IDESG Standards Coordination Committee (SCC)

Work item comments

[1]**Type of comment: ge** = general **te** = technical **ed** = editorial
NOTE: Reviewer to complete columns 1-6. Editor to complete column 7.

Dispositions. One of the following dispositions shall be indicated:

- Accept. The comment is accepted as written and will be incorporated.
- Partial accept. The comment is accepted in principle, but with modifications (as indicated).
- Reject. The comment is not accepted and will not be incorporated. Rationale should be provided, but is not strictly required.
- Noted. The point is taken, but is not actionable.
- Defer. The comment is valid, but is not to be acted upon in the current revision.
- Discuss. This only applies to proposed dispositions (not final/approved dispositions) and indicates that the group should discuss and decide on one of the above dispositions.

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
PA-MC #1	2.3		ge	I think that there are too many use cases that are not particularly central to the goal of guiding the work of the IDESG. I don't think the criteria selected by the work group are sufficiently helpful in determining which are and which aren't central to the work of the IDESG.		**Noted**. 1) Please provide specific guidance on which use cases are useful and which are not and why. 2) The use case criteria were sent out for IDESG review. Are there specific changes requested? NOTE: The intent is to include additional use cases in future revisions of the Use Case document. Also, we have discussed

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
						including a "Guidance for Use" annex in the next revision to aid committees in their usage of the Use Cases. Our hope is that by publishing an initial set, we will encourage contribution of additional useful use cases to fill any identified gaps. A breakout is planned for the April plenary to discuss V2 of the Use Case Criteria.
PA-MC #2	2.5		te	This seems comprehensive. I would like to see flow diagrams, however, in addition to text.		**Partially accept**. Flow diagrams are currently optional within the Use Case Template (Process Flow section). We will add such diagrams where possible in existing use cases and require them for future use cases.
PA-MC #3	2.6	1st bullet	te	These aren't identity ecosystem functions, they're credentialing functions. Identity ecosystem functions are things like policies, practices, technologies, architectures.		**Partial Accept**. Delete section 2.6.
PA-MC #4	2.6	4th bullet	ed	Without making judgments on the categorization of use cases, selecting a single use case to illustrate a category (and a category of significance) would be a better way to start.		**Partial Accept**. Delete section 2.6. We did make an effort to start with use cases from a number of different categories, but did not set an explicit goal of one use case per category.

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
PA-MC #5	3.1	Relations hips	te	I'd like to see some more text describing how/why/what the relationships are.		**Accept**. Delete this item from the Use Cases and Template.
PA-MC #6	3.1	Privacy Considera tions	te	This needs to be clarified. As it stands, it appears to be a non sequitur.		**Partial Accept**. This text came from the Privacy Committee; however, they have since slightly edited the text. Replace with their new text (as slightly modified): Modified 1st sentence. "A privacy implication occurs when raw device data is transferred instead of just claim information. For example this could be through the public key in the integrity certificate. In many cases the device is used by one or a small number of users which would allow linkage of this attribute to a user. Like any attribute, the device integrity claim would only be provided if the user authorized its release. It is certainly also possible to use a privacy enhancing technology provider (PETP) to combine all proffered claims into a composite claim with some identity that cannot be linked back to the original user."
PA-MC #7	3.2		ge	This is a good example of a central function. The problem I have with it is that this function		**Noted**.

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
				has been resolved in a gazillion ways since ENIAC went live in 1946.		The focus of the use case is not to focus on how this is resolved, but rather to describe what it is trying to accomplish.
PA-MC #8	3.2	Privacy Considerations	te	Identity is certainly an aggregation of attributes but the IdP policy defines which of them are required to assert an identity. An RP policy would define which IdP-issued assertions it accepts. We don't need another endless discussion of what attributes are identity and what attributes are extended. Beyond this point, this discussion does not clearly address the privacy considerations, which are that the IdP collects more or less PII (depending on its policy) and therefore incurs obligations under one or more schemes, e.g., EU Directive 460, FIPP, etc. Certainly this is not the place to open up the complex discussion of anonymous vs pseudonymous, a large topic that opens up many areas.		**Partial Accept**. Authentication of a person can release as little as an identifier, which may or may not be persistent from one session to the next. Accordingly, the use case does not address authentication for anonymous or pseudonymous interactions, which are considered important capabilities in the NSTIC. In both cases, trustable assertions from an attribute provider might be provided following authentication, even in the absence of a persistent identifier (in the anonymous case) or attributes that are intended to allow inference of the entity associated with those attributes.
PA-MC #9	3.3		ge	Again, this is a well-worn destination.		**Noted**.
PA-MC #10	3.4	Description	te	This isn't a description, it's a justification for choosing these use cases. It's good that there is one here, but the description should describe the use case. Maybe even a couple of process flow diagrams?		**Partial Accept**. *****Move 2nd para to Goals. Process flow diagrams can be added in the next revision.

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
PA-MC #11	3.5	Process Flow	te	This process flow conflates authorization and attribute management with authentication. It isn't really necessary as a part of the use case in question and should be stripped out so the case can be clearer.		**Partial accept**. ***** In Use Case Description, 2nd para, remove all after 1st sentence (UMA reference). Note – Add process flow diagram(s) in next version.
PA-MC #12	3.5	Success Scenario	te	This is not a success, it is a prerequisite. The success is that the process behaves according to the policy.		**Accept**. *Move to assumptions.
PA-MC #13	3.6		ge	This use case sure seems redundant.		**Noted**.
PA-MC #14	3.6	Success Scenario, 2nd bullet	te	This is not a successful outcome.		**Accept**. *Move to a note at the end of the process flow steps.
PA-MC #15	3.7	Process Flow, Proof of Age, bullet 2	te	This assumes that the subscriber does not have a credential already. Why? At the very least, this assumption needs to be articulated.		**Accept**. *Add to assumptions.
PA-MC #16	3.7	Process Flow, Proof of Age, bullet 3	te	Why anonymous? The desire for anonymity should also be an explicit assumption if one is including this element. In fact, there's really no reason why the Attribute Provider should be credentialing the Subscriber at all. So that should also be an assumption.		**Partially accept**. Anonymous assumption is already addressed. *Add assumption regarding AP as credential issuer.
PA-MC #17	3.7	Process Flow, Verification of Age, bullets 2-4	te	2, 3 and 4 contradict each other.		**Accept**. *Reword to reflect optionality: 2. Service provider discovers the attribute provider by either: a. Subscriber informs Service

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
						Provider of Attribute Provider, or b. Service Provider queries for Attribute Provider that can verify Subscriber.
PA-MC #18	3.7	Process Flow	te	This process flow is unnecessarily tortuous. Look at the number of exchanges and permissions and logins embedded!	Process Flow needs to be revised.	**Noted** The UCAHG will strive to include flow diagrams in future iterations.
PA-MC #19	3.7	Error conditions	te	This is not an error condition. An error condition occurs when the wrong requirement is sent or the wrong attribute is sent.		**Accept**. *Make this a note (perhaps under assumptions).
PA-MC #20	3.8	Description, 3rd sentence	te	Certainly this is one way privacy in the cyber world can be enabled but it is not the only one and saying a Privacy Enhancing Technology Provider is required is just flat inaccurate. An intermediary is not always necessary; RAs can and do function as privacy services in many scenarios.		**Accept**. Clarified wording in the wiki.
PA-MC #21	3.8	Goal #2	ge	"individual user's intent" – Huh?		**Accept**. Clarified wording in the wiki.
PA-MC #22	3.8	Goal #3	te	Suggest rewording	Perhaps this should read, "High comfort level for users that their personal data is only shared when they want it shared."	**Partial accept**. *High comfort level for users that their personal data is only shared when and with whom they want it shared
PA-MC #23	3.8	Assumptions	te	A required assumption is that all nodes in the architecture share protocols and transaction procedures. It is a closed system, btw.		**Noted** Use cases may vary depending

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
						on implementation
PA-MC #24	3.8	Process Flow, step 2	ed	"They" Who?		**Accept**. Clarified wording in the wiki
PA-MC #25	3.8	Success Scenario, 3rd bullet, last sentence	te	this is not a success scenario.		**Accept**. *Move all after 1st sentence to a note or a sub-element of the appropriate process flow step.
PA-MC #26	3.8	Error Conditions	te	The agent failing to abide by requirements for maintaining the privacy and confidentiality of the PII it holds is perhaps the most obvious error condition. Another would be the agent releasing inaccurate data, incorrect data or poorly formatted data that breaks the transaction.		**Noted** Use cases may vary depending on implementation
PA-MC #27	3.9		ed	This use case requires a substantial amount of editing.		**Noted**.
PA-MC #28	3.9	Goals, #1	te	In this bullet, the goal would be for the new user to access the RP site with a low-assurance credential which then must be converted in some fashion into a more trustworthy transaction. Evaluating the RPs' services is not really part of the story.		**Partial accept**. Note that it is not required that the user go to higher levels of assurance unless they want specific services that require those.
PA-MC #29	3.9	Process Flow, Step 8	te	Things get confused here. If the RP has directed the user to a credential provider then it must recognize that credential when the user finally presents it, hence a problem with numbers 9 & 10.		**Partial accept**. Wording changed to improve understanding.
PA-MC #30	3.9	Process Flow, diagram	ed	The transactions between RP and UA should be numbered so the flow can be followed.		**Accept**. Changed.
PA-MC	3.9	Success Scenario,	te	This happens regardless of whether the trust is elevated or not so it is not a success element.		**Noted**

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
#31		1st bullet				A success metric may simple be that the site works well for anonymous visitors.
PA-MC #32	3.9	Success Scenario, 2nd bullet	te	Likewise, this is not a proof of success, it is a description of a required step. Success would be a user acquiring one of the recommended credentials.		**Noted** Reworded bullet points.
PA-MC #33	3.9	Success Scenario, 3rd bullet	te	Yes, this is one.		**Noted**.
PA-MC #34	3.9	Success Scenario, 4th bullet	te	This is not a success, this is again a process step.		**Noted**.
PA-MC #35	3.9	Success Scenario, 5th bullet	te	What?		**Accept**. Reworded.
PA-MC #36	3.9	Success Scenario, 6th bullet	te	This is not a success element; this is a process step.		**Accept**. Reformatted.
PA-MC #37	3.9	Error Conditions, 1st bullet	te	This is not an error condition; it is the starting condition that generates the use case.		**Noted**…however, in some scenario the user may have a credential that does not require the user to acquire another credential.
PA-MC #38	3.9		te	Where are the privacy considerations?		**Accept**. *Incorporate from Privacy spreadsheet: "Pseudonym provided by collection of tokens representing different identity offerings. But RP knows which identity attributes it is asking for. Depending on the

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
						service/attributes requested, the combination of attributes validated could be enough to re-identify user."
PA-MC #39	3.10	Assumptions	te	Assumptions should also include relationships among parties so that the RP can communicate with the AP, the IdP with the RP, etc.		**Accept**.
PA-MC #40	3.10	Process Flow, step 10	te	How does RP know which AP to communicate with?		**Noted**. Implementation details may be added in other iteration.
PA-MC #41	3.10	Error Conditions	te	Certainly there are many more, such as RP cannot communicate with AP or vice versa, AP provides inaccurate information, user provides inaccurate information to AP, etc.		**Accept**.
PA-MC #42	3.10		te	Privacy considerations?		**Accept**. *Incorporate from Privacy spreadsheet: • "Tracking policy determinations across different services a concern - could provide substantial information about user behavior, and could be significantly identifying. • Depending on the variance in the types of actors, other considerations like user consent would be an issue. • Services can also lock out users with strict policies creating incentives for

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
						disclosure. One particularly challenging problem is the case of minors under the age of 13 that are covered by COPPA. • Attributes are potentially highly identifying, even without PII. Example: service member of specific age range, in a specific geographic area, could be enough to ID user. Will require work with RPs to ensure that collection of validated attributes is protected in order to be successful."
PA-MC #43	3.11		ed	This use case also will require substantial editing.		**Noted**.
PA-MC #44	3.11	Description, 3rd para	ge	Really interesting!		Noted.
PA-MC #45	3.11	Scenario, 1st para	te	She wants to acquire a digital identity to access goods and services online. She doesn't give a hoot about the Identity Ecosystem.		**Partially accept**. The use case does not address all possible motive
PA-MC #46	3.11	Scenario, 2nd para	te	This is only step one in the scenario. Using CIP she is proofed. What next? Does she use that proofing to acquire a credential somewhere? Does she actually get a credential? What next?		**Accept**.
PA-MC #47	3.11	Goals, 3rd sentence	ed		Add "online" after "services"	**Accept**.
PA-MC #48	3.11	Goals	te	This summary needs to be revised to focus on the goals of the use case and as noted above, the use case needs to be completely described.		**Accept**.

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
PA-MC-#48A	3.11	Process Flow, diagram	te	The actual scenario occurs here and needs to be prepared. Also, an end user doesn't interact with an ecosystem, she is part of the ecosystem (as the graphic shows) and interacts with other elements of the ecosystem.		**Partial Accept**. *Add introductory text and process flow steps as bullets.
PA-MC #49	3.12	Actors	te	Doesn't this use case require an RP that asks for, and consumes, the attribute?		**Accept**. *Add to RP description.
PA-MC #50	3.12	Goals	ge	Good write-up.		**Noted**.
PA-MC #51	3.12	Process Flow, Step 3	te	Wouldn't this break the transaction flow with the RP? How does the user assert the attribute to the verifier and to the RP? Does the user need to have an antecedent relationship with the verifier or can the user assert the attribute and the RP query the verifier/authoritative source? For that matter, why assume two functionalities there instead of the source being the verifier? Most of the models of this case that I've seen make the RP call for the attribute rather than the Claimant.		**Noted**. Implementation specific details are not currently present.
PA-MC #52	3.12	Error Conditions	ge	Good		**Noted**.
PA-MC #53	3.12		te	Privacy considerations?		**Accept**. *Incorporate from Privacy spreadsheet: • "Claimant should be able to voluntarily participate in the process. • Claimant should control the rights to their own data and that Claimant's information should only be released to a Relying Party at the claimant's discretion.

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
						• Organizations shall limit the collection and transmission of information to the minimum necessary to fulfill the transaction's purpose and related legal requirements. • Same concerns about the identifying properties of validated attributes as above use cases."
PA-MC #54	3.13	Goals, #1, 2nd sentence	te	this is process flow, not goal	[AH] Goal 1) (C) Claimant, who is distal (not in the physical presence) of RA and has an antecedent relationship with the RA, is given approval by RA to acquire a trusted credential.	**Accept**. *Delete this content from "Goals" of the Use Case. The deleted content is included within the "Process Flow" of the Use Case. "(C) Claimant connects via method for attribute collection with RA's IP for an identity proofing antecedent in - person event to submit their attributes. IPVSP collects (C) Claimant attributes and submits to RA/CSP."
PA-MC #55		Goals, #2	te	Goal is to acquire the credential. This is a requirement, not a goal.	[AH] Goal 2) PC, who is remote (not in the physical presence) and does not have a antecedent relationship with an RA, requires a trust	**Accept**. * Delete this content from the "Goals" section of the Use Case. The deleted content is included

1	2	3	4	5	6	7
Reviewer	**Clause No./ Sub-clause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change)**	**Proposed change**	**Disposition**
					credential. Also the word "their" is deleted from the "Assumptions" and "Success Scenario" categories.	in the "Process Flow" of the Use Case. "and via method for attribute collection connects to an IPVSP who has an established trust relationship with a RA/CSP to submit the PC attributes to RA/CSP."