2017-05-25 Meeting Notes (CR)

Date

2017-05-25

Status of Minutes

Approved

Approved at: 2019-12-12 Meeting notes (CR) DRAFT

Attendees

Voting

- Andrew Hughes
- Mark Lizar
- John Wunderlich
- Jim Pasquale

Non-Voting

- David Turner
- Colin Wallis

> ⓘ **Quorum Status**
>
> Meeting was quorate

> ⓘ **Voting participants**
>
> Participant Roster (2016) - Quorum is 4 of 7 as of 2016-10-06
>
> Iain Henderson, Mary Hodder, Harri Honko, MarkLizar, Jim Pasquale, John Wunderlich, Andrew Hughes

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 • David Turner has been contracted to be the Spec Editor for v1.1 with a maximum duration of 6 months. • Andrew and Colin are in the process of signing up an organization to help develop 'Best Current Practice for Consent Management Solutions' (or similar name) as a Kantara Recommendation to support the Consent management work.

1 min	• Status of Consent Receipt Specification v1	Andrew Hughes	• Congratulations! • The Consent Receipt Specification v1.0 is now formally approved as a Kantara Recommendation • The document is now posted on the downloads page

40 min	Discuss work backlog priorities for CR v1.1	David	Github Issues: https://github.com/KantaraInitiative/CISWG/issues
			
			Consent Receipt v1.1 Work Backlog
			
			On Wed, May 10, 2017at 1:56 PM, David Turner <david.turner@voltagegate.com> wrote:
			
			I've been reviewing the input for v1.1 and I've grouped the issues into 5 broad categories to help focus discussions.
			
			    • *Terminology*
			        • *Reconcile terms from various ISO specs (e.g., 29100, 29184) with other significant sources (e.g., GDPR).*
			        • *We need to be clear that the CR spec is not the authoritative source for definitions and be clear that implementers must follow the appropriate definitions according to their relevant jurisdictions.*
			    • *Data model*
			        • *What is the proper relationship between different fields? For example, in the v1 spec there is only one dataController; and purpose, purposeCategory and piiCategory are subordinate to a service. What happens when we allow multiple dataControllers? Do we then make services subordinate to dataControllers, or the other way around? I've attached two views of the current JSON schema. One is pseudo-ERP and the other an expandable tree graph.*
			    • *New fields*
			        • *E.g., duration of consent, retention period*
			        • *Some of these suggested fields raise the question of how much of a policy's details should be repeated in the CR. What is the reason for including the field? Is it just for the implementer, for interchange/interop, for the end user, for regulatory compliance?*
			    • *Field semantics/syntax*
			        • *Some fields need more guidance and possibly specific data types. (e.g., jurisdiction, policyURL, termination)*
			    • *Purpose, purposeCategory, piiCategory, primaryPurpose*
			        • *A big ol' discussion all by itself.*
			
			From David: CR Schema v1_0_0.html
			
			From David: CR-1_0_0 data model v1 (1).gif
			
			2017-05-25 meeting notes:
			
			• David has cleaned up the CISWG github repo - Issues list
			• Added back a current list of issues for this release - 9 open issues at this time
			• David to create moderately fine-grained Issues - to make establishing a cadence easier - schedule issues to be addressed in each weekly block
			• Terminology
			    • A variety of issues
			        • 1) Evolution in terminology - ISO 29100, ISO 29184, GDPR etc (Andrew to set David up with a texts via Liaison committee)
			        • 2) Should resist changing terminology in the v1.1 - but some introductory text is required to clarify that the 'local jurisdiction' definitions are authoritative. the definitions are for the purpose of the specification e.g. the definition of 'consent' in the spec is actually a general term not a specific term
			            • Similar issue with some of the field content names etc - these also vary by jurisdiction and language
			            • **This might be solved by having a Guidance document that explains the customizations and terminology differences e.g. "Guidance on usage of CR for GDPR"; and also a 'Technical Overlay' that supplies values and parameters specific to a jurisdiction or regulation**
			        • **3) Note: the Consent Receipt will probably not become a standard for interoperability due to these kinds of variations - it will be more tilted towards compliance reasons**
			• Data model
			    • Need to avoid 'breaking' changes in v1.1
			        • One exception: the "Data Controller" - there is a need to support multiple Data Controllers - could be an array of objects
			    • v1.1 will have a diagram showing what the current data model is
			• "Parental Consent" is not represented - it's an extension of the 'on behalf of' structures - could be a new field
			• **ACTION: Next call we will discuss and** decide **field formats**
			    • To allow David to get organized with Issues, Backlog and scheduling cadence

| | General discussion | | From 2017-05-18 meeting:

• There is a need to clarify the existence of a 'Record of Consent' as distinct from the 'Consent Receipt'
• There is a need to define 'parameters' that an implementer or assessor would need to use to be compliant with any particular regulation or law
• Discussed the path forward. Mark has contributions on the way on several topics - he committed to send small samples to help the WG plan.
• David described his categorization of the backlog items
  • Security of the Receipt section needs clarification
• Discussed the concept of creating "Implementer's Guidance for xxx" - to explain how terminology in the specification translates into whatever local regulation is applicable
• Discussed what the source of defined terms is: ISO 29184 |

Parked notes about v1.1 approach from previous meetings:

- Mary
  - The caution about "Purposes lists" and "Sensitive data types" needs to be resolved - must be very cautious about how these are displayed to the user, especially if it's sensitive data - need to create recommendations
- Mark
  - Need to set up a backlog - and define a work plan and schedule
  - Set a date for CR v1.1
  - Need to write guidance on spec usage
- Need consensus on
  - Prioritization of backlog
  - Need to consider any issues that are used for GDPR implementation
  - The original agreement was to do 6-month epics
- **ACTION**: compare ISO 29184 (notice requirements) to GDPR definitions to identify discrepancies in concepts and definitions