

Metadata Registration Practice Statement for SURFconext

Version 1.2 (16 June 2023)

SURF operates a hub-and-spoke identity federation (SURFconext) on behalf of educational and research institutions in the Netherlands.

This document describes the Registration practices for both Identity Providers and Service Providers, as well as information on metadata aggregation for eduGAIN.

1. Identity Provider Practices

1.1 Identity Provider Registration Practices

Only institutions that belong to the SURF target group may join SURF and thus join SURFconext. The SURF target group consists of:

- Research universities
- University hospitals and tertiary medical teaching hospitals (STZs)
- Hogescholen (i.e. “universities of applied sciences”)
- MBO schools (i.e. “senior secondary vocational education institutions”)
- Research institutes and comparable institutions
- Libraries
- Other institutions financed by the Dutch Ministry of Education, Culture and Science.

For an Identity Provider to join the SURFconext, the following requirements must be met:

- The institution must have signed the SURFconext Identity Provider contract.
- The institution must have passed technical validation to the SURFconext test environment.
- The institution must provide technical and administrative contact information.

SURFconext operates an opt-in model for institutions, where the institution must agree explicitly to be connected to a specific Service Provider and to release attributes to this specific Service Provider.

1.2 Identity Provider Registration Practices for eduGAIN

There are no additional eduGAIN practices for Identity Providers.

2 Service Provider Practices

2.1 Service Provider Registration Practices

For a Service Provider to join the SURFconext, the following requirements must be met:

- The Service Providers must have signed the SURFconext Service Provider contract.
- The Service Provider must provide SURFconext with a description of the service.
- The Service Provider must provide SURFconext with a description of the technical and administrative contact details.
- The Service Provider must provide SURFconext with the list of minimally required attributes for using the service.

2.2 Service Provider Registration Practices for eduGAIN

The practices below are in addition to the “Service Provider Registration Practices” above.

- SURFconext will only publish metadata to eduGAIN for Service Providers that are connected to the SURFconext production environment.
- The Service Provider must explicitly request to connect to eduGAIN through SURFconext.
- The Service Provider must provide eduGAIN compliant SAML 2.0 metadata to SURFconext.
- Updates to the metadata provided by the Service Provider that is re-published by SURFconext to eduGAIN are reviewed by the SURFconext operational team at least every working day and published after approval.

SURFconext validates the Service Provider information including the attribute requirements, before accepting the Service Provider to the production environment.

3. SURFconext Metadata Aggregate for eduGAIN

SURFconext maintains an aggregate of all metadata it exposes to eduGAIN on the following location:

<https://metadata.surfconext.nl/edugain-upstream.xml>

The metadata document signature can be validated using the following X.509 certificate:

-----BEGIN CERTIFICATE-----
MIIEKjCCAhICEG12w6QqayYAWntxDN59dU0wDQYJKoZIhvcNAQELBQAwpDELMakG
A1UEBHMCTkwxEDA0BgNVBAoMB1NVUkZuZXQxGzAZBgNVBAMMElNVUkZjb25leHQg
Um9vdCBDQTAEFw0xOTAxMTQxNjM5MDVaFw0yNDAxMTgxNjM5MDVaMGsxGzAJBGNV
BAYTAk5MMRAwDgYDVQIDAdVdHJlY2h0MRAwDgYDVQQKDAdTVVJGbmV0MRMwEQYD
VQQLDAPTVVJGY29uZXh0MSMwIQYDVQQDDbPTVVJGY29uZXh0IG1ldGFkYXRhIHNP
Z25lcjCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMckFyqXzW7dbMt4
wDdSLaAjFAbNziUgQaivu4d19Uf/cZ4f36a9DfQBUSraNoIR76ruwK3TPfFalemp
xmWTsoVSQpb3A0sWbU+i0YKS1cmcQMUC1Fef2j1Ibuk4B4nEu9S5saGNVGNvUJ+Y
jDUpC5vyyp7bow9E1md2jIBI6Mw+Zh1mkPucqaphxurWnm0KbxTZrYLOBZ1IXj6r
yrRoFwwtjEH+CW8cRn80ATK0q4yb0BVR2gY2tp/1TpASHZ3WVWBK0prwK0KkusY6
ck+/vv1k46IdEr803NB0Dm3ECh3i65mfCawzVTtd/md874paK+65f1JeVyd5I5a1
M2KEpvkCAwEAATANBgkqhkiG9w0BAQsFAA0CAgEAjvJXXkx0qh3K0k2NdDG5E0Ty
bA+koRbAqhdy/qJoSnqTzwbXJc6aPs+L4q2PIoLo0gNj1Nm1taLusaak+CBx3ar
1kxEika5FM0dqFjD3i7Y5U0FMeDB5cReo8TNdo31VGoY7CbRjtgHLRTuKzNmIfEm
ahLnHIBtarE82b7Mpg0aLxjrrR+t8wScry+e9AEPzC5bWxtPJA+0hU8U9hMu0s5
SzKmHwYue4WY3q1rRaDpK3fqqXRDRfznNn9/RDDbBos7CRMSAPEmA028qLKBw/1z
a2TKQLddZ3uoCurFNbToSTueKYVEnveQN02P5X6uy4rcYkjSiwbmHo7jYuHAXx4
uGzHMpoqo6Nx+2iYjtUo3dJUXzcZai3X+RuuMKXXvqGzrxJsoKayNVAE1dwoUHJl
RouPhDLtdZq/pb10RhFS8r10rKhSScgrNuN9LTTV7EPFeVr8trocnw18IruH+eNL
6/7b5Y7fb7rvpxehjWrTz8a9BXAIAv+bgyrg4OHGRcNIQb0XF438HD9r8Zb92B6Z
VCR3aVS5496+1td+8aN/B1zo59LhKPiHyGZCPHFV/oBqG7nxp603kcWmJ0cG+AgB
9bFiAimF5LLk/LnMfplK9w0vvxwVcdQkdGvPYvEGNtttj0QC7/jM4ZeihGb60yzy
DZA6aeg73/yg0ATQ13A=
-----END CERTIFICATE-----