

# 2017-11-30 Meeting notes (CR)

## Date

2017-10-26

## Status of Minutes

Approved

Approved at: [2019-12-12 Meeting notes \(CR\) DRAFT](#)

## Attendees

### Voting

- [Andrew Hughes](#)
- Mark Lizar
- Jim Pasquale
- John Wunderlich
- Mary Hodder

### Non-Voting

- Chris Cooper
- David Turner
- Robert Lapes
- Colin Wallis

## Regrets

### Quorum Status

Meeting was quorate

### Voting participants

[Participant Roster \(2016\)](#) - Quorum is 5 of 9 as of 2017-11-20

Iain Henderson, Mary Hodder, Harri Honko, Mark Lizar, Jim Pasquale, John Wunderlich, Andrew Hughes, Rupert Graves, Rachel O'Connell

## Discussion Items

Time	Item	Who	Notes
4 mins	<ul style="list-style-type: none"><li>• Roll call</li><li>• Agenda bashing</li></ul>	<a href="#">Andrew Hughes</a>	<ul style="list-style-type: none"><li>•</li></ul>
1 min	<ul style="list-style-type: none"><li>• Organization updates</li></ul>	All	<p>Please review these blogs offline for current status on Kantara and all the DG/WG:</p> <ul style="list-style-type: none"><li>• <a href="#">Director's Corner</a></li><li>• <a href="#">Working + Discussion Group Activity</a></li></ul> <p>There is a new wiki page that will hold all the known <a href="#">implementations of Consent Receipts</a> - Please update the page or inform Andrew of your implementation.</p>

30 min	Recent events updates	All	<ul style="list-style-type: none"> <li>• Kuppinger Cole event in Paris went very well <ul style="list-style-type: none"> <li>• Pre-conference workshop</li> <li>• Facebook seems very interested in the transparency aspects</li> </ul> </li> <li>• Colin is seeking additional speakers for the Singapore event - branch office contacts, etc?</li> <li>• Mark talked about the January 29, 2018 international privacy event that is in planning stages</li> </ul>
	UMA WG joins the call	All	<ul style="list-style-type: none"> <li>• Eve outlined the joint agenda</li> <li>• CIS WG described current status of the work <ul style="list-style-type: none"> <li>• the v1.1 draft has passed WG ballot and is getting ready for 45-day public review now</li> <li>• there are several known implementations</li> <li>• David described some of the technical details of the spec</li> <li>• there is a loose roadmap going forward <ul style="list-style-type: none"> <li>• Contribution to ISO</li> <li>• Forking a 'personal data privacy receipt' concept</li> <li>• Further development for specific use cases</li> </ul> </li> </ul> </li> <li>• UMA WG Presented on current status <ul style="list-style-type: none"> <li>• UMA v2.0 is at all-member ballot stage right now</li> <li>• In UMA 1 there was 'core' plus 'resource set registration' - but it was a bit of a fragment</li> <li>• UMA 2.0 is 2 documents ('Grant' and 'Federated Authorization') - different reorganization of the content from v1 <ul style="list-style-type: none"> <li>• UMA (core) is now written an extension grant of OAuth - a thin layer on top of OAuth - easier for OAuth developers to use <ul style="list-style-type: none"> <li>• Fed Authz is now an 'optional module' of UMA v2</li> <li>• Read the introductions to learn about what each doc covers</li> </ul> </li> </ul> </li> <li>• UMA extension now allows an asynchronous access policy - defining conditions for a future requesting party to meet. OAuth today is a synchronous access policy - when you go to grant access the user must permit or deny immediately <ul style="list-style-type: none"> <li>• Note that UMA conceives of the Authorization Server to be distinct from the Resource Server. Also the Resource Owner is a different entity from the Requesting Party.</li> <li>• Eve describes it as similar to granting access to Google docs</li> </ul> </li> <li>• UMA github has a 'shoebox' endpoint bunch of issues where 'receipts' and other notifications can be posted <ul style="list-style-type: none"> <li>• What can be proven with an audit trail?</li> <li>• The consent receipt is based on research into privacy compliance commonality - notice and consent are the most frequent point of commonality with respect to transparency <ul style="list-style-type: none"> <li>• It captures the notice requirements for consent</li> </ul> </li> </ul> </li> <li>• Note that in the regulations, there is no real concept for person-person data protection <ul style="list-style-type: none"> <li>• But the 'licensing' concept in UMA Legal is the groundbreaking aspect here - it allows for a person-person concept</li> <li>• Consentua's platform allows a business to plug in and get data from a person <ul style="list-style-type: none"> <li>• There is a shift in regulation so that the person 'owns' the data, not the business</li> <li>• Adoption is driven by commercial need - has to be easy to consume and allow engineers to build the tools for this new orientation</li> </ul> </li> </ul> </li> <li>• Could the UMA AS be a place to 'send' receipts? <ul style="list-style-type: none"> <li>• A 'shoebox API'</li> </ul> </li> <li>• Andrew starts to talk about role mapping between 'data controller &amp; data processor &amp; data subject' language from CR to 'Resource Owner, Resource Server, Requesting Party, Authorization Server' of UMA</li> <li>• Andrew asked if we could look at a use case where the Resource is Personal Data? <ul style="list-style-type: none"> <li>• Eve proposed the Origo use case (pensions data)</li> </ul> </li> <li>• Andrew posits that when a data subject and data controller agree on a data access or transfer, the data controller should be prepared to issue a consent receipt <ul style="list-style-type: none"> <li>• Eve proposes a 'role state transition matrix'</li> <li>• Whenever a data subject and data controller come to agreement, a receipt should be issued</li> </ul> </li> </ul> </li></ul>

- **Discussion**

- The link to the UMA WG [UMA telecon 2017-11-30](#)