UMA Implementations

This page gathers information about implementation efforts and interest, along with interoperability testing plans. Maciej Machulak is the UMA group's implementation coordinator. Key existing implementations that we know about are noted below, in alphabetical order of the project or organization.

Date labels indicate when an entry was added or last updated on this page. Implementers are welcome to get in touch with the implementation coordinator or any member of the leadership team to add entries or make corrections.

ForgeRock

MAR '20 The company ForgeRock (also at @ForgeRock) has an Identity Platform that includes an implementation of UMA 2.0, with both an "UMA Provider" (authorization server component) and an "UMA Protector" (resource server component), targeted at individual consent and data sharing use cases. The case studies Users Managing Delegated Access to Online Government Services and and Aggregating and Sharing Pension Information were based on POCs performed with earlier versions of the ForgeRock Identity Platform. In addition, ForgeRock has developed an open-source resource server reference implementation (also available and further described on the ForgeRock Marketplace, and in a series of blog posts – Why ForgeRock Secure Sharing: Trust and Enforce, ForgeRock Secure Sharing Ingredients: Who, What and How, and ForgeRock Secure Sharing: The Framework).

Gluu

MAY '18 Open source software vendor Gluu (Twitter @GluuFederation) has implemented UMA 2.0 Authorization Server endpoints (including claims gathering) since Gluu Server 3.1.2. The Gluu Gateway is an API Gateway that can use UMA (acting as the RS) to enable admins to specify which UMA scopes are required to access certain API's. Gluu also provides a free open source middleware service, oxd, that makes it easy for Clients and RS software developers to use UMA, and enables the generation of client libraries using an OpenAPI (Swagger) document. The Gluu Server is used to map policies to UMA scopes. Policies are defined in python-syntax scripts. If policy fails, the Gluu Server claims gathering interception scripts enable admins to define multi-step workflows. For example, claims gathering can be implemented to support stepped-up authentication. Claims gathering also can be used to implement policy where the web browser cookie (i.e. SSO session) is preferred to gather user claims, versus using the pushed claim token mechanism.

HealthyMePHR

MAR '18 HealthyMePHR, which enables secure patient-mediated clinical data exchange, was implemented by Lush Group, Inc. It implements UMA 1.0, with plans to update to full UMA 2 support. The software is currently in prototype form. It implemented the HEART profiles in conjunction with HEART specification development; it consists of a FHIR-based RS, AS and Client.

HealthyMePHR was selected as a Phase 2 winner of The Department of Health and Human Service's Move Health Data Forward Challenge. Since the intention was to free the patient from the many roadblocks currently in place, the implementers wanted to implement a wide ecosystem for exchange, adding an external OpenID Connect IdP to support that goal. Since other components were not available at the time of development, the solution was developed to be free standing. It is the intention that any of the components could be substituted. While the initial client is a HEART based viewer, it is actually accessing discrete data. This approach demonstrates an important building block for accessing discrete data via an API, under the control of patient-directed consent. HealthyMePHR has also been connected to EMRs via CDS hooks, providing physician's with the ability to access the patient's data which may be external to the EMR. For more information, see the Case Studies page or contact info@lgisoftware.com.

HIE of One - Trustee

JAN '19 The HIE of One open-source project is run by Michael Chen, MD and Adrian Gropper, MD. It implements an UMA2 authorization server, and supports dynamic client registration for resource servers and clients. HIE of One serves as an OpenID Connect relay to other OIDC services, such as Google and Twitter. This authorization server is meant to be deployed as a single instance per patient (user). It is licensed through GNU AGPLv3. Support information is available at the distro link. "Trustee" is an application using HIE of One. A demonstration video can be seen here.

HIE of One acts as a Health Information Exchange service but under control by the patient themselves. It is coupled in the same root domain URL with a resource server that acts as a patient-centered health record (NOSH ChartingSystem), although they are two separate projects. HIE of One allows the patient to control user-managed access to her resources served by NOSH ChartingSystem using a specific RESTful API (FHIR) for health-related information. This allows other third-party applications to take advantage of the patient's health-related information in a secure and privileged manner, governed by the user and not by another third party.

HIE of One is not in production at this time; fully working code is in GitHub and is used for current demonstration of how HIE of One is coupled with NOSH ChartingSystem for the above functionality.

This implementation leverages third-party OAuth and OpenID Connect implementations Google OAuth2, Twitter OAuth2, and mdNOSH (this is for demo purposes for physician single-sign-on, not federated). HIE of One also implements blockchain-based authentication using the uPort implementation and the project is tracking the Decentralized ID (DID) standards for self-sovereign identity and W3C verifiable claims as these progress.

IDENTOS Federated Privacy Exchange (FPX)

FEB '19 IDENTOS Inc. (Twitter @Identos_Inc) has profiled UMA 2.0 to change the rules of Digital Identity and Access Management by putting the citizen in control of their privacy. The open standard specification (Federated Privacy Exchange - FPX) is an ecosystem scheme that taps into the power of UMA 2.0 to enable user-centric interoperability at scale, and offer people, organizations and things a frictionless way to establish digital trust. FPX covers all entities, and includes a new AS first path for the Client. IDENTOS has an AS implementation, and an adapter to help entities onboard as an RS.

The Federated Privacy Exchange was created as a response to an innovation challenge released by the Ontario Government's Ministry of Government and Consumer Services (MGCS) to deliver a privacy-respecting consumer digital identity solution. FPX was built in the image of the Pan-Canadian Trust Framework to bootstrap conformance to many international privacy and security regulations.

PatientShare

NOV '19 PatientShare empowers patients to safely share their health records with users of their choice in an interoperable way. This approach respects and honors patient security and privacy. PatientShare implements UMA 2 and HEART. It includes an enterprise FHIR-based RS, AS and HEART client. It is designed to easily integrate with any health data repository. While the initial client is a HEART-based viewer, it is actually accessing discrete data. This approach demonstrates an important building block for accessing discrete data via an API, across a wide ecosystem, under the control of patient-directed consent. PatientShare has also been connected to EMRs via CDS hooks, providing physicians with the ability to access the patient's data which may be external to the EMR. PatientShare was derived from HealthyMePHR, by Lush Group, Inc, which was a Phase 1 and 2 winner of The Department of Health and Human Service's Move Health Data Forward Challenge.

PatientShare is a product of Patient Centric Solutions, Inc. For more information contact info@patientcentricsolutions.com.

Pauldron

Pauldron is an open-source (MIT license) UMA authorization server, with several extensions catering to use cases that have come out of healthcare-related work in the HL7 environment, available on GitHub.

RedHat KeyCloak

AUG '18 RedHat's KeyCloak (also at @Keycloak) open-source authorization services offering supports UMA2, targeting primarily enterprise use cases (where "the RS is the RO" – the enterprise hosts the resources, and also serves as its own authorization server). Except for the interactive claims gathering flow, most of the specification is implemented, including resource registration. A simple example app (photoz) using UMA is provided. The protection API has been extended to include a new endpoint to manage user permissions (policies). This was a result of contributions from the community in order allow RSs to associate/manage custom policies for resources while still letting users manage them. Another extension allows the RS to push claims when creating a permission ticket. (See more discussion of this extension in this thread.)

WSO2

OCT '18 Open-source company WSO2 (also at @WSO2) has implemented UMA2 in its Identity Server 4.7.0 product. A demonstration recording is available.

Jericho Systems

In 2016 the company Jericho Systems announced a product, EnterSpace 9, with UMA support as follow-on to its Consentral on FHIR product.

MITREid Connect

The open-source MITREid Connect project has UMA1 support. An experimental branch called MPD (for "multi-party delegation") has been used as a sandbox for UMA2 features, but has not yet been updated to full UMA2 support.

SMART project (non-healthcare-related)

This older Java implementation includes an **UMA/j** framework and sample applications. See the SMART blog. The OAuth portion, originally named **leeloo**, was contributed to Apache Amber (now Apache Oltu, which is going to include OpenID Connect and good JWT support too). Part the SMART project involves development of set of open-source Python libraries, called Puma, for UMA-enabling web apps to become UMA resource servers and clients. Note that this SMART project is distinct from the SMART health IT initiative.

Synergetics

The company Cloud Identity Limited (since acquired by Synergetics) developed an UMA Authorization Server - NuveAM (Online Demo).
NuveAM implements the UMA protocol and supports other open standards including OAuth 2.0, OpenID Connect, and SAML 2.0. The company also developed Java and Python SDKs. More information is on the company's website and the company's YouTube channel. The company integrated UMA with its NuveLogin service to simplify the flow for Resource Server and Client applications.

Telia

The Telia telecom company has an identity solution that provides UMA support.

Universidad de Alcalá Telematic Services Engineering Group

This Python implementation, part of the European Union-funded project SITAC, focuses on IoT use cases. See a video here.