Consultation for Trusted Relationships for Access Management: The InCommon Model

Community Review

This consultation on Trusted Relationships for Access Management: The InCommon Model closed on Monday April 10, 2017. The authors are currently revising the text to address the comments.

Documents for review/consultation

- Trusted Relationships for Access Management: The InCommon Model
- Introduction to Identity Federations

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

Please add one comment per row and use as many rows as you need. If you have comments that do not lend themselves well to the tabular format below, you may create a new Google doc and link to it in the suggestion section below.

Number	Current Text	Proposed Text / Query / Suggestion	Proposer	+1 (add your name here if you agree with the proposal)	Action (please leave this column blank)
1	Identity Provider Assertion	In the "Intro to IF" document, this phrase is used a number of times. Was it invented for this text? Consider changing, perhaps to "Identity Assertion." The context makes the meaning clear, but that's from the perspective of someone who already understands the technologies. A newcomer might wonder if the assertion is "about" the IdP or "by" the IdP.	Walter H.	Scott Koranda Scott Cantor Judith Bush	
2	Intro document emphasis	While the "Intro. to Identity Federations" document is intended to overview "identity", paragraphs 1, 3, and 4 (of 4) talk more about information exchange (for authorization). Consider putting something like the two full paragraphs under "What Do We Trust" (i.e., "In a federated..." and "To enable ...") from the "Trusted Relationships" document up front in the "Intro" document to better explain the straightforward way identities are federated. Perhaps then follow with the fact that at the point at which participants are introduced, more can be shared (to the degree that an Identity-providing participant is able and willing).	B. Savage		
3	None	In today's environment executives, managers, and others interested in understanding the purpose of federation can be understandably concerned about security incident response. The document should explain that the Federation Operator is, or will soon be, prepared to coordinate and assist with security incidents that span across organizations.	Scott Koranda	Judith Bush Joseph Schwarze	
4	"Digital certificates to enable authentication of Participants' IdPs and SPs"	If the audience is executives, managers, and others interested in understanding the purpose of federation but without technical expertise than the less said about digital certificates the better. Consider eliminating that bullet.	Scott Koranda	-1 Jill Gemmill	
5	"Certifications" section of "Trusted Relationships" doc	a) Decision-makers may be looking for more regarding "why" one would want each certification - the benefit(s) of complying with a formal set of requirements. b) certifications seem listed in reverse order of frequency so readers may assume becoming a participant requires a high level of assurance compliance c) the limits of self-assertion is difficult to convey, so may be a bit confusing to readers: "The certification process may be self-asserted..." followed by "In all cases, the Federation Operation is responsible for ensuring the certification process has been followed." followed by (in bullet "Being an InCommon Participant") "Most aspects of compliance are self-asserted, but the Federation Operator does verify ..."	B. Savage		
6	Introduction to Identity Federations	The caption in the lower-left corner of the diagram is truncated. The final step should read "6 Participant operating the SP provides service."	David Walker / Mike Grady		
7	None	This is probably an extension to Point 2 above, for the Identity Federation Document. It helps to provide some examples of what the resources might be – an HPC system funded by the NSF; homework exercise provided by a textbook publisher; Box or Dropbox file sharing cloud service etc. Emphasize that federations allow policy to be exercised locally (the IdP controls what information is shared; the SP controls access).	Jill Gemmill		
8	"Provision of Identity Provider Assertions" in "Trusted Relationships"	I would add that requests for identity information by an SP are initiated when a person (or entity) attempts to access a specific resource; ie, user driven and happens just-in-time.	Jill Gemmill	Joseph Schwarze, Laura Paglione	
9	comment on 4, above	I think Scott's concern can be addressed by one more entry in the Glossary - certificates are part of the Public Key Infrastructure, a technology that secures the Internet and is used in applications such as on-line banking	Jill Gemmill		

10	Introduction to Identity Federations	I was struck by a couple of things that are absent from the "Introduction" document: a) there's no mention at all (in the text) of authentication, and b) there's only an incidental mention (in parentheses) that information can only be disclosed as part of a transaction initiated by the user. There's a lot of concern this side of the Atlantic at the moment about sharing of information between organisations: partly prompted by new legislation, partly by misbehaviour by large commercial players. With that background I could see this document being badly misunderstood. If were writing it over here, I'd start with "user approaches service; service needs reliable information about that user; ask an organisation that already knows them. FEDERATION :)". Having established that context, I think there would be much less risk of misunderstandings	Andrew Cormack	B.Savage David.Bantz Joseph Schwarze, Laura Paglione	
11	Glossary / Certifications	As someone new to the community, I am trying to identify / understand the definitions of all major components. In the glossary I could not find a definition for "Federation Operator", proposing that this definition be added. I find this definition to be crucial as the "Certifications" section mentions, "In all cases, though, the Federation Operator is responsible for ensuring that the certification process has been followed." Ultimately I want to make sure it is a reasonable ask of Federation Operators to do so.	Joseph Schwarze	Laura Paglione	
12	Glossary / Certifications	Suggest including the definition of "Community Member" to the glossary since it is used in quite a bit of the document	Laura Paglione		
13	Use of Identity Information	Perhaps also include that the IdP trust is not only in preventing release to unauthorized SPs, but also the release of only appropriate information to these authorized SPs.	Laura Paglione	David.Bantz	
14	General	Is it worth mentioning anything about the individual's role in the potential release of optional attributes through consent. It likely would complicate this document (which is really clear as is), though it seems like this is the area that has gotten a lot of exploration lately.	Laura Paglione		
15	Introduction to Identity Federations	Perhaps a restatement of 10 above, but I think the point should be made clearly that without the user identifying themselves in a secure fashion to the IdP, nothing about them is released to the requestor.	Brendan Bellina		

See Also

- Trust and Identity Consultations Home
- InCommon Working Groups Home