Using Levels of Assurance to express strength of authentication

SURFsecureID uses Levels of Assurance (LoA) to express the strength of authentication. This page describes how a service or institution can request a LoA for a specific service or part of a service. Furthermore, the LoA identifiers differ between the environments and between the authentication method used.

How to request a Level of Assurance?

A service can communicate the required LoA to the SURFsecureID gateway and verify the strength at which a user was authenticated.

There are three scenarios how to request a LoA, explained below. They can be combined: the gateway will use the scenario having the highest LoA.

1. Minimum LoA specified by the institution (static)

The institution requires, for a specific SP, its users always to be authenticated at a certain minimum LoA.

The institution must ask SURFnet to set this minimum. SURFnet will configure this on the SURFsecureID gateway.

2. Minimum LoA specified by SP (static)

The SP requires always a certain minimum LoA.

The SP must ask SURFnet to set this minimum. SURFnet will configure this on the SURFsecureID gateway.

3. LoA defined during authentication (dynamic)

A SP can request authentication at a certain LoA by specifying it in the SAML `AuthnRequest`. The SP can send this request to the gateway at any time, also when a user is already logged in. This makes it possible to raise the LoA for a user depending on the context, e. g. if the user wants to enter the admin part of the site.

The LoA is passed to the SURFsecureID gateway in an `AuthnContextClassRef` element in a `RequestedAuthnContext` element in the SAML `AuthnRequest`.

The requested LoA is interpreted as a minimum. The SURFsecureID gateway:

- Will not perform authentication below the requested loA.
- May perform authentication at a higher level, in which case the higher level LoA will be expressed in the returned SAML `Assertion`.

The LoA identifiers are used in SAML messages communicating the LoA between the SURFsecureID gateway and SP. The actual method of authentication itself (e.g. SMS + password) is not communicated!

- The SURFsecureID gateway will report the SP the actual LoA at which authentication was performed. This is done with the AuthnContextClassRef element of AuthenticationContext in the SAML Assertion in the SAML response.

Standard Authentication LoA's

When using the standard authentication with SURFsecureID, four levels of assurance (LoA) are supported:

- LoA 1: Only password authentication at the institution's IDP
- LoA 1.5: LoA 1 + any SURFsecureID second factor, no extra validation of the user's identity
- LoA 2: LoA 1 + SMS, Tiqr or AzureMFA authentication AND the identity of the user is validated
- LoA 3: LoA 1 + YubiKey or FIDO2 (hardware token) authentication AND the identity of the user is validated

Each LoA is assigned to an identifier and is different for each type of environment used:

	Test	Production
LoA 1	`http://test.surfconext.nl/assurance/loa1`	`http://surfconext.nl/assurance/loa1`
LoA 1.5	`http://test.surfconext.nl/assurance/loa1.5`	`http://surfconext.nl/assurance/loa1.5`
LoA 2	`http://test.surfconext.nl/assurance/loa2`	`http://surfconext.nl/assurance/loa2`
LoA 3	`http://test.surfconext.nl/assurance/loa3`	`http://surfconext.nl/assurance/loa3`

These identifiers are used to communicate the strength of authentication between the SURFsecureID gateway and the Service Provider. The actual method of authentication (e.g. SMS + password) at the institutional IdP is not communicated.

- The SURFsecureID gateway will report the LoA at which authentication was performed to the SP in a `AuthnContextClassRef` element in a `AuthenticationContext` in the SAML `Assertion`.
- A SP may request authentication at a specific LoA by specifying the identifier in a `AuthnContextClassRef` element in a `RequestedAuthnContext` in a SAML `AuthnRequest`. See SAML message examples for an example `AuthnRequest` that requests authentication at a specific LoA.

Second Factor Only (SFO) authentication LoA's

With Second Factor Only (SFO) Authentication "level" is used to indicate the authentication strength:

- Level 1.5: any SURFsecureID second factor, no extra validation of the user's identity
- Level 2: SMS, Tiqr or AzureMFA authentication AND the identity of the user is validated
- Level 3: YubiKey or FIDO2 (hardware token) authentication AND the identity of the user is validated

The following identifiers are used:

	Test	Production
Level 1.5	`http://test.surfconext.nl/assurance/sfo-level1.5`	`http://surfconext.nl/assurance/sfo-level1.5`
Level 2	`http://test.surfconext.nl/assurance/sfo-level2`	`http://surfconext.nl/assurance/sfo-level2`
Level 3	`http://test.surfconext.nl/assurance/sfo-level3`	`http://surfconext.nl/assurance/sfo-level3`