SURFsecureID

With SURFsecureID users have to do a second authentication step, above their 'normal' username and password login. The result is a higher security for the Service Provider (SP) and the Identity Provider (IdP). This wiki explains the principles behind SURFsecureID and gives you all the information you need to install it.

- The introduction explains the basics of SURFsecureID. Mainly there are only three steps to be taken.
- On the next page (Architecture) you will find a picture showing the relation between the different 'actors': the SURFsecureID gateway, the SURFconext gateway, the SP's and the Second factors (SMS, Tiqr and YubiKey). Also the authentication flow, consisting of 6 steps, is explained.
- On the page Levels of assurance you can read that in SURFsecureID there are four different levels of assurance:
  - LoA 1: only username/password authentication
  - LoA 1.5: username/password + second factor
  - LoA 2: user's identity is checked, authentication with username/password + SMS, Tiqr or AzureMFA
  - LoA 3: user's identity is checked, authentication with username/password + Yubikey or FIDO2 (hardware token)

  Explained is also why in SURFsecureID the attributes do not have a level of assurance.
- The road map shows you the plans SURF has to improve further the qualities of SURFsecureID. You are encouraged to engage in our periodic SURFconext meetings or contact us at info@surfconext.nl to discuss your authentication needs.
- In the FAQ you will find a list of the most commonly asked questions, together with our answers on them.
- In the Documentation for Identity Providers (Dutch), you will find information on how institutions are able to use this service. This has above all an organizational impact, rather than a technical one.
- The last part of this wiki, Documentation for Service Providers, gives a lot of detail (technical) information specific for Service Providers.