# Documentation for Service Providers

For Service Providers there are normally no changes needed to make use of SURFsecureID. To require SURFsecureID for all logins to a specific Service Provider, or for all logins by one or more IdP's to a specific Service Provider, the SURFconext team can set a configuration option to enforce this.

The following documentation is for *special requirements* which can not be satisfied with this configration and that require the service to make use of a special SAML endpoint.

This part of the wiki gives all the (technical) information that can be of importance for Service Providers working with SURFsecureID.

- To start with it is explained how you can connect your service with the SURFsecureID gateway. Actually it is very similar to connecting to SURFconext. The are only small differences, like using other metadata. Also you will have to tell the gateway the required Level of assurance (LoA1, LoA1.5, LoA2 or LoA3). For an overview of all the differences between SURFsecureID and the SURFconext authentication procedure, have a look on this page.
- Else in the wiki we already described the concept of levels of assurance. Here you will find the (technical) details needed to communicate the strength of authentication between the SURFsecureID gateway and the Service Provider.
- With SURFsecureID you have also the possibility to have second factor only authentication. In that case the first factor authentication (username and password) is done at the IdP (and not at SURFconext). We explain the differences between second factor only authentication and the 'normal' authentication. After that the SAML AuthRequest and SAML response for second factor only authentication are explained. Also you can read how to implement second factor only authentication and finally you will find a link to an example.
- To be able to use SURFsecureID metadata is needed. Each of the three environments has two types of metadata; one for the regular SAML endpoint, and the other for the second factor only endpoint.
- On the next page we give examples of an authentication request at a specific LoA, You will see also two examples of the SAML response in case of an authentication failure.
- You can use SimpleSAMLphp to request a specific minimum level op assurance (LoA) from the SURFsecureID gateway and to verify the LoA at which the user is authenticated. For both instances you will find an example.
- If you use Shibboleth as your sign-on system, you can read here how to configure it for SURFsecureID.
- For testing your connection to SURFsecureID you should not use any 'regular' account, but a special eduID account