Information for SPs from other federations

ⓘ If you are a Service Provider from another federation and you would like to offer your service(s) to an Identity Provider within SURFconext, please read on.

Non-technical: policies and contracts

Besides offering the federation as a technical infrastructure described below, SURFconext also has policies and contracts in place. These are meant to increase the level of trust between the participants of the federation, as well as to comply with European laws on privacy and data protection. SURFconext assists their Identity Providers with all the necessary legal affairs that must be taken care of when using (online) services. In practice, this means:

- If you are a **commercial** Service Provider, you need a SURFconext Connection Agreement before you can offer your service through SURFconext. Also, in many cases, you will probably have to sign a Processor Agreement with any Identity Provider that uses your service. Of course, this is between you and the Identity Provider; SURF however provides useful templates. Before you intend to connect to SURFconext, please contact the SURFconext Team through support@surfconext.nl.
- If you are a **Research & Scholarship** Service Provider, please note that SURFconext does not yet fully support this Entity Category.
    - Our current policy is that only R&S SPs which *also* support the GÉANT Data Protection Code of Conduct (CoCo) will be connected to IdPs with R&S enabled
    - Attribute release between a R&S IdP and a R&S and CoCo SP still has to be configured manually, by the SURFconext Team. This happens once per day, so there might be a small delay between the availabilty of R&S in the eduGAIN metadata and the actual attribute release
    - Please contact the SURFconext Team through support@surfconext.nl if you have any questions or requests

ⓘ **SURFconext strongly recommends** every Service Provider to support the GÉANT Data Protection Code of Conduct (CoCo). If you do not yet support this document but are able to do so, please express your support as soon as possible. Identity Providers from SURFconext are much more likely to connect to your service if support for the CoCo is present.

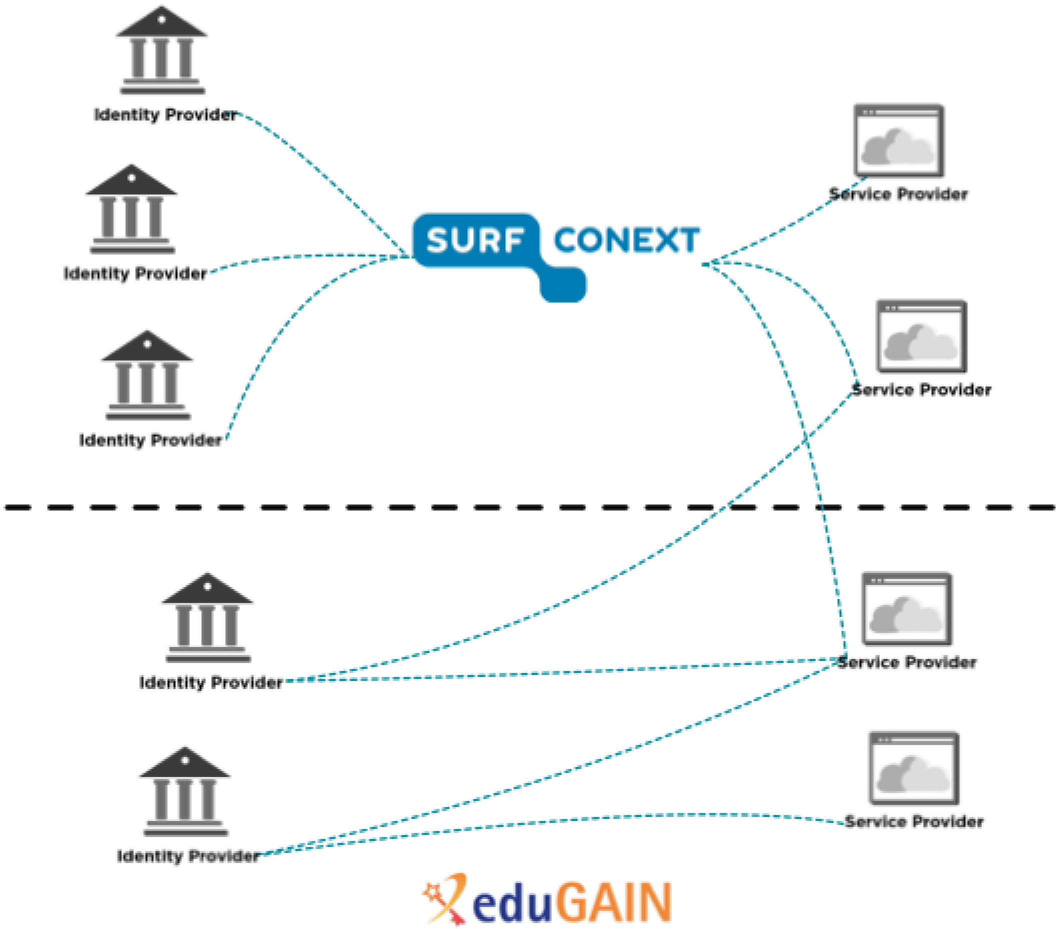
Technical: SURFconext - hub-and-spoke architecture

In contrary to most federations, SURFconext operates a hub-and-spoke model. This means all Identity Providers are only connected to a single Service Provider (namely: SURFconext) and all Service Providers are connected to a single Identity Provider (namely: SURFconext). This is different from a *mesh* federation, where all Identity Providers and Service Providers are responsible for their own connections to each other.

eduGAIN also operates in a *mesh* manner. SURFconext supports this as follows:

- Within SURFconext, all (local) Identity Providers and (local) Service Providers connect to and flow through the hub. **Note:** this doesn't mean all Identity Providers automatically release their attributes to all Service Providers! The hub keeps a record of which Identity Providers want to release attributes to which Service Providers.
- Service Providers from SURFconext who want to offer a service to Identity Providers from other federations (through eduGAIN) must **also** support *mesh*, besides connecting to our hub. A connection from a Service Provider within SURFconext to an Identity Provider from another federation is **direct** and **does not** pass through the SURFconext-hub.
- It is different the other way around: when an Identity Provider from SURFconext wants to connect to a Service Provider from another federation, the connection **does** flow through the SURFconext hub. In this case, the Service Provider must connect to the SURFconext-hub, in contrary to connecting directly to the Identity Provider (the SURFconext-hub **is** the Identity Provider for your service).
- SURFconext publishes all opted-in Identity Providers in eduGAIN. Please take note of the following:
    - All login URLs start with https://engine.surfconext.nl, but they contain a unique identifier to point the user to the correct Identity Provider
    - All contact details in the metadata are equal
    - All signing certificates are equal. **Note:** this can be problematic for Service Providers using certain versions of Microsoft software.

The following image describes how connecting your service to an Identity Provider in SURFconext and eduGAIN works:


Identity Provider
Identity Provider
Identity Provider
SURF CONEXT
Service Provider
Service Provider
Identity Provider
Service Provider
Identity Provider
Service Provider
eduGAIN