Levels of Assurance

When users access online services, they want to be confident that their data and services are secure and their privacy is protected. Institutions and Service Providers that offer online services also need to verify a user's identity to make sure only the right users are accessing the right information. That is why identity assurance is needed.

In general there are three types of authentication factors:

- Something the user knows (password or PIN)
- Something the user has (mobile phone or token)
- Something the user is (fingerprint or other bio-metric data)

Strong authentication refers to the use of more than one of these factors. Generally this results in a higher level of assurance (LoA) about the user.

Assurance level standards

There are several international standards for identity assurance, like NIST (US), eIDAS (Europe, previously STORK) and ISO29115. SURFsecure ID is based on ISO29115. The four levels of identity assurance commonly used are:

LoA 1	Little or no confidence in the asserted identity
LoA 2	Some confidence in the asserted identity
LoA 3	High confidence in the asserted identity
LoA 4	Very high confidence in the asserted identity

The different specifications elaborate on the meaning of these labels by specifying requirements for:

- registration
- authentication token management
- online authentication

The resulting assurance level depends on the combination of these aspects. The aspect with the lowest score determines the overall assurance level (a chain is only as strong as its weakest link).

Level of assurance requirements: risk based

The required level of assurance can be estimated on:

- the importance of the data and
- the potential damages if these data were to be obtained or modified by unauthorized users

These risks must be assessed to be able to decide what level of assurance is needed for your service (see also SURFnet guidelines).

Using levels of assurance to express strength of authentication

To express the strength of authentication and the identity of the user an assurance framework as described in ISO/IEC 29115 is used (similar to NIST Special Publication 800-63-1). The SURFsecureID gateway supports three levels of assurance:

- LoA 1: Password authentication through SURFconext at the users home IdP
- LoA 2: LoA 1 + SMS or Tiqr authentication
- LoA 3: LoA 1 + YubiKey (hardware token) authentication

Second Factor Only (SFO) authentication

With Second Factor Only (SFO) Authentication "Level" is used to indicate the authentication strength: LoA does not apply. There are two levels:

- Level 2: SMS or Tiqr authentication
- Level 3: YubiKey (hardware token) authentication

Level of assurance vs robustness of infrastructure

The LoAs described by NIST and STORK primarily focus on the robustness of the authentication. The robustness of the technical infrastructure is mostly beyond their scope.

It is assumed that proper measures are taken to prevent authentication protocol threats such as eavesdropping, man-in-the-middle, replaying, and hijacking. Attacks are not limited to the authentication protocol itself. Other attacks include the use of malicious code to compromise authentication tokens, insider threats to compromise authentication tokens, social engineering to get a subscriber to reveal his password to the attacker, “shoulder-surfing”, fooling claimants into using an insecure protocol, when they think that they are using a secure protocol, or intentionally denying ever having registered by subscribers who deliberately compromise their tokens.

Other types of threats are (SAML) assertion related such as modification, disclosure, repudiation, reuse or redirect. Countermeasures should be taken to prevent these attacks as well. The most important ones are the use of digital signatures to sign assertions and the use of SSL/TLS to secure the communication channel.

Both control measures are required to fulfill the requirements for LoA2 and LoA3 and are already in place in SURFsecureID.

Level of assurance vs attributes

SURFsecureID solely focuses on authentication LoA. No LoA is assigned to the attributes of the user's identity.

Several attributes provided by the IdP (e.g. first and last name, e-mail address) will be validated during registration and identification. In theory a LoA could be assigned to these attributes, which in attribute-based access control scenario’s could make authorization more reliable. There are however some arguments against doing this:

- Mixing attributes with different LoA’s is complex
- There is no suitable way to express differing LoA’s for attributes in SAML assertions
- The registration process will be more complex

Because of these arguments SURFsecureID solely focuses on authentication LoA.