Domain control validation procedure

This article has moved.

This article has moved to the InCommon Federations Operations wiki. The new page location is: ttps://spaces.at.internet2.edu/x/3wDGCg. P lease update your bookmark accordingly.

Jump to:

What is Domain Control Validation? | Demonstrate control with a DNS TXT record | Additional reading

What is Domain Control Validation?

Domain Control Validation (DCV) is a way to demonstrate that you have authority to register a service or DNS host name using the DNS domain in question. A common way to achieve this is to create a DNS TXT record containing a randomly generated token as the value.

InCommon uses this method to validate your authority to use a DNS domain or host when you register an entity in the InCommon metadata. If you submit an entity with either an entity ID or scope containing a previously unvalidated domain, the InCommon Registration Authority (RA) will ask you to perform the following to validation steps:

Demonstrate control with a DNS TXT record

Triggering condition

- The requesting Site Administrator (SA) submits metadata for approval via the InCommon Federation Manager (FM).
- The InCommon Registration Authority (RA) reviews metadata per the InCommon metadata validation procedure.
- If WHOIS data for any domain under review does not match the submitting organization -OR- the WHOIS data is not available, complete the following steps.

Validation steps

Step 1: RA emails the DCV TXT record creation instructions to the requesting SA. The instruction will include a 20-character validation code. Each assigned mixed-case, alphanumeric code is unique to the domain to be to be validated.

Step 2: SA uses the appropriate DNS management tool to: create a TXT record with the following information

```
Host: “_incommon.{domain}”
Type: TXT
Value: “incommon-dcv={unique_validation_code}”
```

Step 3: SA emails InCommon at help@incommon.org when this has been accomplished.

Step 4: RA verifies, archives evidence, and approves the metadata.

What is the `{domain}` mentioned in the steps above?

When validating an entityID, `{domain}` is the entire hostname in the URL. For example, if your entityID is "`https://idp.example.edu/services/idp`", the `{domain}` to be validated is "`idp.example.edu`".

When validating a SAML shibmd:Scope, `{domain}` is the domain you enter in the Scope field.

Additional reading

- Federation Manager

Related content

- Working with user data
- InCommon metadata validation procedure
- Domain control validation procedure
- InCommon Federation Software Guidelines
- Requirements to use Federation Manager
- What's New in Federation Manager
- Review and submit metadata
- Understanding the Endpoint Encryption Score
- Reset your Federation Manager user password
- Federation Manager

Get help

Can't find what you are looking for?

help Ask the community

- InCommon metadata validation procedure