(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 purpose of this Work Group is threefold:

- To develop a set of draft specifications that enable a resource owner to control the authorization of data sharing and other protected-resource access made between online services on the owner's behalf or with the owner's authorization by an autonomous requesting party, and to facilitate the development of interoperable implementations of these specifications by others. It is a particular priority in this effort to enable and empower individual people in the resource owner role, for the purpose of gaining personal control of his or her personal information.
- To develop contractual framework specifications that facilitate establishing obligations to which operators and users of services taking part in access-related interactions must adhere, and to encourage the adoption of the framework in identity and access federations and other ecosystems that enable distributed authorization. It is a particular priority in this effort to enable setting the rules of engagement for informed, meaningful control of access.
- To develop or facilitate the creation of one or more technical-level and business-level profiles that enable the interconnection of interoperable UMA-compliant ecosystems with high-value, privacy-preserving identity federations and ecosystems.

Specifically, this Work Group is responsible for:

- Developing use cases and requirements to guide the specification design work
- Developing modular draft specifications meeting these use cases and requirements, influenced by contributions as appropriate
- Developing contractual framework specifications as appropriate
- Developing deployment profiles as appropriate
- Developing and maintaining liaisons as appropriate with external bodies and other Kantara groups
- Fostering the creation of multiple interoperable implementations, particularly in open source
- Promoting progressive harmonization with existing specifications and protocols as appropriate
- Developing educational materials in support of the overall Work Group effort
- Overseeing the contribution of each resulting draft specification to a standards-setting organization

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

The specifications must 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-access relationships ("access relationships" for short) between an individual and his or her online services that request such access
- Allow an individual 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 an individual to conduct short-term and long-term management of access relationships, including modifying the conditions of access or terminating the relationship entirely
- Allow an individual 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

The specifications must meet the following basic design principles, in addition to any emergent design principles later identified by this Work Group:

- 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

(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.*

It is anticipated that the following technical specifications will be produced, with modular spec boundaries subject to change; both are anticipated to be submitted to the IETF for further work and completion:

- User-Managed Access (UMA) Profile of OAuth 2.0
- OAuth Dynamic Client Registration Protocol
- OAuth 2.0 Resource Set Registration
- Binding Obligations on User-Managed Access (UMA) Participants

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

It is anticipated that the following auxiliary materials will be produced, at a minimum:

- User-Managed Access Use Cases and Requirements
- User-Managed Access Overview
- User-Managed Access Implementation Guide

At the group's option, some of this material may be considered non-normative (equivalent to white papers), and some may be split up into multiple pieces (for example, an Overview document and companion slide deck).

(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, XMLgrrl.com
- Vice-chair: Maciej Machulak, Cloud Identity Ltd
- Technical specification editor: Thomas Hardjono, MIT
- Contractual framework editor: Dazza Greenwood, Civics.com
- Graphics/UX editor: Domenico Catalano, Oracle

(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 online services that act on behalf of individual users. 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 Work Group is an ongoing effort; it anticipates developing a draft V1.0 set of technical specifications and other auxiliary materials by the end of 2013, facilitating the development of multiple independent draft implementations as appropriate during this time, and a draft contractual framework soon after. This targeted duration and other aspects of this charter (except the IPR policy stated below) are subject to review, amendment, and extension as approved by the Kantara Leadership Council.

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

Kantara IPR Policy - Option Liberty

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):

- OASIS XACML Technical Committee
- OASIS XDI TC and other personal cloud standards efforts
- OpenID Foundation
- IETF OAuth Working Group

- Direct, Blue Button Plus, and other external and related Kantara healthcare groups

(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)

History

Date	Note
July 15, 2009	The Leadership Council ratifies this charter for operation.