Metadata Registration Practice Statement for SURFconext

Version 1.1 (20 February 2019)

SURFnet 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 SURFnet target group may join SURFnet and thus join SURFconext. The SURFnet target group consists of:

- Research universities
- University hospitals and tertiary medical teaching hospitals (STZs)
- Hogescholen (i.e. “universities of applied sciences”)
- Research institutes and comparable institutions
- Company R&D departments
- 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.

SURFnet 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.

- SURFnet 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.
- The metadata provided by the Service Provider that is re-published by SURFconext to eduGAIN is updated by the SURFconext operation al team by request of the Service Provider. Service Providers can request an update of their metadata by contacting the SURFconext ope rational team at support@surfconext.nl.

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

3. SURFnet Metadata Aggregate for eduGAIN

SURFnet 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
A1UEBhMCTkwxEDAOBgNVBAoMB1NVUkZuZXQxGzAZBgNVBAMMElNVUkZjb25leHQg
Um9vdCBDQTAeFw0xOTAxMTQxNjM5MDVaFw0yNDAxMTgxNjM5MDVaMGsxCzAJBgNV
BAYTAk5MMRAwDgYDVQQIDAdVdHJlY2h0MRAwDgYDVQQKDAdTVVJGbmV0MRMwEQYD
VQQLDApTVVJGY29uZXh0MSMwIQYDVQQDDBpTVVJGY29uZXh0IG1ldGFkYXRhIHNp
Z25lcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMckFyqXzW7dbMt4
wDdSLaAjFAbNziUgQaivu4dl9Uf/cZ4f36a9DfQBUSraNoIR76ruwK3TPfFalemp
xmWTsoVSQpb3AOsWbU+i0YKS1cmcqMUC1fef2j1IbuK4B4nEu9S5saGNVGNvUJ+Y
jDUpC5vyyp7boW9E1md2jIBI6Mw+ZhlmkPucqaphxurWnm0KbxTZrYLOBZ1IXj6r
yrRoFwwtjEH+CW8cRn8OATK0q4yb0BVr2gY2tp/lTpASHZ3WVWBK0prwK0KkusY6
ck+/vvlk46IdEr803NB0Dm3ECh3i65mfCaWzVTtd/md874paK+65f1JeVyd5I5al
M2KEpvkCAwEAATANBgkqhkiG9w0BAQsFAAOCAgEAjvJXXkxOqh3K0k2NdDG5EOTy
bA+koRbAqhdY/qJoSnqTzwBxJc6aPs+L4q2PIoLo0gNJj1Nm1taLusaaK+CBx3ar
1kxEika5FM0dqFjD3i7Y5U0FMeDB5cReo8TNdo31VGoY7CbRjtqHLRTuKzNmIfEm
ahLnHIBtarE82b7Mpg0aLxjrRR+t8wSCriy+e9AEPzC5bWxtPJA+OhU8U9hMuOs5
SzKmHwYue4WY3q1rRaDpK3fqgXRDRfznNn9/RDDbBos7CRMSAPEmAO28qLKBW/1z
a2TKQLddZ3uoCurFNbToSTueKYVEnveQNO2P5X6uy4rcYkjeSiwbmHo7jYuHAxx4
uGzHMpoqoGNx+2iYjtUo3dJUXzcZai3X+RuuMKXXvqGzrxJsoKayNVAE1dWoUHJl
RouPhDLTdZq/pblORhFS8r10rKhSScgrNuN9LTTV7EPFeVr8trocNwl8IruH+eNL
6/7b5Y7fb7rvpxeHjWrTz8a9BXAIAv+bgyrg4OHGRcNIQb0XF438HD9r8Zb92B6Z
VCR3aVS5496+1td+8aN/Blzo59LhKPiHyGZCPHFV/oBqG7nxp603kcWmJOcG+AgB
9bFiAimF5LLk/LnMfplK9w0vvxWVcdQkDgVPYvEGNtttj0QC7/jM4ZeihGb6Oyzy
DZA6aeg73/ygOATQ13A=
-----END CERTIFICATE-----
```