UMA Requirements

Abstract

This document is a product of the User-Managed Access Work Group. It records the specific requirements governing the development of the User-Managed Access protocol and guiding associated implementations and deployments.

Status

This document is now **historical/obsolete**. To see the current list of design principles and requirements, see the Work Group charter.

Editors

- Eve Maler

Table of Contents

Introduction

This document is a product of the User-Managed Access Work Group. It records the specific requirements governing the development of the User-Managed Access protocol and guiding associated implementations and deployments.

Each requirement has a number, a short title, normative requirement text, and optionally further explanation that is informational. Please copy and revise an existing requirement in adding new ones. Following are the meanings of the status keywords:

- **Proposed:** Status when first submitted or still under discussion
- **Approved:** Needs to be met in UMA V1 and/or its associated compliant implementations
- **Deferred:** Relevant to the problem space; may be considered in future versions
- **Rejected:** Out of scope

Design Principles

The UMA Work Group charter states some design principles that shape the nature of our work. In addition, we have identified emergent design principles in the course of the work.

DP#	Title	Original Design Principle	Explanation/commentary
DP1	Simple	Simple to understand, implement in an interoperable fashion, and deploy on an Internet-wide scale	
DP2	OAuth	OAuth-based to the extent possible	We may contribute bug reports and RFEs around extensibility, security, and privacy to the IETF OAuth group.
DP3	ID-agnostic	Agnostic as to the identifier systems used in an individual's various services on the web	This is in order to allow for deployment in "today's Web".
DP4	RESTful	Resource-oriented (for example, as suggested by the REST architectural style) and operating natively on the Web to the extent possible	
DP5	Modular	Modular	For example, 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.
DP6	Generative	Generative	Able to be combined and extended to support a variety of use cases and emerging application functionality.

DP7	Fast	Developed rapidly	In an "agile specification" process that can refactor for emerging needs.

DP#	Title	Emergent Design Principle	Explanation/commentary
DP8	Cryptography	We should avoid adding crypto burdens as part of our simplicity goal	Avoid adding crypto requirements beyond what existing web app implementations do today. This principle was discussed on 2009-09-10.
DP9	Privacy	Protect the privacy of the Authorizing User	The protocol should not provide ways to breach the Authorizing User's privacy, though out-of-band methods are beyond our control. Also, this principle should not be construed as support for protecting the privacy of other parties, or even the same person in a different role (the Requesting User). This principle was discussed on 2009-10-08.
DP10	Complexity	Complexity should be borne by the AM endpoint vs. the host or requester, if possible	We anticipate dozens of AMs (maybe lots more if corporations have them), hundreds of thousands of hosts, and hundreds of millions of requesters. This principle was discussed on 2009-11-02.
DP11	Authentication	Stay out of the authentication business as much as possible	There are many technology choices here. Some scenarios may need stronger authentication. OAuth will be our preferred means of service authentication per DP2, but even it could be supplanted. This principle was discussed on 2009-11-02.
DP12	User experience	Ease of end-user experience should inform our protocol design	Even though the goal for authorizing users is to allow them to set policy that can applied without inconvenience to them at run-time, the mechanisms of introducing hosts to AMs, setting policy at AMs, auditing access at AMs, and provisioning resource locations to requesters should be as easy as possible. This principle was discussed on 2010-03-18.
DP13	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	We see opportunities to leverage JSON Web Tokens, which didn't exist when the group was first launched, and we have more overall experience with judging what is "reasonable" vs. "undue" crypto burdens now (see DP8, "Cryptography"). This principle mitigates the potentially heavy-handed effects of DP1 ("Simple") and DP10 ("Complexity") in forcing bearer tokens as a universal solution. Finally, this principle is consistent with DP11 ("Authentication") if we leverage a widely supported external solution for digital signatures and avoid defining a whole new one. This was discussed primarily on 2011-01-27 and 2011-02-10.

Approved Requirements

The requirements with numbers starting at zero all come from the UMA Work Group charter, and were thus approved when the group was launched.

R#	Title	Requirement	Explanation/commentary
R0a	Access relationship service	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.	
R0b	User-driven policies and terms	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.	
R0c	User management of access relationship	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.	
R0d	Auditing	Allow an individual to audit and monitor various aspects of access relationships.	
R0e	Requester-Host direct access	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.	
R0f	Multiple Hosts	Allow requesting services to interact with multiple responding services associated with the same individual.	
R1	Host/AM separation	It must be possible to provide Host and AM functions in separate Web domains.	Approved on 2009-10-01.
R2	Resource orientation	User data access and service access must be enabled through accessing Web resources that have URLs.	Approved on 2009-10-01.
R3	Correlation of Authorizing User by multiple Hosts	For resources at Host X and resources at Host Y, X and Y must not find out, through their relationship with the AM, that the same Authorizing User uses the other Host.	Approved on 2009-10-15.
R4	Representation-agnostic AM	The AM is not required to understand the representations of resources it is charged with protecting.	Examples of differential filtering of resources include photos of different resolutions, calendars covering different time periods or levels of detail, and locations at address vs. city level. Approved on 2009-10-15.

Proposed Requirements

Crossed-out numbers indicate proposed requirements that have been discussed and rejected. Bold numbers indicate proposed requirements that have been discussed and accepted, in some form, in the list above.

P#	Title	Requirement	Explanation/commentary
P1	Representation-agnostic AM	The AM is not required to understand the representations of resources it is charged with protecting.	We reworded this heavily and approved it on 2009-10-15 as R4.
P2	Terms persistence	A set of terms for accessing a resource must be accessible as a Web resource with a URL.	
P3	Host impersonation of Requesters	A Host must not be able to impersonate Requesters in interacting with an AM.	This came up on 2009-10-01.
~~P4~~	Host correlation of multi-Requester activity	A Host must not be able to correlate the same Authorizing User's activity at multiple Requester applications.	Discussed on 2009-10-08; this is wrongly stated and should be rejected. See P9 for a replacement. Officially rejected on 2009-10-15.
P5	User AM choice	The UMA protocol must not negatively impact a User's prerogative to choose or even self-host the AM that will protect a resource on any Host.	
P6	Host following authorization instructions	A Host must allow or deny Requester access to a resource according to a User's desires as conveyed by an AM access decision, or inform the AM of instances where the User wished to grant access but the Host did not or could not.	
P7	User-defined constraint on access	A Host must not grant a Requester access to a resource in cases where the AM gave instructions denying access.	
P8	Access audit log	A Host must inform the AM protecting a particular resource on that Host in a timely way of all successful Requester access events.	
P9	Correlation of Authorizing User by multiple Hosts	For two resources on different Hosts owned by the same Authorizing User and managed by the same AM, the AM must not allow one Host to be able to discover the User's relationship with the other Host.	For example, a user might use the same AM to protect resources at LinkedIn along with their personal interests and hobbies. We reworded this on 2009-10-15 and approved it as R3.
P10	POST once	Ensure that it's possible for AMs to offer a "POST once" setting.	This is critical for payments and the like.
P11	Verifiable claims	Ensure that access-agreement claims have the option of being independently verifiable.	In a lot of cases, self-asserted claims are acceptable for forging access agreements, but having the option of claims that are verifiable by third parties – such as mediators in a dispute – can allow for stronger agreements in a legal sense. This was discussed on 2009-12-10.

Change History

Version	Date	Comment
Current Version (v. 15)	**Mar 08, 2018 07:20**	**Eve Maler**: With the 2018 charter refresh, decided to incorporate all active DPs and requirements.
v. 14	Dec 15, 2015 14:39	**Eve Maler**
v. 13	Feb 10, 2011 23:06	**Eve Maler**: Migration of unmigrated content due to installation of a new plugin
v. 12	Feb 10, 2011 23:06	**Eve Maler**: Migration of unmigrated content due to installation of a new plugin
v. 11	Feb 10, 2011 23:06	**Eve Maler**: Migration of unmigrated content due to installation of a new plugin
v. 10	Feb 10, 2011 23:06	**Eve Maler**: Migrated to Confluence 4.0
v. 9	Feb 10, 2011 23:06	**Eve Maler**: New emergent design principle #13 on "digital signatures" added.
v. 8	Mar 20, 2010 13:57	**Eve Maler**: Add DP12 as discussed on 2010-03-18
v. 7	Dec 16, 2009 21:02	**Eve Maler**
v. 6	Nov 12, 2009 11:00	**Eve Maler**
v. 5	Nov 03, 2009 12:39	**Eve Maler**: Added new emerging design principles generated during the first half of UMA F2F 2009-11-02
v. 4	Oct 16, 2009 13:45	**Eve Maler**: General editorial changes, and decisions made 2009-10-15
v. 3	Oct 08, 2009 15:20	**Eve Maler**: Added the requirements that were pre-approved as part of the charter approval process
v. 2	Oct 08, 2009 15:11	**Eve Maler**: Added notations to P4, added P9, and added section for Design Principles
v. 1	Oct 01, 2009 16:23	**Eve Maler**