2016 eduGAIN Policy Consultation

From July - October 2016, the GN4 project has been undertaking a review of the eduGAIN Constitution with the following aims:

- To make the consitution technology agnostic.
- To better reflect current operational practice within the Constitution.

This is part of a wider review of the full eduGAIN policy set as described on the GÉANT wiki.

The review group has undertaken an initial review of the documentation and would like to collect feedback from the eduGAIN SG on the current change proposals. It is recognised that making eduGAIN technology agnostic raises significant questions about how the Constitution is written and that there are unknown elements to operating multiple profiles as part of the eduGAIN service, so areas of the proposed text might still be open for discussion and amendment.

- Revised version 3 of the eduGAIN Constitution - marked-up.
- Revised version 3 of the eduGAIN Constitution - clean.

Comments from the eduGAIN SG were invited until 9th December 2016. The table below shows the comments received and the actions taken.

Reference	**Comment**	**Commenter**	**Actions**
line 152-3	I have a question about line 152-3 in the marked-up version. It says that a participant that misses two consecutive votes will be moved to the non-active list for the purposes of voting, but may move back to the active list by voting. So, what does the non-active list do, if it doesn't prevent a participant from voting?	Nick Roy	Brook has proposed wording changes to help clarify this. The intention is to avoid having non-active federations counting towards quorum
line 121	typo	Nick Roy	Fix
??	Since the OT is empowered to remove a participant federation from one or more technology profiles or all of eduGAIN under this new constitution, I'd like to ask that the OT also be tasked with developing an incident handling framework that it will use in guiding its actions in security or other relevant circumstances. The OT should then open up this incident handling framework for review by the eSG and then acceptance by the eEC if the eSG recommends moving it forward. See: https://docs.google.com/document/d/1jo7X06sfKNuG2bVhzslpmRe_z11dsPpkudPO3pGUUf8/edit?usp=sharing	Nick Roy	Should be part of the eduGAIN OP - pass to Brook and Tomasz.
1.2	Federation Operator - Organisation providing or commissioning the infrastructure for Authentication and Authorisation to Federation Members. s/Federation Members/the members of the Federation/ Lowercase since member is not a defined term. BTW: The term 'Federation Operator' is no longer used in the document.	Thomas Lenggenhager	Fix
1.2	Identity Provider - A server acting in an Identity Provider role. In this document, an Identity Provider refers to the Identity Provider who is a Member of a Participant Federation and whom the Participant Federation has exchanged its metadata through eduGAIN. I think that's wrong: The Home Organisation is the member, not the Identity Provider. Suggested change: Identity Provider - The system that issues assertions on behalf of end users of a Home Organisation who use them to access services of Service Suppliers.	Thomas Lenggenhager	Fix
1.2	The Service Provider has a double role. An organisation as well as an entity. I think we need to split these two roles. I named the organisational one 'Service Supplier', please suggest better terms. Service Supplier - An organisation that is responsible for offering the end user the service s/he is going to log in to. It is a member of a Participant Federation whose Service Provider metadata the Participant Federation has published to eduGAIN. Service Provider - The system that evaluates the assertion issued by an Identity Provider and uses the information from the assertion for controlling access to protected services	Thomas Lenggenhager	This would require substantive changes to the Declaration as well and we do not want to make a Declaration change at this point. Keep on record for future review.

Line 155	Two weeks voting is too short	Thomas Lenggenhager	This will not be changed, although it is noted that the eduGAIN team will always make sure that holiday periods are avoided.
Line 201	s/as a Member/as a Member Federation/	Thomas Lenggenhager	Fix
Definitions	Add a definition of edugain (appropos comments on "what do we mean by edugain")	GÉANT Board	Implement
Section 1	Add a paragraph clarifying the role of all the eduGAIN documents - this can be repeated across the suite.	GÉANT Board	This is covered in 1.1. They are not explicitly listed to prevent issues with change control across documents with different change rules. A reference t the website has been inserted.
Section 1	Swap sections 1.2 and 1.3 to add clarity	GÉANT Board	Implement
2.1	URL for Executive is missing (known issue, this still needs to be created)	GÉANT Board	This is a to do for Nicole / Tomasz
2.2	Add sentence about non-voting observers	GÉANT Board	Implement
2.2	Add sentence on exception on voting for Constitutional changes	GÉANT Board	Implement
2.2	clarify "peering relationships"	GÉANT Board	Implement
2.2	Does the SG "review" membership?	GÉANT Board	Yes - there is a process for this.

2.3	Describe composition of the OT and profile operators	GÉANT Board	This has been left purposefully under-specified due to the fluid nature of profile operator undertstanding at the moment. This will be further decsribed in the eduGAIN OP.
section 3	Better describe the difference between a member federation and a participant federation	GÉANT Board	Implement
Definitions	Add a definition for Federation Policy and reference at line 198	GÉANT Board	Implement
Definitions	Add a definition of interfederation	GÉANT Board	Implement
line 152	delete participant	Brook Schofield	Fix
line 148	"Federations from the active ~~participants~~ list"	Brook Schofield	Fix
line 151	delete participants	Brook Schofield	Fix
line 300	"of ~~active Participant~~ Federations from the active voting list. "	Brook Schofield	Fix

Post Review Comments

Reference	**Comment**	**Commenter**	**Actions**
2.1	The comment on the comment (meta comment?) of the GÉANT Board "Describe composition of the OT and profile operators" says: "This has been left purposefully under-specified due to the fluid nature of profile operator undertstanding at the moment. This will be further decsribed in the eduGAIN OP." Insofar, would it hurt to amend section 2.3 accordingly - informing the reader that composition /appointment etc. of the OP is/will be specified in a separate profile/document?	Wolfgang	Add a link to the edugain Operational Profile

1.1	1.1: Overview "The eduGAIN service enables Federations to interfederate. The Member Federations primarily serve the authentication and authorisation interests of research and education sectors." seems identical to 1.2: Goal "The goal of eduGAIN is to support Identity Federations primarily engaged in research and education by providing a service which enables them to interfederate." If you want to keep a separate section 1.2 I'd suggest dropping the paragraph from 1.1.	Peter	This makes no substantive difference so a change is not recommended
3	3. Membership Nowhere in that document does it state that you have to be a Member Federation in order to become a Participant Federation, AFAICT. At least my understanding was that this is 2-stop process: The first/lower step is becoming a Member Federation. Only Member Federations then may also become Particpant Federations (by adopting Tech Profiles). So maybe change its defintion like this (having added "are Member Federations" that "additionally") in section 3: "Participant Federations [are Member Federations] that [additionally] are actively participating in eduGAIN via the use of a Technology Profile." Alternatively, adding something to 3.3 to that effect would also take care of this, e.g.: 1. The Federation has joined eduGAIN as a Member Federation (renaming all other 3 items +1) Or maybe simply by changing the first sentence in 3.3 by prefixing it with "For a Member Federation", so that it becomes: "[For a Member Federation] the process to become a Participant Federation in a Technology Profile is as follows:"	Peter	This is defined in the definitions - no change recommended.
3.6	3.6: Suspension This section only talks about Participant Federations, even when it's about policy issues. Does that mean that only Participant Federations can be suspended or disqualified? I.e., Member Federations cannot do anything that would change their member status? Either way, the following sentence is a bit weird then: "* Announces suspension or disqualification of eduGAIN membership to all Participant Federations and," So it's the "membership" that's being suspended/disqualified, and that's only communicated to all Participant Federations? Everything prior in that section is about Participant Federations and their suspension. And why only communicate the fact that someone was suspended to all Participant Federations instead of all Member Federations?	Peter	This is a leftover from the original document. **Could delete the word "participant" from 10th bullet in section 3.6.**
3.6	Suspension reasons. The no confidence vote opens a very vague area. I have a problem explaining this to the lawyer since I cannot imagine a reason for suspension which does not result from one of the first three points. Perhaps we do not need such an open and arbitrary possibility for suspension?	Tomasz	The vagueness is intentional, no change proposed.
3.6	Disqualification reasons. Contrary to the title of the section no real reasons except for a vote from the SG is given.	Tomasz	It's intended to be a possible end results of suspension, so behaviour that has led to suspension that is so bad permanent disqualification is proposed.
3.6	Automatic suspension by the OT. I believe this really was meant for technical blocking incoming federation data in cases requiring urgent action. Such a technical action by the OT should not be seen as a suspension. If I misinterpret this then some guidance would be nice.	Tomasz	still see that as suspension. Anything that causes service outage = suspension.
All	No governing law is specified. Pointed out by the lawyer as a flaw.	Tomasz	This is in the Declaration, not the Constitution: "Neither the existence of this declaration, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any federation. Members and operators remain bound only by their own respective laws and jurisdictions."