Consultation for SP 800-63 / Digital Identity Guidelines Feedback

> This consultation closed on March 15, 2017. This feedback mechanism was used to enable the Trust and Identity community supporting the R&E mission to aggregate its comments on NIST's 800-63-3 Digital Identity Guidelines. You are encouraged to provide individual feedback directly to NIST, or to contribute to this aggregation of community feedback and also provide individual feedback. If you have written an extensive feedback piece, please feel free to include a link and summary in your Proposed Text / Query / Suggestion to that external material. And as usual with this consultation process, also feel free to +1 the feedback of your colleagues.
>
> Your collective feedback will be given to NIST on behalf of the community. This consultation process will be described as the source of the feedback; it will not be attributed to InCommon, Internet2, or any other organization.

Documents for review/consultation

- SP 800-63 Digital Identity Guidelines
- SP 800-63A (Enrollment and Identity Proofing)
- SP 800-63B (Authentication and Lifecycle Management)
- SP 800-63C (Federation and Assertions)

NIST Instructions for Submitting Comments: https://pages.nist.gov/800-63-3/

Change Proposals and Feedback - We welcome your feedback/suggestions here

If you have comments that do not lend themselves well to the tabular format below, please create a new Google doc and link to it in the suggestion section below.

Number	Section, if applicable (overall comments also welcome)	Current Text if applicable (overall comments also welcome)	Proposed Text / Query / Suggestion	Proposer	+1 (add your name here if you agree with the proposal)
1	9.3 in 63C	Data Minimization	Providing insufficient attributes may impact the functionality of the application. If the RP can identify which attributes are needed for which functions, it will help a user determine what to release.	Ken Klingenstein	
2	9.3 in 63C		Data minimization for portals is particularly vexing. Guidance on how to do this would be helpful.	Ken Klingenstein	Brett Bieber
3	10.1.1 in 63C	Provide users means to delete their identities completely, removing all information about the user, to include transaction history.	There are often legal or audit reasons to not delete transaction histories.	Ken Klingenstein	Brett Bieber
4	10.2.1 in 63C and 9 in 63A		Neither section appears to offer guidance on the translation of technical attribute names and values into user-friendly language.	Ken Klingenstein	
5	10.1		It might help to qualify what is meant by minimizing user actions. While I think this is a worthy goal overall, we have struggled on CAR with a temptation to minimize user actions in ways that allow important concepts and information to be glossed over. Happy to show examples where we chose not to minimize user actions if it would help foster a discussion. The link to Account Chooser isn't formatted so as to be clickable. I did navigate to http://openid.net/wg/ac/ but didn't get very far because the title of the page (and working group) uses the word "login" incorrectly, which (especially in the IAM space) I find very distracting. Used as a verb, it should be "you only log in once", not "you only login once".	Mary McKee, Duke	

6	10.1.1		The suggestion to "provide users with the ability to easily verify, view and update attributes" is (perhaps deliberately) ambiguous about whether this function needs to be part of the context in which the attributes are being shown and/or released. For CAR, we've determined that it's counter to the primary goal of facilitating authentication to invite submissions of updated values at the time of an attribute release decision. Expanding the range of decisions from simple "yes/no" or "permit/deny" from current values to anything a user might choose to release (especially when the user may be an acceptable authority for values of some attributes but not others) adds (in our determination) an unacceptable amount of cognitive load on the user during a time-sensitive transaction. "Provide users means to delete their identities completely, removing all information about the user, to include transaction history." - I'm not sure if I disagree with this from a philosophical standpoint, but it's hard to even consider given how unlikely it is that we could support this at Duke as written. Audit requirements will make this a non-starter in many areas, and I hate to think that "we can't do this fully" might translate to "we can't improve the status quo". Speaking for CAR: I would personally advocate for the ability to deactivate undesired policies in CAR. The ability to completely remove a policy is something we should discuss and form a position on - is auditing more important than user privacy? Speaking for Duke as a resource holder: I think we could improve by giving users more visibility into our (deliberately short) history retention policies, but I would not advocate for the ability for a user to be able to wipe his/her history within that window. I would also support users having visibility into what parts of his/her identity could be redacted, but would not support user-initiated deletion of an identity. Credentials are another story - personally, I'm of the opinion that users should have complete latitude to destroy those if undesired (though based on some InCommon expectations like EPPN not being re-usable, we'd still have to track of the fact that some electronic credentials existed).	Mary McKee, Duke	
7	10.1.3		Just another grammar nitpick: in the penultimate sentence in last bullet point, "logout" is used as a verb. The use of "logout" in the last sentence is fine.	Mary McKee, Duke	
8					

See also

Consultation wiki