Minimal LoA recommendation

Community consultation (until 17th Jan 2016)

Comments on the LoA recommendation (https://wiki.geant.org/x/wIEVAw)

Section and item	Proposed change	Justification for the change	Proposer's name and affiliation
overall	Should this be presented as only a report, or a report plus a recommendation on further process to establish an assurance profile, instead of a recommendation for an assurance profile?	Although the interviewees present good information on their expectations of IdPs, there are many more stakeholders to any potential LoA scheme that is to be adopted globally (1000s more). They must be consulted in some fashion as well before they can be expected to accept the assurance profile. A good next step might be to either propose such a process or propose formation of a group that would do so. In fact, if the global R&E sector might need more than one assurance profile, it may be reasonable to create a standing group focused on this task.	Tom Barton, InCommon & UChicago +1 Glenn Wearen +1 Daniela Pöhn
general	don't use the word level	"Level" implies this will form part of a strictly tiered approach with future "levels" that are increasingly better. I think it is unlikely that this space will grow in this way but be closer to the vectors of trust approach, with overlapping assurance profiles that meet the specific needs of certain scenarios but that aren't strictly hierarchical levels	Nicole Harris, GEANT +1 Glenn Wearen +1 Thomas Lenggenhager, SWITCH
general		Combining a requirement for identity proofing with an acceptance of passwords seems like an awfully good approximation of NIST's LOA 2 and InCommon Silver, neither of which have gotten traction. Unclear why this	Scott Cantor, Ohio State +1 Nick Roy,

		would be different	InCommon
Don't know - you probably want a separate document with a risk profile in it	Define what "low-risk" means in such a way that it matches the assurance profile and in such a way that a service can determine with some degree of confidence if they are "low risk" or not. Right now the "low risk" concept is dangerously undefined. Take a look at the "classical" document OMB-0404 that defined the risk profile that went on to for the basis for NIST SP-800-63 for an example of the type of concrete and (comparatively) actionable definition of "low risk" I think this document needs.	Because you want to make sure assumptions about risk to match what the assurance profile can deliver. All current assurance work (Kantara, 800-63, ISO-29115) ultimately draw on OMB-0404 because they are all derived from 800-63 but that document was written in terms of economic loss for US federal services which is hardly the only, or even an appropriate way to value risk for a research project or community. Note that "over-compensating" - i.e over-valuing risk - is a really bad idea because it results in an assurance profile that will drive cost for IAM: high assurance is *not* free.	Leif Johansson, SUNET +1 Glenn Wearen +1 Eefje van der Harst (SURFnet)
1.2.2	Typo: WLGC	Should be WLCG	Bob Jones, CERN
1.2.2	replace 'either of the following reasons" with "one or both of the following reasons"	Did any of the interviewees cite both reasons for a higher LOA?	Bob Jones, CERN
2.1	The six requirements for the minimal assurance profile seem rather arbitrary.	Why not align this more with LoA1 requirements and phases (enrolment, credential management & authentication phase) as formulated in ISO29115?	Eefje van der Harst SURFnet
2.1.1	Accounts are not assigned to multiple users and the Home Organisation must be able to trace each account back to its holder.	A Home Organization can not prevent users from sharing their account credentials. It is known that many professors provide their credentials to their administrative staff...	Thomas Lenggenhager, SWITCH

	instead of 'Accounts must not be shared and the Home Organisation must be able to trace each account back to its holder.'		
2.1.1	the Home Organisation must be able to trace each account back to its holder during the time the account is active.	The traceability requirement must be defined in terms of some time period.	Jim Basney, NCSA
	Response to Jim Basney's comment immediately above	Agreed, but see other comments for problems with definition of 'active'. Does there need to be some attribute that signals a user aligns with the overall profile, such that an 'inactive' person could fall out of the profile without needing to affect other parts of the person's user experience?	Nick Roy, InCommon
2.1.2	consider ePPN, ePPN non-reassigned, ePTID as 3 different attributes.	all IdPs in IDEM (italy) have "ePPN non-reassigned" for IDEM policy. All IdPs in IDEM are releasing ePTID to any SP independently to the entity category of the SP	Lalla Mantovani, IDEM
2.1.2 and 3	Consistently use the phrase "persistent, non-reassigned identifier" throughout this document.	The meaning of "persistent identifier" is commonly misunderstood. Adding the word "non-reassigned" makes the requirement more clear.	Tom Scavo, InCommon
2.1.2	Replace this phrase "Currently, in the federated AAI, the most widely used identifier eduPersonPrincipalName is lacking this property" with this: Any of the following attributes will	Please don't rule out ePPN. At least 75% of IdPs in the InCommon Federation assert ePPN that is non-reassigned.	Tom Scavo, InCommon

	satisfy this requirement: 1. ePTID 2. ePUId 3. ePPN (if non-reassigned) A conforming IdP MUST NOT assert ePPN if reassigned.		
2.1.3	3. Documented identity vetting procedures (not necessarily face-to-face) = too vague	The Home Organisation must publish its identity proofing policy, and perform all identity proofing in accordance with the published identity proofing policy (to ensure the identity is unique within the intended context and the cannot be associated with two different entities)	Eefje van der Harst SURFnet
2.1.4	This section is ambiguous. Please be explicit about password requirements (and I sure hope "change cycle" isn't one of them :)	I'm afraid that vague password requirements are worse than no requirements at all.	Tom Scavo, InCommon
2.1.4	Password acceptance	Document should not focus on just passwords, it should state any other credential systems that are not acceptable. For example, should 2F auth, IP auth, Social login auth (integrated with IdP) be accepted?	Glenn Wearen, HEAnet
2.1.4	Password acceptance + there must be certain widely approved good practices for the password quality= too vague	Why not make this more generic: one factor authentication regardless of the method? Some IdPs use a personal certificate instead of a password There is nothing like a 'widely approved good practices for the password quality'	Eefje van der Harst SURFnet +1 Thomas Lenggenhager, SWITCH
2.1.4	Password acceptance	Specifying password requirements are useless if there's no brute-force protection.	Glenn Wearen, HEAnet
2.1.5	What does "departing" mean?	If IdPs maintain users in their identity management	Lalla Mantovani,

		systems, that means that there are reasons to do in that way (collaborations are still in place for examples)	IDEM
2.1.5	The 30 day limit seems arbitrary, and the ePA values listed might not be the only ones of interest to SPs globally.	How and when should an IdP signal that someone is gone? As Lalla commented above, there are many circumstances that don't agree with the concept of "they're totally here and then they're totally gone". One use case In particular at UChicago enables a research computing center to assign UChicago credentials to non-UChicago researchers using their facility. No ePA value is shown for them, no access to enterprise UChicago services is assigned to those credentials, yet they must have federated access to CILogon (at least) to login to research computing resources. When are they "present" or "departed"? There are many such examples in a large complex research organization.	Tom Barton InCommon & UChicago
2.1.5	5. Departing user's eduPersonAffiliation must change promptly => why restrict this requirement to the affiliation attribute?	Every change in attributes during the lifecycle of an identity (not only at departure) should be changed promptly by the Home Organisation	Eefje van der Harst SURFnet
2.1.5	Differentiate between students and faculty.	For students, the university generally does not know whether they will continue or not until the deadline for registration for the next semester is over. So even a student might depart at the end or even during a semester, the university might not be aware of it until a few weeks into the next semester. For faculty one month seems reasonable to me, for students it is surely unrealistic.	Thomas Lenggenhager, SWITCH
2.2	A new bullet on how to map a federation defined assurance profile to the minimal assurance profile.	For federations that has defined their own assurance profiles (at least inCommon and SWAMID) it can be very hard to sell in another assurance profile that the home organisation should do an assessment against. Therefore	Pål Axelsson, SWAMID

		there should be a bullet that describes the possibility of assurance profile mapping by the federation operator. This could be done either with an “automatic” mapping rule by the federation operator or by that the services is aware of the federation assurance profile.	
Appendix - Tool to support HOs’ self-assesments	The idea that this tool would add an EC directly to the eduGAIN metadata (MDS) appears to be problematical. IMHO, a decentralized or mixed approach would be more convenient.	Three reasons: 1. Technical Some federations still follow the opt-in approach for entities joining the eduGAIN upstream metadata - and therefore provide the downstream metadata as a separate stream - to be consumed only by the entities really needing it. In order to prevent any duplicates (and any strange side-effects), we (DFN-AAI) automatically remove all entities from the eduGAIN downstream metadata which are already registered with the DFN-AAI - as far as I know, the same holds true for SWITCHaai. As for German IdPs, this EC would never appear in our own federation - unless we reassign it, which would require additional technical efforts extending our metadata registry. 2. Trust According to the draft, "identification/authorisation of the IdP admins could be done by picking the contact information from the IdP metadata and sending a log-in link to that email address". The problem here is that especially larger institutions don't use personal but role/list email addresses (which is encouraged by the eduGAIN metadata profile, btw). Insofar, the level of assurance applied to the process of identification and authorization of an IdP/IdM admin is far weaker than the one required for the so-called "Minimal Assurance	Wolfgang Pempe, DFN +1 Nicole Harris +1 Thomas Lenggenhager, SWITCH

		Profile" which this admin is meant to assert. In that case, some kind of re-confirmation by the federation operator would be necessary. 3. Easy LoA-EC mapping In cases where the requirements of some federation-internal LoA meet those of the Minimal Assurance Profile (SWAMID perhaps, DFN-AAI Advanced with some limitations), the EC could be easily assigned by the metadata registry and exported with the upstream metadata - without the overhead of using yet another online form/tool.	
Appendix A	This won't work: "The tool is an eduGAIN Service Provider to which any eduGAIN Identity Provider admin can log in" since contacts in metadata are often (by design) group contacts.	We would prefer to tag InCommon IdPs locally. We already have mechanisms that allow authorized site administrators to self-assert entity attributes in metadata.	Tom Scavo, InCommon +1 Nicole Harris
Appendix A	In lieu of restricting access to the self-assessment tool, why not allow anyone to run it and transmit the results to their local federation operator for appropriate tagging		Nick Roy InCommon