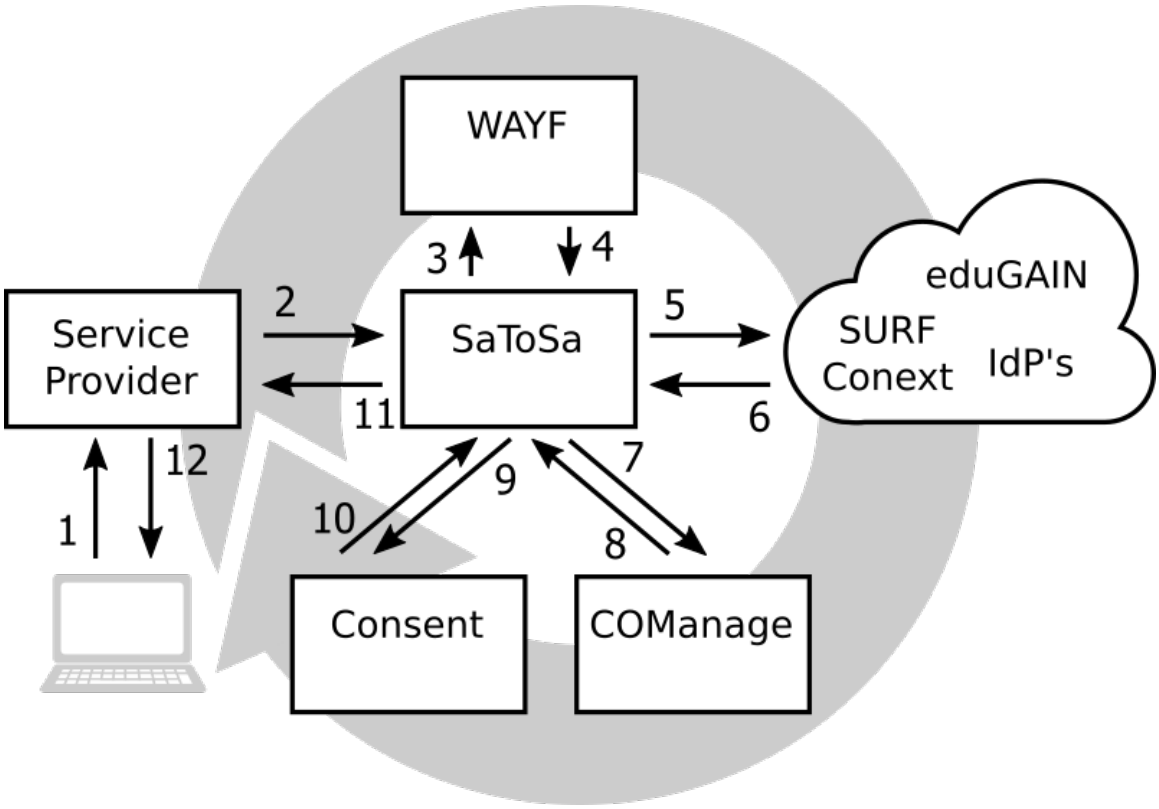
Userflow

This page shows the steps a user goes through when accessing a service connected to the SCZ-environment (after initial sign-up with a CO in COmanage):



1. A user visits the URL of a service (like a wiki) and clicks a link to authenticate via SCZ
2. The (browser of the) user is (automatically) redirected to the SCZ component SATOSA
3. If necessary, a Where-Are-You-From-screen is presented so the user can select the IdP where he/she wants to authenticate
4. After the optional WAYF, the user is directed back to SATOSA (almost invisible to the user)
5. The user is directed to his/her IdP/institution (can be via SURFconext, which would be transparent for the user, can be eduGAIN or an IdP connected to SATOSA directly)
6. After successful authentication at the IdP, the user is redirected back to SATOSA, with their attributes. If authentication is via SURFconext, SURFconext is using an Attribute Release Policy (ARP) to only release R&S-attributes to SATOSA
7. SATOSA uses a combination of attributes that uniquely identify the user and SP entityID to gather supplementary CO specific COmanage attributes.
8. If the IdP has provided identifying attributes, SATOSA searches a database the SCZ component COmanage has provisioned and uses them together with the entityID of the service to find the CO and CO-specific attributes:
    a. On initial provisioning of the user in COmanage, so where COmanage is the SP, the IdP attributes can be used (for instance when we want to use the name supplied by the user's IdP).
    b. In all other cases, the CO specific COmanage attributes are injected into the SAML flow to the SP, while removing the original IdP attributes. If the identifying attributes are not supplied, SATOSA will send an empty assertion.
9. SATOSA can be configured to show an Inform screen. If so configured, an inform is shown, telling the user she is leaving the boundaries of the institution explaining the (legal) consequences of this action.
10. The user can only choose to completely grant or deny continuation to the service. There is no middle road on a per-attribute basis. If the user chooses to deny access, the flow stops here.
11. If consent was given (or configured not to be required) SATOSA will send the SP/CO specific attributes to the service.
12. Based on the internals of the service (like required attributes and whether they are supplied), the user does or does not get access to the service.

More info about the technical components and their relations that make up the SCZ environment can be found on Technical overview of SCZ .
How to configure invite-flows, invite users etc can be found in (subpages of) End user documentation SCZ COmanage .