Working Group Summary and Charter - 2018

Page status - informational

March 12, 2019 – This document includes the working group charter for the period ending in 2018. In 2019, the working group refocused on more specific deliverables. The Objectives section wasn't part of the original summary and charter, but it has been added because it helped define the activities and coordination of efforts for the same period.

Summary

A recent survey confirmed that there is already substantial use of the OIDC/OAuth2 protocols by campuses. However, using these protocols is substantially “less mature” in the higher education environment than the SAML protocols that have been used for the last fifteen years. This working group will bring together current users to develop and propose standard deployment practices in order to improve the likelihood of interoperation “just working”.

Problem Statement

The last several years have seen broad adoption of two different cross-domain authentication frameworks and their associated identity spaces. Higher education worldwide, a growing number of business systems (especially cloud-based), and groups particularly concerned with security have adopted the SAML protocol and profiles and associated infrastructure (e.g., metadata describing participants). More recently, personal web use and a growing number of apps that are of interest to the higher ed community are using the OIDC/OAuth2 protocol and frameworks. Today, using these protocols requires two different identity spaces (identifiers, credentials). The growing use of OAuth2 to protect API endpoints by higher ed has increased the interest in bridging these spaces, and providing a single software package supporting multiple protocols. This is expected to provide better security, improved usability, and better interoperability in a multi-protocol world.

The report from the recently completed OIDC/OAuth2 Survey Working Group, confirmed that there is already a high volume of campus-based activity exploring the use of the OIDC-related protocols, and particularly OAuth2. That report identified three trends driving this interest:

- The adoption of API-centric application architecture - organizations need to enable end-to-end authentication and authorization between SSO-enabled web applications and the APIs behind the applications.
- Native (mobile) application deployment - campuses are deploying native mobile applications seeking compatible authentication and authorization solutions for native applications accessing campus resources (usually in the form of API).
- Social and SaaS platform integration - organizations either need to support social identities in their applications, or need to integrate campus SSO with Social/SaaS applications that only support OIDC/OAuth.

Today, most of this activity is intra-campus, providing a campus community with easier access to local applications. However, several of the submitted use cases were intra-system (multi-campus systems) and required some form of Federation support. The previous Working Group expected that inter-campus Federated use cases will begin to emerge, and recommended that a follow-on Working Group identify common practices and standards so that interoperation will be easier for the expected inter-campus use cases. (Already the TIER-API Working Group has proposed an approach to API authentication that includes reliance on federated OAuth2 - see TIER API Authentication in a Federated World.) It is not yet clear where the intra-campus, intra-system, and inter-campus uses overlap (and do not overlap). However, Shibboleth/SAML has evolved to directly address all three scenarios, and does so with a single set of solutions. That is the vision of how campus-based OIDC/OAuth2 use might be managed, and how these two efforts (TIER Software development and InCommon) might facilitate that outcome. The recommendations of this Working Group should move us toward that vision, to the greatest extent possible.

The previous group recommended a number of next steps. This Charter is derived from their recommendations. This Charter specifies a number of Work Products. They are related (they all have to do with OIDC/OAuth2), but in most cases they are not dependent on each other. It is hoped, therefore, that work can progress in parallel on several of these items, rather than addressing the items in a sequential manner within the “working Group as a whole”.

Charter

1. Review recommendations from the previous WG and determine what is In Scope (and out of scope) for this WG. This should pay particular attention to what was determined to be campus-specific (TIER/CACTI WG?) vs. Federation-specific.
2. Create channels for sharing information within and from the existing Higher Ed OIDC/OAuth2 deployers and interested parties. The international Higher Ed community should be asked to participate. This could include email lists, wiki pages, and regular webinars.
3. Track and document the lessons learned; develop recommended practices for deployment, configuration, and use. Document the software architectures campuses are currently using to provide OIDC/OAuth2 services.
4. Report on the ways campuses are using OIDC and OAuth2. This includes identifying those aspects of the protocol definitions that campuses are not using.
5. Work with the organizations that are currently implementing these use cases to identify areas where organizations would be helped by increased standardization (e.g., use of OIDC claims, development of deployment profiles, etc.).
6. Work within existing efforts or create new efforts to develop the required standards. New efforts might be created within existing standards bodies (e.g., I2 T&I, REFEDS, Kantara, http://openid.net/ , etc.)
    a. Develop or adopt a higher education deployment profile for OIDC/Oauth (e.g., profile similar in concept to the one for healthcare: http://openid.net/wg/heart/)
    b. Ensure the development of a Higher Ed attribute schema for OAuth2 claims (i.e., map eduPerson schema to OIDC/OAuth compatible format, likely in JSON Web Token forms), possibly by participating in the current European effort: Mapping SAML Attributes to OIDC Claims.
    c. Track (and possibly participate in) the GEANT OpenID Connect Federation task chaired by Maarten Kremers. This effort includes Roland Hedberg's efforts to develop an OAuth federation framework.
7. Develop and share information about best practices with native mobile application authentication using SAML and OIDC/OAuth2.

8. Identify use cases that require multilateral federation support, and bring them forward to the TAC and Internet2 T&I.

Work Products

1. Document above Charter items on Working Group Wiki in an organized manner:
    a. Define the scope of this effort.
    b. Channels for sharing information (e.g. email lists, wiki pages, and regular webinars)
    c. Track and document use cases and lessons learned; Develop and share best practices. Describe how campuses are using these protocols (and which ways of using them that campuses are not using).
    d. List areas where organizations would be helped by increased standardization
    e. Identify areas requiring more standardization, and facilitate the development of those standards, as required (Work within existing efforts or create new efforts to develop the required standards)
    f. Identify use cases that require multilateral federation support
2. Work within existing efforts or create new efforts to develop the required standards.
3. The group should submit a draft status report to the TAC by TechX 2017 (Oct. 15, 2017). This DRAFT should include an initial list of issues and concerns that Higher Ed Federations will have to address in order to provide their members with a manageable framework for using Federated OIDC/OAuth2.

Objectives

Note: unless otherwise noted, this working group is focused on organizations in the Higher Education community.

1. Refine scope
    a. Review recommendations from the previous WG
    b. Define scope for this WG
2. Share information
    a. Collect and share learning materials
    b. Facilitate information sharing among deployers and interested parties
    c. Coordinate with international community
    d. Examples: email lists, wiki pages, conference calls, trainings, workshops, and regular webinars
3. Develop best practices
    a. Document OIDC and OAuth2 use cases
    b. Document lessons learned
    c. Include what is and is not being used
    d. Include software architectures in use including SAML IdPs and proxies
    e. Include native mobile application authentication using SAML and/or OIDC/OAuth2
    f. Consider campus-specific vs. federation-specific
    g. Identify use cases that require multilateral federation support
    h. Develop recommended practices for deployment, configuration, and use
4. Guide standardization
    a. Identify where increased standardization would benefit organizationn
    b. e.g., Map SAML Attributes to OIDC Claims
    c. e.g. map eduPerson schema to OIDC Claims
    d. e.g. develop profile similar to healthcare, iGov, financial
    e. Facilitate related standardization
    a. Work within existing standardization efforts
    b. Or create new efforts
5. Support multilateral federation
    a. Identify issues R&E federations must address to provide federated OIDC/OAuth2
        i. Include metadata, discovery, etc.
    b. Coordinate with GEANT OpenID Connect Federation
        i. https://wiki.geant.org/display/gn42jra3/T3.1A+OpenID+Connect+Federation
        ii. Part of GN4-2 JRA3 – Meeting notes include OIDCfed meetings
        iii. Includes Roland Hedberg's efforts to make OIDC “federation and interfederation capable”
        iv. Includes potential OIDC profile for eduGAIN
        v. Includes implementation blueprint requirements
        vi. Includes OJOU (OAuth2/JW*/OIDC/UMA) training courses – e.g. November 2017
    c. Coordinate with REFEDS OIDCre working group
        i. https://wiki.refeds.org/display/GROUPS/OIDCre
        ii. Includes OIDC Federation; carried out with help from GEANT OIDC Federation (above)
            1. Refers to OIDC Federation draft specification
            2. Refers to OIDCfed test suite
            3. Refers to Roland's federation-aware RP and OP implementations
            4. Refers to Ioannis and Andres federation-aware OP (based on pyoidc)
            5. Refers to Andreas federation-aware OIDC NodeJS library
            6. Refers to Janusz federation-aware OIDC PHP library
            7. Refers to Janne & Henri adding OIDC functionality to Shibboleth
            8. Refers to Herve, Jule and Maarten interviewing federations on plans, requirements, and use cases
        iii. Includes SAML to OIDC mapping
        iv. Refers to Registration in the IANA JSON Web Token Claims registry
        v. Refers to Report on mapping of the R&S bundle in OIDC
        vi. Refers to AARC2
            1. Includes MJRA1.3-Design-for-the-integration-of-an-Attribute-Management-Tool.pdf
                a. Includes SAML to OIDC mappings (§3.2)
            2. Includes AARC2 JRA1.2B – OIDC-based services in research collaborations

3. Includes AARC2 JRA1.3B – Guidelines for registering OIDC Relying Parties in AAIs for international research collaboration

vii. Referred to by CILogon OIDC
   1. To establish OIDC interoperability profiles
   2. Recommends use of Certificated OIDC implementations

d. Coordinate with AARC2?
e. Coordinate with IGTF for Research and e-Infrastructures?
f. Present to TAC and Internet2 T&I