InCommon Federation Participant Domain Use Policy (09/22/2017)

Repository ID: TI.53.1
Authors: Nicholas Roy, The InCommon Registration Authority Team, The InCommon Operations Team
Sponsor: Ann West
Superseded documents: (none)
Proposed future review date: December 1, 2019
Subject tags: federation, metadata, trust, dns

Background

For any given domain name submitted in metadata, the InCommon Federation has historically required the organization name in an InCommon Participant's Participation Agreement to match the organization name in the domain's DNS registrant record. Today, while this is no longer a requirement for domains in endpoints, this procedure for establishing "ownership" still exists for domains in three locations in SAML metadata: Org URL, entityID, and shibmd:Scope. Today, many organizations anonymize their DNS registrant information, making this form of proof of ownership/control unusable.

In fact, "ownership" is increasingly synonymous with proof of control. The CA-Browser Forum, which maintains the policies for domain validation for all SSL and EV certificates, has, over the years, completely removed its use of the overly loaded term, ownership, to now entirely rely on the notion that proof of control of a domain or website is sufficient for validation purposes. See the most recent version of the CAB-Forum's EV Guidelines [1]

For InCommon's domain validation function, other forms of proof of control, other than the Registrant Organization found via manual WhoIs lookup, can and should suffice as well.

[1] https://cabforum.org/extended-validation/

Policy

InCommon allows a Participant to submit federation metadata pending the verification of domain names in the following elements that are subject to proof of control: Organization URL, SAML entityID and shibmd:Scope. 'Verification of domain names' means:

Demonstration that a domain name is under the control of an InCommon Participant.

Proof of control may be demonstrated in a number of ways including but not limited to:

1. Organization name in the DNS Registrant Record matches Organization name on the submitted InCommon Participation Agreement.
2. A nonce generated by InCommon, and securely communicated to Participant, is subsequently published as a DNS record (procedure to be determined by InCommon operations). This record is then verified as present by InCommon.
3. A nonce generated by InCommon, and securely communicated to Participant, is subsequently published in a predetermined location on an HTTP server responding at the requested DNS name (A or AAAA record). The nonce is then retrievable via an HTTP GET at that location.
4. Other methods approved for EV certificates by the CAB Forum may also be explored and added. See section 3.2.2.4 of the CAB-Forum's Baseline Requirements. [2]
5. Proof of control of a parent domain is sufficient validation for all subdomains submitted thereafter. An example follows: proof of control of example.com is sufficient for the party demonstrating control to subsequently use any subdomain of example.com such as foo.example.com.

[2] https://cabforum.org/baseline-requirements-documents/