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	• Roll call • Agenda bashing	Andrew Hughes	•
1 min	• Organization updates	All	Please review these blogs offline for current status on Kantara and all the DG/WG: • Director's Corner • Working + Discussion Group Activity There is a new wiki page that will hold all the known implementations of Consent Receipts - Please update the page or inform Andrew of your implementation.

30 min	Recent events updates	All	• Kuppinger Cole event in Paris went very well
			  • Pre-conference workshop
			  • Facebook seems very interested in the transparency aspects
			• Colin is seeking additional speakers for the Singapore event - branch office contacts, etc?
			• Mark talked about the January 29, 2018 international privacy event that is in planning stages

	UMA WG joins the call	All	• Eve outlined the joint agenda
			• CIS WG described current status of the work
			  • the v1.1 draft has passed WG ballot and is getting ready for 45-day public review now
			  • there are several known implementations
			  • David described some of the technical details of the spec
			  • there is a loose roadmap going forward
			  • Contribution to ISO
			  • Forking a 'personal data privacy receipt' concept
			  • Further development for specific use cases
			• UMA WG Presented on current status
			  • UMA v2.0 is at all-member ballot stage right now
			  • In UMA 1 there was 'core' plus 'resource set registration' - but it was a bit of a fragment
			  • UMA 2.0 is 2 documents ('Grant' and 'Federated Authorization') - different reorganization of the content from v1
			  • UMA (core) is now written an extension grant of OAuth - a thin layer on top of OAuth - easier for OAuth developers to use
			  • Fed Authz is now an 'optional module' of UMA v2
			  • Read the introductions to learn about what each doc covers
			  • 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
			  • 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.
			  • Eve describes it as similar to granting access to Google docs
			  • UMA github has a 'shoebox' endpoint bunch of issues where 'receipts' and other notifications can be posted
			  • What can be proven with an audit trail?
			  • 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
			  • It captures the notice requirements for consent
			• Note that in the regulations, there is no real concept for person-person data protection
			  • But the 'licensing' concept in UMA Legal is the groundbreaking aspect here - it allows for a person-person concept
			  • Consentua's platform allows a business to plug in and get data from a person
			  • There is a shift in regulation so that the person 'owns' the data, not the business
			  • Adoption is driven by commercial need - has to be easy to consume and allow engineers to build the tools for this new orientation
			• Could the UMA AS be a place to 'send' receipts?
			  • A 'shoebox API'
			• Andrew starts to talk about role mapping between 'data controller & data processor & data subject' language from CR to 'Resource Owner, Resource Server, Requesting Party, Authorization Server' of UMA
			• Andrew asked if we could look at a use case where the Resource is Personal Data?
			  • Eve proposed the Origo use case (pensions data)
			• 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
			  • Eve proposes a 'role state transition matrix'
			  • Whenever a data subject and data controller come to agreement, a receipt should be issued

- **Discussion**
  - The link to the UMA WG UMA telecon 2017-11-30