(1) WG NAME: *(and any acronym or abbreviation of the name): The WG name, acronym and abbreviation must not include trademarks not owned by the Organization, or content that is infringing, harmful, or inappropriate.*

User-Managed Access (UMA) Work Group

(2) PURPOSE: *Please provide a clear statement of purpose and justification why the proposed WG is necessary.*

The UMA 2.0 Recommendations define a) a means for a client, representing a requesting party, to use a permission ticket to request an OAuth 2.0 access token to gain access to a protected resource asynchronously from the time a resource owner authorizes access and b) a means for an UMA-enabled authorization server and resource server to be loosely coupled, or federated, in a secure and authorized resource owner context.

The purpose of this Work Group is:

- To maintain the UMA specifications and consider developing enhancements to and any future versions of them
  - For example, to consider whether extension and profile proposals contributed to the Work Group should result in Work Group deliverables
- To develop Business Model reports and/or specifications that support the enablement of a license-based model for controlling access rights to personal digital assets, in liaison with other relevant bodies
  - For example, working with the Kantara Consent and Information Sharing Work Group
- To promote UMA adoption
  - For example, by offering support for profiling and extension creation and creating educational materials
- To promote interoperability of independent implementations of UMA

(3) SCOPE: *Explain the scope and definition of the planned work.*

Deliverables must meet the following core design principles:

- Simple to understand, implement in an interoperable fashion, and deploy on an Internet-wide scale
- OAuth-based to the extent possible (while contributing bug reports and RFEs around extensibility, security, and privacy to the IETF OAuth group)
- Agnostic as to the identifier systems used in an individual's various services on the web, in order to allow for deployment in "today's Web"

- Resource-oriented (for example, as suggested by the REST architectural style) and operating natively on the Web to the extent possible
- Modular (e.g., incorporating other existing specifications by reference where appropriate, and breaking down this Work Group's draft specifications into multiple pieces where reuse by different communities is likely)
- Generative (able to be combined and extended to support a variety of use cases and emerging application functionality)
- Developed rapidly, in an "agile specification" process that can refactor for emerging needs

They must also meet the following additional design principles:

- Avoid cryptography: avoid adding crypto burdens as part of the simplicity goal
- Protect privacy: protect the privacy of the resource owner and requesting party
- Avoid complexity: complexity should be borne by the authorization server vs. the resource server or client, if possible
- Outsource authentication: UMA should stay out of the authentication business as much as possible
- Consider user experience: ease of end-user experience should inform UMA's protocol design
- Permit digital signatures: don't preclude strong authentication through digital signatures, and leverage widely supported signature solutions as options if a reasonable measure of interoperability can be achieved

They must also meet the following ~~basic~~ functional requirements~~, in addition to specific use cases and requirements later identified by this Work Group~~:

- Support the notion of a distinct online service for managing data-sharing and service- and device-access relationships ("access relationships" for short) between an individual and ~~his or her online services~~ other parties that request such access
- Allow a person (individual or legal person) to select policies and enforceable contract terms that govern access, as well as data storage, further usage, and further sharing on the part of requesting services
- Allow a person to conduct short-term and long-term management of access relationships, including modifying the conditions of access or terminating the relationship entirely
- Allow a person to audit and monitor various aspects of access relationships
- Allow requesting services to interact directly with responding services in a fashion guided by policy while an individual is offline, reserving real-time user approval for extraordinary circumstances
- Allow requesting services to interact with multiple responding services associated with the same individual

(4) DRAFT TECHNICAL SPECIFICATIONS: *List Working Titles of draft Technical Specifications to be produced (if any), projected completion dates, and the Standards Setting Organization(s) to which they will be submitted upon approval by the Membership.*

The following technical specifications may be developed in 2018:

- One or more extension and/or profile specifications
- Business Model Clause Templates for User-Managed Access (this may be a report instead; final title to be determined)

(5) OTHER DRAFT RECOMMENDATIONS: *Other Draft Recommendations and projected completion dates for submission for All Member Ballot.*

The following reports are anticipated to be developed in 2018 (final titles and document boundaries to be determined):

- A Licensing-Based Model for User-Managed Access
- Business Model Scenarios for User-Managed Access
- Additional business model-related reports

(6) LEADERSHIP: *Proposed WG Chair and Editor(s) (if any) subject to confirmation by a vote of the WG Participants.*

At the time of this charter's revision, following are the members of the leadership team:

- Chair: Eve Maler, ForgeRock
- Vice-chair: Maciej Machulak, HSBC
- Graphics and User Experience Editor: Domenico Catalano, Oracle
- Implementations Coordinator: Maciej Machulak, HSBC

(7) AUDIENCE: *Anticipated audience or users of the work.*

The anticipated audience for the documents produced by this Work Group includes developers, deployers, and designers of digital services, including IoT device ecosystems, that act on behalf of natural and legal persons, including legal representatives of organizations operating such services. ~~The group also anticipates gathering input from individual users of online services in order to respond to their needs and preferences.~~

(8) DURATION: *Objective criteria for determining when the work of the WG has been completed (or a statement that the WG is intended to be a standing WG to address work that is expected to be ongoing).*

This is intended to be a standing Work Group to address work that is expected to be ongoing.

(9) IPR POLICY: *The Organization approved Intellectual Property Rights Policy under which the WG will operate.*

Kantara IPR Policy - Option Patent & Copyright: Reciprocal Royalty Free with Opt-Out to Reasonable And Non discriminatory (RAND) (HTML version)

10) RELATED WORK AND LIAISONS: *Related work being done in other WGs or other organizations and any proposed liaison with those other WGs or organizations.*

This Work Group has a number of dependencies on, and shared goals with, the output of other efforts. The Kantara groups and external efforts with which this Work Group intends to liaise informally include (but are not limited to):

- Kantara Consent and Information Sharing Work Group
- Kantara Consent Management Work Group
- OpenID Foundation HEART Work Group
- Open Identity Exchange
- IETF OAuth Working Group

(11) CONTRIBUTIONS (optional): *A list of contributions that the proposers anticipate will be made to the WG.*

The draft ProtectServe protocol flow diagrams were contributed.

(12) PROPOSERS: *Names, email addresses, and any constituent affiliations of at least the minimum set of proposers required to support forming the WG.*

The original proposers of the Work Group were:

- J. Trent Adams, ISOC
- Hasan Akram, Fraunhofer Institute of Secured Information Technology
- Joe Andrieu (individual participant affiliated with SwitchBook)
- Gerald Beuchelt (individual participant affiliated with MITRE)
- Paul Bryan, Sun Microsystems
- Andy Dale (individual participant affiliated with OCLC)
- Iain Henderson (individual affiliated with Mydex CIC)
- Hubert Le Van Gong, Sun Microsystems
- Mark Lizar (individual affiliated with Identity Trust CIC)
- Eve Maler, Sun Microsystems
- Andrew Nash, PayPal
- Drummond Reed, Information Card Foundation
- Christian Scholz, DataPortability.org

- Paul Trevithick (individual participant affiliated with Azigo)
- Robin Wilton (individual participant affiliated with Future Identity)