Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)
Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*IDmachines LLC https://idmachines.com*
Name of Submitter/POC:	*Sal D'Agostino, Mark Lizar*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	General				A critical component to consent is transparency over who the accountable PII controller is, who is makes the policy and responsible for personal data. The security of notice Transparency is a critical component of any privacy, security or legal framework. It is suggested that transparency assurance be included in determing conformance at assurance levels with the level of transparency adequate for the level of assurance.	Table with transparency performance indicators, see example https://kantara.atlassian.net/wiki/spaces/WA/pages/82542593/Trust+Performance+Indicator+s+TPI+s
2	63C	5.1	14	670	When logging in to the service for the first time, each subscriber is prompted for their consent to release their attributes to the RP.	Simply saying a prompt without the requirement that it should convey the context and any risks, liability, rights, and responsibilities. Ideally the user gets this information at the same time or even before the prompt. The timing of this information and notice is a measure of the transparency. It is a critical component of any assurance regime. The level of assurance has to be commeasureate with the leve of risk, etc. The subscriber needs to be made fully aware by the IdP and any RPof any changes. The receipt of this notice can be used to create a record to maintain these assurance relationships.
3			15	674	In another scenario, a dynamic trust agreement is established implicitly when a subscriber goes to access an RP that is otherwise unknown by their IdP. The RP informs the subscriber about the uses of all attributes being requested from the IdP, and the IdP prompts the subscriber for consent to release their attributes to the RP.	The agreement is not established until consent takes place. The information about use needs to include other conditions and the terms of the release, restrictions on sharing, and importantly capture by whom, or by what device or service.
4			22	880	In this mode of operation, the authorized party is prompted by the IdP during the federation transaction for their consent to provide an authentication assertion and release specific attributes to the RP on behalf of the subscriber.	Again the IdP is not able to provide consent, they can authorize, give permission, take responsibility, among other things but they do not convey consent, that comes from the suscriber.
5	63C	5.3.3	22	882	the this sections asks for actions consistent with privacy considerations (9.2) and SHALL provide explicit note.	There needs to be a set of requirements and performance measurements for the delivery of the explicit notice. The subscriber is the party who acts on the notice. the IdP is relaying the notice, not creating it. In this case the IdP should be confirming/relaying the notice, in this way the subscriber remains the authority in the actions of the identity services.
6	63C	6.5.2	45	1511	The authorized party consents to and is notified of the use of a shared pseudonymous identifier;	The term consent, it authorizes, give permission, the creation of identifiers.
7	63C	6.5.2	45	1527	All RPs sharing an identifier consent to being correlated in such a manner (i.e., one RP cannot request to have another RP's PPI without that other RP's knowledge and consent).	Same comment on use of the term consent. Permission in identity management systems and consent are not the same thing.
8	63C	9.1	56	1739	For example, absent applicable law, regulation or policy, it may not be necessary to get consent when processing attributes to provide non-identity services requested by subscribers, although notices may help subscribers maintain reliable assumptions about the processing (predictability).	Notice is fundamental and MUST be provided and the details should be stanardarized to convey the legal requirements and privacy rights.
9	63C	9.2	57	1755-1762	In determining when a set of RPs should share a common pairwise pseudonymous identifier as in Sec. 6.2.5.2, the IdP considers the subscriber's understanding of such a grouping of RPs and the role of notice in assisting such understanding.	The IdP should not consider it should provide a receipt that captures the notice, and proof of notice (effectively its acceptance), the IdP is NOT empowered to do anything more that explictly agreed with the suscriber. This applies to any sharing independently of the derivative identifier type. Particulalry in the light of the follow on acknowledgements in the section that privacy policies are not effective as notice.
10	63C	10.2.2	64	2002	Allow users to control their information disclosure and provide explicit consent 1through the appropriate use of notifications (see Sec. 9.2). Balancing the content, size, and frequency of notifications is necessary to avoid thoughtless user click- through.	This is one type of transparency measurement, where the timing of the notice and other information for the subscriber. Ideally this notice is provided before any surveillance takes place and then its acceptance as proof provides policy for any further enrollment, identifier, attribute, authenticator, authorization actions.
11	63C	10.2.2	65	2009	Enable users to consent to a partial list of attributes, rather than an all-or-nothing approach. Allow users some degree of online access, even if the user does not consent to share all information.	User/subscribers/data subjectss/people MUST be able to designate the relationship and control attributes release and use.
12	63C	10.2.2	65	2012	Allow users to update their consent to their list of shared attributes.	Consent to attributes is not adequate description in that consent is related to the use of attributes in context, attribute release is always relational and conditional.
13	63C	10.2.2	65	2017	Minimize user steps and navigation. For example, build attribute consent into the protocols so they're not a feature external to the federated transaction. Examples can be found in standards such as OAuth or OpenID Connect	More accurately build notice and consent and authority into authentication protocols, see above reference related to the role of notice and consent receipts and records and their ability to prioritize, energize and legitimize at the beginning of identifer technical flows to capture this state, so that it can be applied thereafter.
14	63C	10.2.2	65	2022	Minimize the number of times a user is required to consent to attribute sharing. Limiting the frequency of consent requests avoids user frustration from multiple requests to share the same attribute.	User centric authorization flows are the only way to reduce the frequency of consent. The user SHOULD dictate the terms and receive confirmation of their consent, after notice and consent prerequisities. This then applies to all instances that are capture in the person's consent gran.
15	63B	B.3.4			In this sentence there is revealed a mis-definition and use of consent. "limited to its intended use (authentication) unless the subscriber consents to additional use". Consent is for the intended purpose of use by the subscriber, this is in context of a service. In this regard, authentication is not relevant to consent, but is instead a permission for digital identity / security to be engaed, to create / allow for a profie to be used, as the security requirements for the purpose of service use. Consent is relative to the human context and the digital notice.	Recommend "unless the subscriber, provides permission for another method of authentication, required to achieve the purpose of the service use. ..