# Connecting your service to SURFsecureID

Depending on the integration option you choose for your service, you need to follow a different connection procedure and technical implementation.

1) SFO authentication

- **Procedural**
  An institution must give permission for a SFO integration in the SURFsecureID production environment. Although an SFO integration is almost always implemented by the institution itself, it is possible that someone else may want to implement it. By requiring permission from the institution we make sure that the proper persons are notified. The SURFconext contactperson (SURFconext-verantwoordelijke) needs to provide this permission by sending an email to support@surfconext.nl.
- **Technical**
  Implement the SFO connection. There is a technical description of how a SFO connection works and what is needed to connect with it. This integration is based on the widely used open standard SAML2, so an integrating can be easily made. However, for some popular systems, we've created a description or even software to make it even easier:
  - ADFS MFA plugin
  - F5 BIG-IP
  - Citrix NetScaler
  - SimpleSAMLphp

2) Standard authentication. For the majority of cases this just means connecting to SURFconext as a regular Service Provider (if not already done).

- **Procedural / contractual**
  Because this integration option uses SURFconext for the first factor and privacy sensitive information from the user is transferred to the service, it is necessary to have the correct agreements in place. Make sure you follow the SURFconext contractual obligations. This step is not necessary when you use the SURFsecureID test environment.
- **Technical: standard**
  Follow the standard connection procedure for SURFconext. When the SP is working, you have several options to enable SURFsecureID for the SP.
  - The SURFconext team can enable the desired Level of Assurance in configuration to enable SURFsecureID for your connection.
  - The SURFconext team can enable the desired Level of Assurance based on a step-up policy
  - The SP can also request a specific Level of Assurance.

More info:

- Service Provider technical requirements
- Differences between SURFconext and SURFsecureID
- SURFsecureID metadata
- Using Levels of Assurance