Network Roaming with Certificates

Jim Basney
jbasney@ncsa.uiuc.edu

This material is based upon work supported by the National Science Foundation under grant number 0943633. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
Catch-All Roaming Scenario

• A faculty, staff, or student member of an InCommon Higher Education Participant travels to an eduroam-enabled campus and asks, “Can I use eduroam for guest network access even though my home campus isn’t an eduroam member?”
  – Does my InCommon SAML IdP logon help?
  – Does my InCommon user certificate help?
Policy Issues

• Should a member from a campus that is not an eduroam subscriber be allowed to use eduroam?
  – Even if that campus is an InCommon Federation Participant or InCommon Certificate Service subscriber?

• We don’t want to discourage eduroam subscription
Basic Approach

• Provide a “catch-all” eduroam-us RADIUS server to authenticate users from non-eduroam-enabled InCommon HE Participant home campuses

• Use certificates for authentication
  – Provided by CILogon via InCommon SAML authentication
  – Provided by the InCommon Cert Service
CiLogon Project Goal

• Enable campus logon to CyberInfrastructure (CI)
  – Use user’s existing security credentials from their home institution
  – Ease credential management for users and CI providers
CILogon for eduroam-us

• An experiment
• Provide certificates customized for the eduroam catch-all use case
  – subjectAltName set to enable RADIUS routing
Status

CILogon: operational
CILogon+eduroam: early experimenting

For more info about CILogon:

www.cilogon.org/faq
info@cilogon.org