OpenID Connect as a Service in Cloud-based Diagnostic Imaging Systems

Weina Ma
Kamran Sartipi
Hessan Sharighi

{Weina.Ma, Kamran.Sartipi, Mohammadhassan.Sharghigoorabi}@uoit.ca

Department of Electrical, Computer and Software Engineering
University of Ontario Institute of Technology (UOIT)

SPIE 2015
February 22, 2015

Outline

Motivation

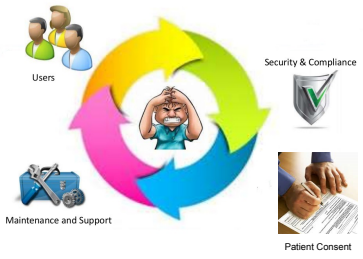
- Distributed computing is coming in the new form as Cloud computing
- 83% of healthcare organizations are using cloud-based apps

- SaaS (Software as a Service)-based applications are the most popular (66.9%)
- Healthcare industry will invest $5.4 billion in Cloud computing by 2017

Background

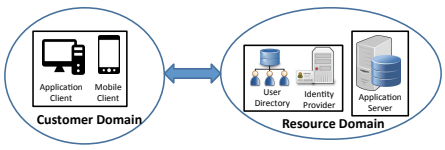
- Any Device, Any Platform Access medical images without installation
- Seamless and collaborative working across functional and geographical locations
- Pay-as-you-go provides lower cost delivery for healthcare IT services
- Focusing on Healthcare Quality Managements

Challenges



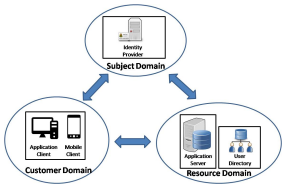
Identity Framework (1)

- User identity is local to each system, e.g., inter-connected PACS systems
- Imposes significant administrative burden for uniform identification

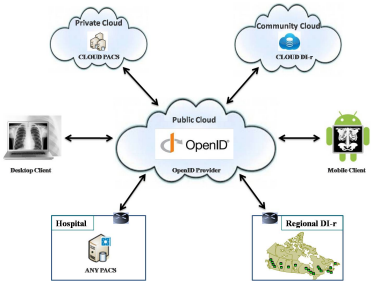


Identity Framework (2)

- External centralized identity provider and decentralized user directory, e.g., IHE XUA integration profile
- Cross-domain identity solution, not dedicated to Cloud and mobile applications



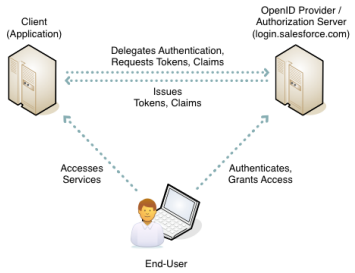
Solution



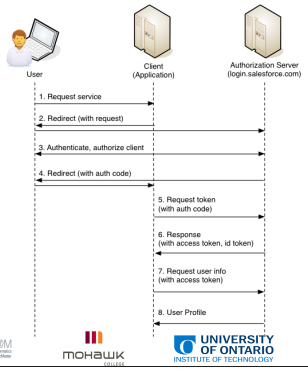
What is OpenID Connect

- User-centric Single-Sign-On solution.
- Simple identity layer on top of OAuth
- Next generation of OpenID
- REST-basd
- Support advanced authentication technologies (e.g., two-factor, biometrics)
- Over 1 billion user account and 50,000 websites
- Specification
  - Core
  - Discovery
  - Dynamic Registration
  - Session Management

OpenID Connect Basics



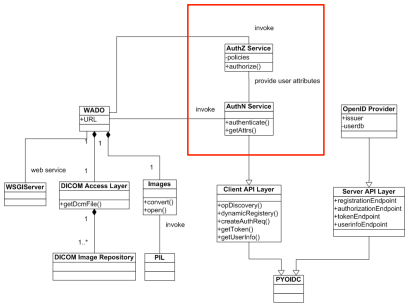
OpenID Connect Protocol



OpenID-Connect-as-a-Service

- OpenID Connect authentication is implemented as a service named "AuthN Service"
- AuthN Service defines two operations
  - Authentication request
  - User information query
- REST/JSON message flows which are easy for developers to integrate
- "PYOIDC" is an open source implementation of OpenID Connect written in Python

OpenID-Connect-as-a-Service

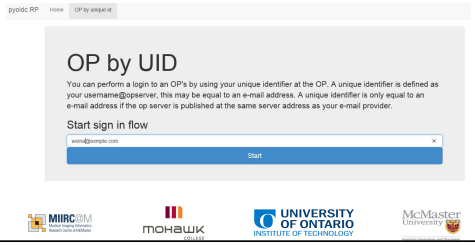


Prototype (1)

- A prototype constitute
  - WADO server
  - DICOM respository
  - OpenID Provider
  - AuthN Service integrated with WADO and OpenID Provider
- A user account is predefined in OpenID Provider weina@example.com
- Enter WADO service URL in browser to access image stored in DICOM repository

Prototype (2)

- WADO server receives the access request and asks for AuthN Service to do authentication.
- AuthN Service redirects page asking for user to enter OpenID identifier



Prototype (3)

- AuthN Service is able to find the location of OpenID Provider using "example.com"
- OpenID Provider redirects to user login page and needs user input username and password

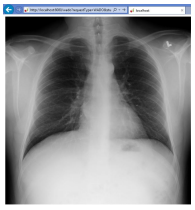
Prototype (4)

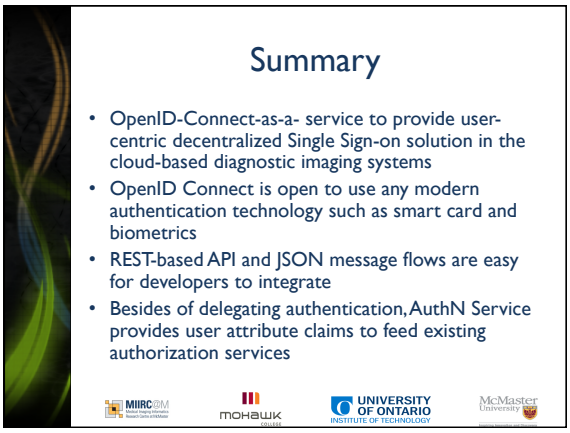
Access Token Response


```
{
   "access_token": "MXDhGGpKqxZusTu1+Sp9QbSRWaDG/
   L0laSWReecSeZHRExbm/+E3nTwfJuYbuYwq6oAEfltW/
   cAAtgntbKAGn/oH6AQcWU3aIVyrq+GiUSg=",
   "expires_in": 3600,
   "token_type": "Bearer",
   "state": "urn:uuid:44186db6-8409-4371-ab9a-ccff368746bb",
   "scope": "openid profile email address phone",
   "refresh_token": "MXDhGGpKqxZusTu1+Sp9QbSRWaDG/
   L0laSWReecSeZHRExbm/+E3nTwfJuYbuYwqeh/E
   +HRB0ESKLLSgVuhg253dbwWaCM3PDEO3cu+OJtI="
}
```


Prototype (5)

- After authentication, the DICOM image is retrieved from DICOM file repository and displayed in browser




Summary
• OpenID-Connect-as-a- service to provide user-centric decentralized Single Sign-on solution in the cloud-based diagnostic imaging systems
• OpenID Connect is open to use any modern authentication technology such as smart card and biometrics
• REST-based API and JSON message flows are easy for developers to integrate
• Besides of delegating authentication, AuthN Service provides user attribute claims to feed existing authorization services
MIIRC
mohawk
UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY
McMaster University