Consultation for InCommon Federation Participant Domain Use Policy

This consultation is now closed

Document for review/consultation

- Federation Participant Domain Use Policy DRAFT
- Federation Participant Domain Use Policy FINAL v1.0 (with updates from comments from this consultation)

Background

InCommon is seeking to modify its policy with regard to Participant use of domains in SAML metadata. This consultation seeks input on the new proposed policy.

For a definition of the word nonce as used in the document under consultation, please see: https://en.wikipedia.org/wiki/Cryptographic_nonce

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	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	Domains must be controlled by the registrar	A service must be operated by or on behalf of the registrar, but may be hosted in an arbitrary domain, with InCommon performing vetting replacing the DCV/WHOIS system of today	Nate Klingenstein (California State University)	Marcus Mizushima (California State University, Office of the Chancellor)	The new policy says: "Demonstration that a domain name is under the control of an InCommon Participant." which should meet this need.
2	"securely communicated to Participant"	is it worth covering what mechanisms are proposed? (and if the nonce is to be on a known record/URL or published in DNS why does there need to be a secure channel?	Alan Buxey (MyUNiDAYS Ltd.)		The word 'securely' has been removed from the updated text. Regarding specific methods, we did not want to lay those out in policy, but rather in our process documentation which will be built based upon this policy and may change over time.
3	"...at the requested DNS name (A or AAAA record)"	There are valid use cases where the InCommon Participant owns /controls the domain but uses CNAMEs to direct traffic to infrastructure operated by other organizations on behalf of the InCommon Participant. The restriction requiring A or AAAA records should be removed.	Scott Koranda (LIGO)	Patrick Radtke (Cirrus Identity)	Updated to remove the requirement for specific DNS record types.

See Also

- Trust and Identity Consultations Home
- TIER Working Groups Home
- TIER Data Structures and APIs Working Group (sponsoring group for the TIER Grouper Deployment Guide)
- Grouper Website
- Grouper Wiki