Single-Sign-On with SAML 2.0

Technical information to setup Login Module SAML

Company Details

Name:	SEEBURGER AG
Address:	Edisonstraße 1
	DE-75015 Bretten

Contact Details

Name:	SEEBURGER Cloud Service Team
E-mail:	support@cloud.seeburger.de
Phone:	+49 (0) 7252 96 1443

The SAML Login Module enables the Single-Sign-On (SSO) authentication by using an external SAML Identity Provider (IDP at customer side) and acts on SAML Service Provider (SP, SEEBURGER Cloud) side, how it can be seen in the SAML Process (see diagram below). For a better understanding, the configuration data is respectively referred to the SAML Process. Hereby, it can be seen during which SAML authentication steps the respective data is needed.
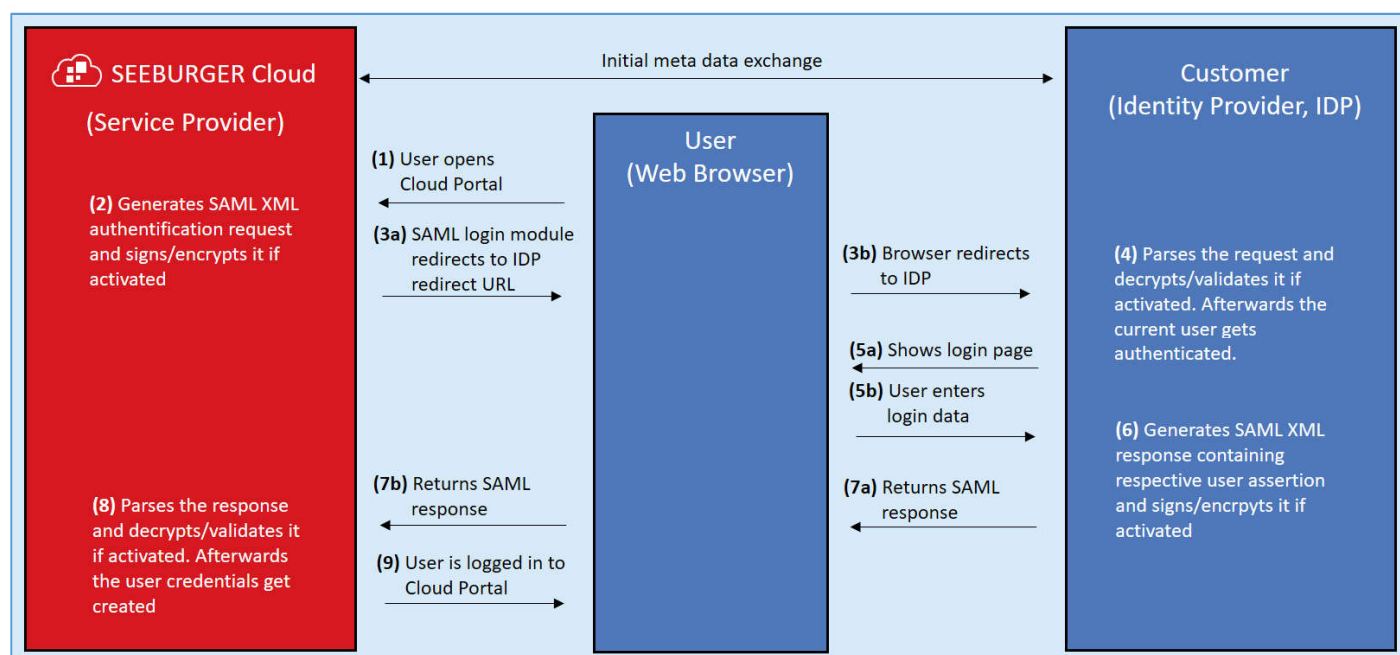
To configure your IDP with the SEEBURGER Cloud, please use this data sheet we prepared for you. The first information is for your administrator, the **data you require** to use SAML with the SEEBURGER Cloud. The second part contains the **data, which needs to be delivered** to use SAML with the SEEBURGER Cloud.

Note: After SAML is activated for the organization, each new user, which is invited via the **My Company** App, will be created directly without the need for registration process. An invitation email is sent in this case containing the SAML Login URL.

Hint: To exclude users from the SAML process, please provide login name via e-mail to the contact address named above. The affected user will receive a password change request via e-mail. After changing the password, he will be able to login without using SAML login module. The same procedure can be used to include users to the SAML process.

1. SSO with SAML – Information for YOUR configuration

Issuer (SP):	SEECLOUDID
Assertion Consumer URL (SP):	https://portal.cloud.seeburger.de/cas/login[1]
SIGNATURE Certificate:	saml.portal.seeburger.cloud.cer[2]
ENCRYPTION Certificate:	saml.portal.seeburger.cloud.cer[2]

2. SSO with SAML – Information for SEEBURGER Cloud configuration

Your URL (IDP):	This information is required.
	Note: The URL of the SAML Identity Provider. After the authentication request is created and executed by the Login Module, the browser redirects the user to this URL (see step 2/3 of SAML Process).
SIGNATURE Certificate:	Note: We classified SHA-1 as medium secure. We recommend using an SHA-2 algorithm to meet the highest standards of security.
ENCRYPTION Certificate:	Note: We classified 3DES as medium secure. We recommend using AES/256 to meet the highest standards of security.

Assertion Attributes

After the Login Module has retrieved, extracted and verified the authentication assertion from the IDP (see step 8 of SAML Process) the respective attributes within the assertion are used to create the required user credentials.

Use Subject For User Credential	Activated // Deactivated
	Note: If "UseSubjectForUserCredential" is activated, the Login Module extracts the name of the user from the assertions subject NameID.
User:	This information is required.
	Note: If "UseSubjectForUserCredential" is deactivated the authenticated user is extracted as normal assertion attribute by the name which can be defined by setting this User attribute.
E-Mail:	This information is required.
First Name:	This information is optional.
Last Name:	This information is optional.
Full Name:	This information is optional.
Language:	This information is optional.
Phone Number:	This information is optional.
Department:	This information is optional.

---

[1] When using an individual layout, this value corresponds to the custom URL.

[2] You can download our data sheets and certificates on the following URL: **www.seeburger.com/cloud/connect-the-cloud/**