Unified Identity Authentication
System of CSTNET

Chun Long
October, 2016
Chinese Science and Technology Cloud Passport

• Unified identification management of CST Cloud
• 300+ Applications supported
  – Team libraries
  – Conference service management platform
  – Research main page
  – Mail system of CAS
  – Document and information aggregation system
  – Institute applications
• 10 years research and development
Cloud Service supported by CST Cloud Passport

Total Num of Users: 480,000 (220,000 CAS Users)
Application

- 480’000 users
- 95% institutes In CAS
- 300+ systems support by OAuth 2.0:
  - Information systems of institutes
  - Public service systems of institutes
  - Key project service platform
  - Domestic literature services
- 5 systems by support by SAML2:
  - Springer/IEEE/Wiley/IOP/ELSEVIER
Basic Function

- Register and login
  - Mail address/Mobile Phone Number/User Name
- Account management
- Personal information management
- Third party account binding
  - Unified Authentication of CAS
  - QQ
  - Weibo
  - Wechat Account
- Security mail and password recovery
Application Open Access

• Support SSO
• Support OAuth 2.0 Applications
• Support SAML2 Applications
  – Base on CST Cloud federation, Compatible with eduGAIN
  – Shibboleth
• OAuth 2.0 and SAML2 Interoperability
• LDAP Applications
  – Eduroam Account
CST Passport and UMT

- UMT (User Management Toolkit)

- Software to Implement unified identity management and SSO.

- CST Passport is based on UMT 8.15

- UMT is an open source software from 2013
  - https://github.com/duckling-falcon/
UMT OAuth 2.0

- UMT use standard OAuth 2.0 Protocols
- OAuth Provided a secure, open and simple authentication standard for user’s resources.
- Third party can not access user account information when authenticated by OAuth.
- Any applications can use OAuth authentication services.
- Any application providers can implement their authentication service by OAuth

[UMT OAuth 2.0 Diagram]

An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications. Read the OAuth 2.0 specification.

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service.

For Consumer developers...
- web applications
- desktop applications
- mobile applications
- JavaScript or browser-based apps
- web page widgets

For Service Provider developers...
- web applications
- mobile applications
- server-side APIs
- mashups

OAuth is a simple way to publish and interact with protected data. It's also a safer and more secure way for people to give you access. We've kept it simple to save you time.

Learn more about the emerging OAuth 2.0 framework.

http://oauth.net/
Develop With UMT

- Scenarios
  - Web site or web apps
  - Desktop and mobile apps

- Development doc:
  - http://passport.escience.cn/help.jsp
  - UMT OAuth2 authorization solution: download
  - UMT OAuth2 SDK: UMT-OAuth2-client-0.1.5.jar

- 3 steps to access
  - Submit an access request
  - Implementation of login process
  - Exchange access token and other information, authentication complete
• Planning with Unify Identity Authentication System of CAS

• Mobile terminal access
  – Most work can be done on mobile phones.
  – Unified Identity Authentication is a basic requirement of mobile business.
  – Multiple security levels need different Authentication method. Digital certificates, tokens, biological characteristic
  – Interaction of mobile terminals and PCs
• More flexible authentication methods
  – Now support:
    • User name and password
    • Hardware digital certificates
  – Need more authentication methods:
    • Biological characteristic
      – Finger print, retina, face recognition.
    • SMS validation code
    • QR code
    • Software digital certificates
    • Terminal characteristic
• Capability and stability
  – Support more users and applications
  – Avoid unstable system incidents

• System monitoring and analysis
  – Real time monitoring and measurement.
  – Alert function
  – Aggregate operation and user behavior data
  – Visualization
  – Abnormal detection
  – Block attackers
Thank you!