Allowing Access to External Resources

- Requires Partner to hold account and profile details for all of your users that need to access the application.
  - Partner manages the life-cycle of those users
    - Does your partner keep you informed of changes?
    - The Yale users need to remember yet another password
Allowing Access to Yale Resources for External Users

- Requires Yale to locally hold account and profile details for all of your users that need to access the application.
  - Yale needs to manage the life-cycle of those additional users.
    - Does Penn State keep us informed of changes?
  - External users need to remember yet another password
The Security Token
Contains claims about the user
For example:
• Name
• User NetID
• Group membership
• User Principal Name (UPN)
• Email address of user
• Email address of manager
• Phone number
• Other attribute values

Signed by Yale

Authentication request

Yale
Identity Provider (IDP)

Active Directory

Security Token Service (STS)

Issues Security Token

ST

Issues Security Token “Authenticates” user to the application

Relying party / Resource provider

Trusts the Security Token from Yale

User / Subject /Principal
Federation Client

User

Resource/Application

Not authenticated

Redirected to STS

ADFS STS

App trusts STS

Authenticate

Query for user attributes

Active Directory

Send Token

Return Security Token

ST

Return page and cookie

ST
Where are we now?

- We have Yale Secure Token services like Shibboleth, ADFS etc.
- We already have the ADFS Service setup in Dev, Test and Production Environments and are ready to launch.
- Actively working across the University to implement Federation Trusts.

Who to go to?

**Sai Ravula**
*Identity & Access Management Lead*
*ITS Info Security*
*Email: sai.ravula@yale.edu*
*Dial: (203) 436-9823*