Lightning Talks
TechEx 2018
October 16, 2018

Ester Cha, University of Illinois Urbana-Champaign
Colin Thompson, University of California, Merced
Slavek Licehammer, CESNET
Jim Basney, National Center for Supercomputing Applications
Nathan Dors, University of Washington
Rob Carter, Duke University
<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ester Cha</td>
<td>University of Illinois</td>
<td>You Can Call Me Al</td>
</tr>
<tr>
<td>Colin Thompson</td>
<td>UC Merced</td>
<td>Ideas for running Midpoint using the AWS Well Architected Framework</td>
</tr>
<tr>
<td>Slavek Licehammer</td>
<td>CESNET</td>
<td>Non-web federated access using QR codes</td>
</tr>
<tr>
<td>Jim Basney</td>
<td>NCSA</td>
<td>SciTokens: Capability-Based Secure Access to Remote Scientific Data</td>
</tr>
<tr>
<td>Nathan Dors</td>
<td>University of Washington</td>
<td>OIDC-OAuth Madness: Learning Materials Championship 2018</td>
</tr>
<tr>
<td>Rob Carter</td>
<td>Duke</td>
<td>Enabling Multi-Cloud Storage</td>
</tr>
</tbody>
</table>
Ester Cha
You Can Call Me Al
You can Call me Al
The Importance of Names and Identities

Ester Cha, University of Illinois
Name Display: Joyce Cha (estercha)

Staff and faculty may now set a custom display name in the Illinois Directory to better reflect their identity. By default, your display name consists of your legal name, unless you have set up a published professional name or preferred first name (as a student). Your display name is used in the Illinois Directory, university email, and other services that use name data from the Active Directory.

Choose which name to display in your Directory profile.

<table>
<thead>
<tr>
<th>Name Data Source</th>
<th>First Name</th>
<th>Middle Name</th>
<th>Last Name</th>
<th>Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal</td>
<td>Ester</td>
<td>J</td>
<td>Cha</td>
<td></td>
</tr>
<tr>
<td>Custom</td>
<td>Joyce</td>
<td></td>
<td></td>
<td>Cha</td>
</tr>
</tbody>
</table>

Need to Make Changes?

If you want to change your name:

- **Legal name changes** must be submitted by an employee's home department.
- Updating your custom display name does NOT change your legal name across University systems.
- If you have a published professional name, it will always be your display name.

Guidelines for Custom Entries

You may not use a custom display name to misrepresent who you are, nor may you use any profane or offensive language in your custom display name. Those who intentionally misuse the custom display name option may be subject to disciplinary action.

Read more about acceptable uses of custom names.
Colin Thompson
Ideas for running Midpoint using the AWS Well Architected Framework
Ideas for Running Containerized Midpoint in AWS

- Use RDS instead of traditional database servers. (Multi-AZ, Read Replicas across Regions, no Administrative Overhead)
- Use one or more autoscaling groups for Dockerhosts, (min/max/desired capacities of 1 for self-healing), connect with Elastic Load Balancer(s)
- Use Secrets Manager or SSM Parameter Store for storage of keystore & midpoint repository usernames and passwords (more on this in BoFs & hallway chats)
- Consider offloading SSL on Elastic Load Balancer and eliminate Apache, Shib, & OpenSSL from container image
- Use Cloudwatch Logs Agent/STDOUT and Log Streams
- Code as much as possible in Cloudformation templates, and SHARE!
Cloudformation Templates:
https://github.com/cfthompson/aws-midpoint-infrastructure
(for now...)

Colin Thompson
UC Merced
cthompson31@ucmerced.edu
@Colin Thompson (Internet2 Slack Channel)
Technological background

- Out of band authentication
- OpenID Connect (OIDC)
  - Standardized OAuth2 Device flow
- Pluggable Authentication Module (PAM)
  - Can be used by any application supporting PAM
  - PAM module with OAuth2 Device flow support
- Easy to use for user
  - Retype URL to browser
  - Scan QR code to device with browser
Device Client

<table>
<thead>
<tr>
<th>Client Identifier &amp;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification Code, User Code,</td>
</tr>
<tr>
<td>&amp; Verification URI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>End user</th>
</tr>
</thead>
<tbody>
<tr>
<td>at</td>
</tr>
<tr>
<td>Browser</td>
</tr>
</tbody>
</table>
ukko-3:~ michalp$ ssh root@cloud255-130.cerit-sc.cz
Scan QR code:

URL: https://login.elixir-czech.org/oidc/device?user_code=9RYJGX

Hit ENTER when you are done...
Scan QR code:

URL: https://login.elixir-czech.org/oidc/device?user_code=9RyJGx

Hit ENTER when you are done...

URL is safe

https://login.elixir-czech.org/oidc/device?user_code=9RyJGx

Open

Share  Copy  Info
your previous selection

- Masaryk University

or

Sign in with Google
Sign in with LinkedIn
Sign in with ORCID

or

your institutional account

Type the name of your institution

- Aalborg University
- Aalto University
- Aarhus Basic Health Care College
- Aarhus School of Marine and Technical Engineering

Approval Required for ELIXIR Cloud Demo

Caution:
This client was dynamically registered.
It has been approved 0 times previously.

Access to:
- Log in using your identity

Do you authorize "ELIXIR Cloud Demo"?

Authorize  Deny
Thank you for your attention

Source code for PAM module:
https://github.com/ICS-MU/pam_oauth2_device

Slávek Licehammer
slavek@ics.muni.cz

Internet2 Technology Exchange
16. 10. 2018
Jim Basney
SciTokens: Capability-Based Secure Access to Remote Scientific Data
Capability-Based Secure Access to Remote Scientific Data

Job Submission
- condor_submit
- condor_schedd
- condor_credd
- condor_shadow

Job Execution
- condor_startd
- condor_starter
- User’s job

Data Access
- Data Server
  - (CVMFS / XRootD)

Token Server
- Identity Provider

Policy DB

User

R = refresh tokens
A = access tokens
**Federated IDs and Capabilities**

**CILogon**
- Federated Identity Management
- OpenID Connect
- ID Tokens

**SciTokens**
- Federated Authorization
- OAuth 2.0
- Access Tokens

https://scitokens.org/

This material is based upon work supported by the National Science Foundation under Grant No. 1738962. 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.
# OIDC-OAuth Learning Materials

<table>
<thead>
<tr>
<th>Title</th>
<th>Year</th>
<th>Type</th>
<th>Category</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppAuth SDK</td>
<td>2019</td>
<td>SDK</td>
<td>Application development - Integration - AppAuth</td>
<td></td>
</tr>
<tr>
<td>OAuth4J 2.0 Flow</td>
<td>2018</td>
<td>Article</td>
<td>OAuth - Grania</td>
<td></td>
</tr>
<tr>
<td>SAML 2.0: How to Use</td>
<td>2019</td>
<td>Book</td>
<td>Application development - Integration - AAO</td>
<td></td>
</tr>
<tr>
<td>A Guide to OAuth 2.0 Grants - Alex Billie</td>
<td>2018</td>
<td>Article</td>
<td>OAuth - Grania</td>
<td></td>
</tr>
<tr>
<td>Getting Started with OAuth 2.0 - Ryan Boyd</td>
<td>2012</td>
<td>Book</td>
<td>OAuth - General</td>
<td></td>
</tr>
<tr>
<td>To Use Which OAuth(2) Grants and (OICF) Flows - Robert Broockenstein</td>
<td>2017</td>
<td>Article</td>
<td>OAuth - Grania</td>
<td></td>
</tr>
<tr>
<td>SAML2 vs JVT. Understanding OAuth 2.0 - Robert Broockenstein</td>
<td>2017</td>
<td>Article</td>
<td>OAuth - General</td>
<td></td>
</tr>
<tr>
<td>OAuth 2.0 Playground - Google</td>
<td>Live</td>
<td>Site</td>
<td>OAuth - Playground</td>
<td></td>
</tr>
<tr>
<td>OAuth 2.0 Playground - sponsored by Okta</td>
<td>Live</td>
<td>Site</td>
<td>OAuth - Playground</td>
<td></td>
</tr>
<tr>
<td>The Profile of OpenID Connect - COID 2017 - Paul Grave</td>
<td>2017</td>
<td>Video</td>
<td>OICF - Profile</td>
<td></td>
</tr>
<tr>
<td>OAuth History - OAIIN</td>
<td>2018</td>
<td>Article</td>
<td>OAuth - Grania</td>
<td></td>
</tr>
<tr>
<td>OAuth History - OAIIN</td>
<td>2013</td>
<td>Video</td>
<td>OAuth - OICF</td>
<td></td>
</tr>
<tr>
<td>OAuth 2.0 and the Road to Hell - Erwin Hanmer</td>
<td>2012</td>
<td>Article</td>
<td>OAuth - OICF</td>
<td></td>
</tr>
<tr>
<td>IETF 73 OAuth BOF</td>
<td>2018</td>
<td>Article</td>
<td>OAuth - Grania</td>
<td></td>
</tr>
<tr>
<td>iGen OAuth Profile</td>
<td>Spec</td>
<td>Article</td>
<td>OAuth - Prole</td>
<td></td>
</tr>
<tr>
<td>International Government Assurance Profile for OAuth 2.0</td>
<td>Spec</td>
<td>Article</td>
<td>OAuth - Prole</td>
<td></td>
</tr>
<tr>
<td>International Government Assurance Profile for OpenID Connect 1.0</td>
<td>Spec</td>
<td>Article</td>
<td>OAuth - Prole</td>
<td></td>
</tr>
<tr>
<td>OAuth 2.0 Tutorial - by Jacob Jemio</td>
<td>2014</td>
<td>Article</td>
<td>OAuth - General</td>
<td></td>
</tr>
<tr>
<td>Introduction to JSON Web Tokens - JVT</td>
<td>2007</td>
<td>Article</td>
<td>JVT - Openal</td>
<td></td>
</tr>
<tr>
<td>The Simplest Guide to OAuth 2.0 - Tatsukai Kawasaki</td>
<td>2017</td>
<td>Article</td>
<td>OAuth - General</td>
<td></td>
</tr>
<tr>
<td>Diagrams And Movies Of All The OAuth 3.0 Flows</td>
<td>Mix</td>
<td>Article</td>
<td>OAuth - General</td>
<td></td>
</tr>
<tr>
<td>Full-OAuth2 Implementation of OAuth and OpenID Connect Tells About Finding - Tatsukai Kawasaki</td>
<td>Spec</td>
<td>Article</td>
<td>OAuth - OICF</td>
<td></td>
</tr>
<tr>
<td>OAuth 2 Explained - Le Dang</td>
<td>2015</td>
<td>Article</td>
<td>OAuth - General</td>
<td>11min</td>
</tr>
<tr>
<td>Where should the OpenID Foundation go in 2011? - Chris Messina</td>
<td>2011</td>
<td>Article</td>
<td>OpenID - OICF</td>
<td></td>
</tr>
<tr>
<td>OpenID Connect Core 1.0</td>
<td>Spec</td>
<td>Article</td>
<td>OpenID - Core</td>
<td>17min</td>
</tr>
<tr>
<td>OpenID Connect Federation 1.0 (draft04)</td>
<td>Spec</td>
<td>Article</td>
<td>OpenID - Core</td>
<td></td>
</tr>
</tbody>
</table>

**Changes saved**
OIDC-OAuth
Learning Materials Championship
2018
Sweet 16

Hammer Movin On
Parecki OAuth 2.0 Servers
MARCH 23

Schwartz's Verses
Le Deng Explains
MARCH 27

RFC 6819
Sanso Top 10
MARCH 30

What the Heck Okta
RFC 6749
MARCH 23

Richer & Sanso
OIDC FAQ
MARCH 23

Oracle Vids
Sakimura Vid
MARCH 30

Google Playground
ORCID Playground
MARCH 27

Globus Dev Guide
iGov OAuth Profile
MARCH 23

Kawasaki Findings
Kawasaki Guide
MARCH 23

Broeckelmann II
Parecki OAuth Simplified
MARCH 27

Auth0 on Flows
Richer Patterns
MARCH 27

Bibbie Guide
Bibbie Guide
MARCH 23

OIDC Implementer's
Grass iGov Vid
MARCH 23

OJOU Materials
OJOU Vids
MARCH 27

OIDC Core
OneLogin on OIDC
MARCH 23

Links to materials here:
https://spaces.internet2.edu/ivy/7yBw
#OIDC-OAuth-Madness
OAuth 2.0 is the modern standard for securing access to APIs.
Read on for a complete guide to building your own authorization server.

Learn about OAuth 2.0
Solve it with Okta
OIDC-OAuth Learning Materials Championship 2018

Sweet 16

Links to materials here: https://spaces.internet2.edu/v/kY2yb8w

#OIDC-OAuth-Madness
The Simplest Guide To OAuth 2.0

For the past three years, I've repeated to explain OAuth 2.0 to those who don't have a technical background, mainly to investors as a co-founder of Authlete, Inc. ('Tech In Asia: "API security startup Authlete raises $1.2m in seed funding"'). As a result, I found a way to explain OAuth 2.0 in an easily understandable manner. This article introduces the steps.

1. There are data of a user.
Full-Scratch Implementor of OAuth and OpenID Connect Talks About Findings

1. Introduction

In this post, a developer who has implemented an OAuth 2.0 and OpenID Connect server from scratch (me) talks about findings. Basically, consideration points for implementation are written discursively. Therefore, this is not a document for those who are looking for information like “How to set up an OAuth 2.0 and OpenID Connect server promptly”. If you are looking for such information, please visit java-oauth-server and java-resource-server on GitHub. Using these, you can start an authorization server and a resource server, issue an access token and call a Web API with the access token, in 10 minutes with no need to set up your DB server.

Bias

I’m a co-founder of Authlete, Inc, which is a company providing implementations of OAuth 2.0 and OpenID Connect on cloud, so this

Never miss a story from Takahiko Kawasaki, when you sign up for Medium. Learn more
OIDC-OAuth
Learning Materials Championship 2018
Sweet 16

Links to materials here:
https://spaces.internet2.edu/u/kY2vBw
#OIDC-OAuth-Madness
International Government Assurance Profile (iGov) for OpenID Connect 1.0 - draft 01

Abstract

The OpenID Connect protocol defines an identity federation system that allows a relying party to request and receive authentication and profile information about an end user.

This specification profiles the OpenID Connect protocol to increase baseline security, provide greater interoperability, and structure deployments in a manner specifically applicable to (but not limited to) government and public service domains.

This profile builds on top of, and inherits all properties of, the OAuth profile for iGov.

Table of Contents

1. Introduction
   1.1. Requirements Notation and Conventions
   1.2. Terminology
   1.3. Conformance
2. Relying Party Profile
   2.1. Requests to the Authorization Endpoint (Authentication Request)
   2.2. Requests to the Token Endpoint
   2.3. ID Tokens
   2.4. Request Objects
   2.5. Discovery
3. OpenID Provider Profile
   3.1. ID Tokens
   3.2. Pairwise Identifiers
   3.3. UserInfo Endpoint
   3.4. Request Objects
   3.5. Vectors of Trust
   3.6. Authentication Context
   3.7. Discovery
   3.8. Dynamic Registration
4. User Info
   4.1. Claims Supported
   4.2. Scope Profiles
   4.3. Claims Request
OAuth 2 in Action

Justin Richer and Antonio Sanso
Forward by Ian Glazer
March 2017 - ISBN 9781617293276 - 360 pages - printed in black & white

Provides pragmatic guidance on what to do … and what not to do.

From the Foreword by Ian Glazer, Salesforce

OAuth 2 in Action teaches you the practical use and deployment of this HTTP-based protocol from the perspectives of a client, authorization server, and resource server. You’ll learn how to confidently and securely build and deploy OAuth on both the client and server sides.

PART 1: FIRST STEPS

1. WHAT IS OAUTH 2.0 AND WHY SHOULD YOU CARE?
2. THE OAUTH DANCE

PART 2: BUILDING AN OAUTH 2.0 ENVIRONMENT
OIDC-OAuth Learning Materials Championship 2018
Final Four

Links to materials here:
https://spaces.internet2.edu/wkYv7yBw
#OIDC-OAuth-Madness
### My Projects

<table>
<thead>
<tr>
<th>Project Name</th>
<th>PI</th>
<th>Fund Code</th>
<th>Providers</th>
<th>Admin Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>OIT First Test</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
<td>000-3059</td>
<td>AWS</td>
<td>urn:mace:duke.edu:groups:group-manager:roles:oit-objectstore-portal-admins</td>
</tr>
<tr>
<td>OIT Second Test</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
<td>000-3059</td>
<td>AWS</td>
<td>urn:mace:duke.edu:groups:group-manager:roles:portunus-test2-admins</td>
</tr>
<tr>
<td>Demo project 1</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
<td>000-3059</td>
<td>AWS</td>
<td></td>
</tr>
</tbody>
</table>

### Other Projects

<table>
<thead>
<tr>
<th>Project Name</th>
<th>PI</th>
<th>Fund Code</th>
<th>Providers</th>
<th>Admin Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>OIT Third Test</td>
<td><a href="mailto:rb186@duke.edu">rb186@duke.edu</a></td>
<td>000-3059</td>
<td>AWS</td>
<td>urn:mace:duke.edu:groups:group-manager:roles:portunus-test3-admins</td>
</tr>
</tbody>
</table>
### Authorized Providers

<table>
<thead>
<tr>
<th>Provider</th>
<th>Provider Id</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services S3 Service</td>
<td>AWS</td>
<td>AWS S3 storage incurs monthly charges for both storage used and data transferred out of the cloud service; govern your usage accordingly.</td>
</tr>
<tr>
<td>Name</td>
<td>Provider</td>
<td>Owner</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>carter-bucket-test1</td>
<td>AWS</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
</tr>
<tr>
<td>carter-bucket-test2</td>
<td>AWS</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
</tr>
<tr>
<td>newt-test-bucket</td>
<td>AWS</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
</tr>
<tr>
<td>dukeoit-bucket-test3</td>
<td>AWS</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
</tr>
<tr>
<td>dukeoit-bucket-test4</td>
<td>AWS</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
</tr>
<tr>
<td>dukeoit-bogus-1</td>
<td>AWS</td>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
</tr>
</tbody>
</table>
carter-bucket-test2 (Project: OIT First Test Project)

Provider AWS
Bucket Name carter-bucket-test2
Owner rob@duke.edu
AWS Handle arn:aws:s3:::carter-bucket-test2
Fund Code 000-3069

Authorized Permissions for carter-bucket-test2

<table>
<thead>
<tr>
<th>User</th>
<th>Permission</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:rob@duke.edu">rob@duke.edu</a></td>
<td>owner</td>
<td></td>
</tr>
<tr>
<td><a href="mailto:hiro@duke.edu">hiro@duke.edu</a></td>
<td>read-only</td>
<td></td>
</tr>
<tr>
<td>Provider</td>
<td>Buckets</td>
<td>Options</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>------------------</td>
</tr>
<tr>
<td>AWS</td>
<td>carter-bucket-test1,carter-bucket-test2,newt-test-bucket,dukeoit-bucket-test3,dukeoit-bucket-test4,dukeoit-bogus-1</td>
<td>Retrieve Keys</td>
</tr>
<tr>
<td>AWS</td>
<td>None</td>
<td>Retrieve Keys</td>
</tr>
</tbody>
</table>