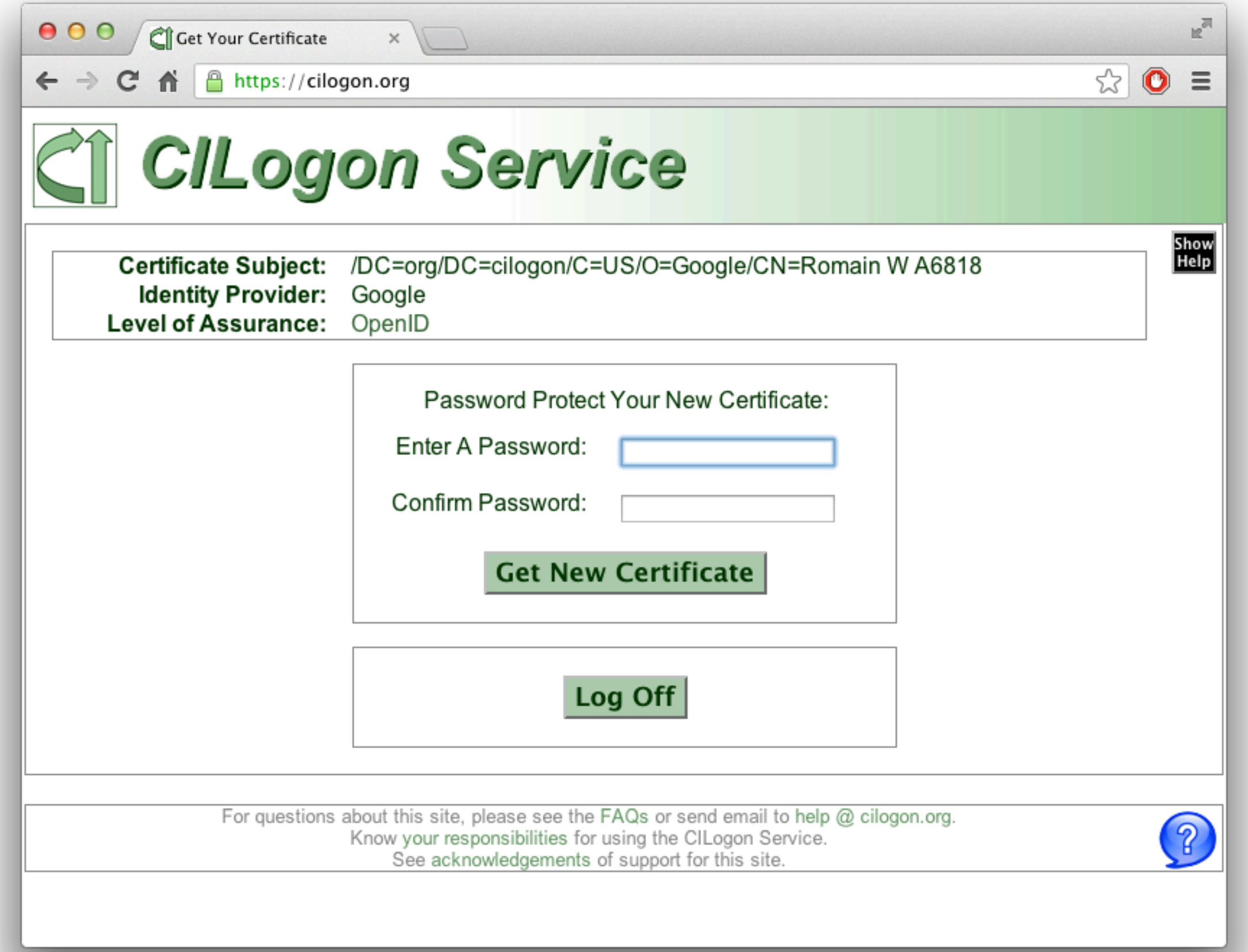
CILogon


Google Accounts
https://accounts.google.com/ServiceLogin?service=lso&continue=https%3A%2F%2Faccount...
Google
Accounts
Cilogon.org is asking for some information from your Google Account. To see and approve the request, sign in. Learn more
Sign in
Google
Email
w.romain@gmail.com
Password
Sign in
Can't access your account?
Sign out and sign in as a different user
© 2013 Google
Terms of Service
Privacy Policy
Help
English (United States)

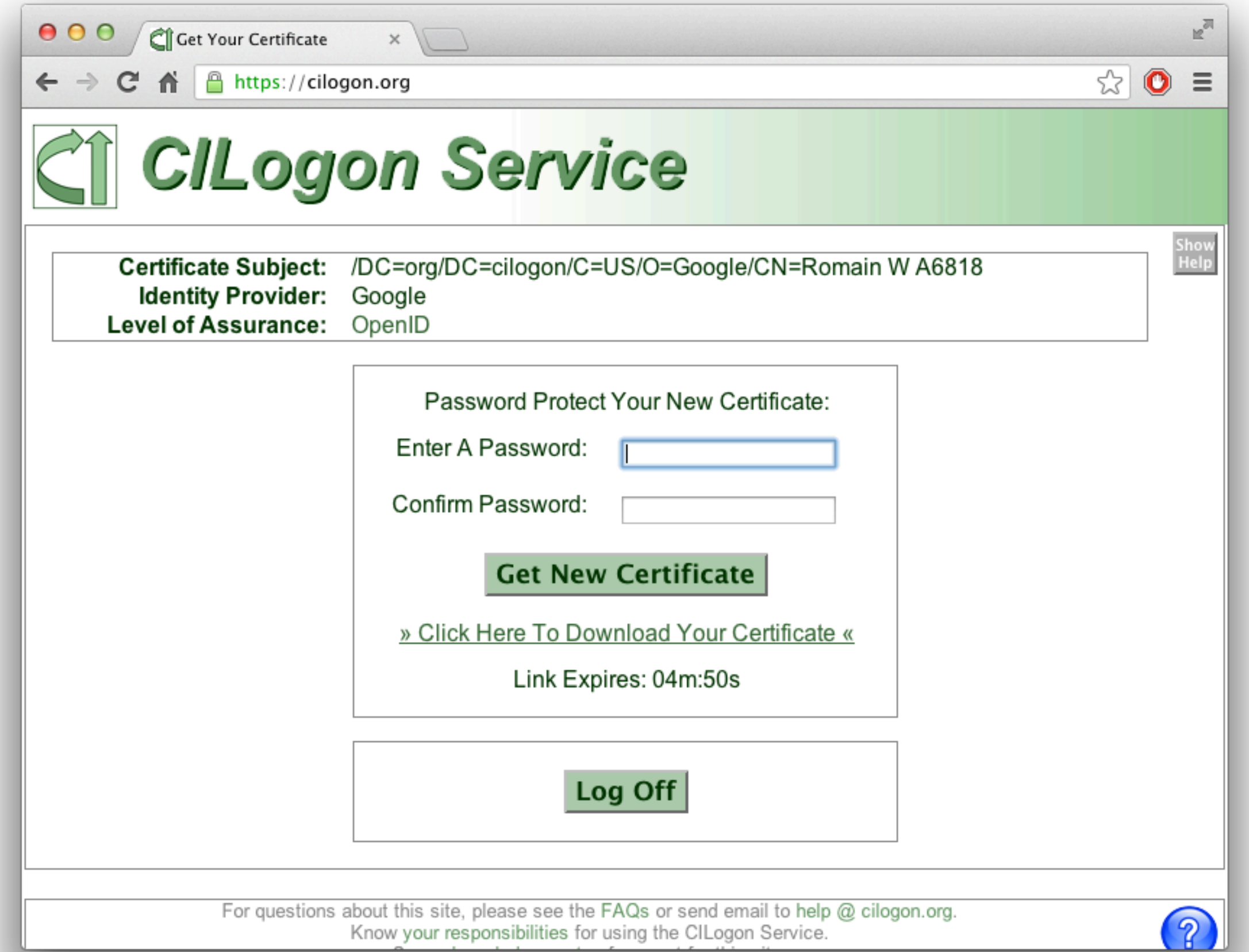
CILogon


New User
https://cilogon.org
CILogon Service
Welcome! Your new certificate subject is as follows.
/DC=org/DC=cilogon/C=US/O=Google/CN=Romain W A6818
You may need to register this certificate subject with relying parties.
You will not see this page again unless the CILogon Service assigns you a new certificate subject. This may occur in the following situations:
You log on to the CILogon Service using an identity provider other than Google.
You log on using a different Google identity.
The CILogon Service has experienced an internal error.
Click the "Proceed" button to continue. If you have any questions, please contact us at the email address at the bottom of the page.
Proceed
For questions about this site, please see the FAQs or send email to help @ cilogon.org.
Know your responsibilities for using the CILogon Service.
See acknowledgements of support for this site.

CILogon


Get Your Certificate
https://cilogon.org
CILogon Service
Show Help
Certificate Subject: /DC=org/DC=cilogon/C=US/O=Google/CN=Romain W A6818
Identity Provider: Google
Level of Assurance: OpenID
Password Protect Your New Certificate:
Enter A Password:
Confirm Password:
Get New Certificate
Log Off
For questions about this site, please see the FAQs or send email to help @ cilogon.org.
Know your responsibilities for using the CILogon Service.
See acknowledgements of support for this site.

CILogon


Get Your Certificate
https://cilogon.org
CILogon Service
Show Help
Certificate Subject: /DC=org/DC=cilogon/C=US/O=Google/CN=Romain W A6818
Identity Provider: Google
Level of Assurance: OpenID
Password Protect Your New Certificate:
Enter A Password:
Confirm Password:
Get New Certificate
» Click Here To Download Your Certificate «
Link Expires: 04m:50s
Log Off
For questions about this site, please see the FAQs or send email to help @ cilogon.org.
Know your responsibilities for using the CILogon Service.

Current plan

- Conduct no further work on an ECP-based CLI pilot for now
  - Pilot works, but ECP will not be available for some time, making deployment difficult
  - Investigate alternative solutions for a CLI (supported by CILogon)
    - Browser interface offering the end user to download a certificate ?
    - A Java webstart client, offering a PEM-formatted certificate that will be downloaded by the client
    - An OAUTH-based (but not yet compliant with OAUTH specs) system, offering the user to get an activation code via the web browser, to be copy/pasted on the CLI
- Focus on the Web use case
  - Understand what WLCG users (LHC experiments) need exactly
  - Determine how best the pilot should interface with existing services
  - CILogon in the US

Current plan

- Also need to discuss other important issues:
  - Trust, Levels of Assurance (LoA)
  - Required attributes
  - Deployment model in WLCG

Summary

- An WLCG working group is investigating a pilot service
  - WLCG services rely on x509
  - Both the Web and CLI use cases are needed
- A CLI-based proof-of-concept is ready
  - But deployment relies on the availability of ECP
  - ECP is virtually not used by IdPs at the moment
  - This is a major issue
- Alternative, less appealing, CLI solutions will be investigated
- The working group will refocus on the Web use case
  - Including integration with existing workflows used by LHC experiments
- Start discussions on trust, attributes, LoA