Connecting services to the SCZ-environment

Basic checks

The SCZ is great, but not the best solution for every situation. Some basic questions you might want to think about before contacting us (please do contact us, we will help 😊):

- If the service you want connected is
    - web/browser based, does it already have support for federated authentication protocols such as SAML or OIDC? If not: is there anybody willing and able to change (and maintain) the application/service so it is able to handle a SAML or OIDC connection?
    - a non-web service, SCZ will provision an LDAP under your control. Does your application already use an LDAP?
- What users need to access the service?
    - Only people from the Netherlands? Or also from other parts of the world?
    - Only people with an educational account, or also people without such an account?
    - Will the home organisation of the potential users connect their IdP to the SCZ?
- Do you actually need the SCZ, or does SURFconext also supply what you want? SURFconext offers federated authentication for browser based services, teams, authorisation rules, SURFsecureID (step up/strong authentication), guest users etc.

In case you're not sure about these questions, please contact the SCZ-team, for instance raoul.teeuwen@surfnet.nl .

Followed technical standards

The SCZ solution adheres to/plans to adhere to the following standards:

- Status: implemented
    - SAML 2.0 (as implemented by SURFnet in SURFconext)
        - urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect (preferred in accordance to SAML2int profile)
        - urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST (can only be used in case your software doesn't support HTTP-Redirect)
    - OpenID Connect (for Service Providers).
    - LDAP.
- Status: planned
    - for exchanging group information, we plan to follow the "AARC guidelines on expressing group membership and role information" . Those guidelines are also adopted by large research infrastructures, see for example https://www.egi.eu/about/newsletters/aegis-group-endorses-aarc-guidelines-on-membership-information-exchange/ .

Technical and Policy part

Connecting a service to the SCZ-environment has a technical as well as policy aspect. During the pilot, we will be less strict on the policy part, but if the pilot leads to a Go and a production ready service will be built, it's important to realise the following policy is currently considered for services that want to connect:

1. Policy.
    a. We want to make CO's use the service they seem fit for use. If SCZ starts demanding services need to comply to certain standards before we connect a service, we could get a situation where CO's can't use a service they themselves deem fit to use. Therefor, currently, SCZ does connect services CO's and service providers want to have available. We do advise CO's to check out the AARC Policy Development Kit (MOOC), which provides templates of all kinds of policies like Acceptable Use Policy. The AARC Policy Development Kit references links like
        i. services to comply to the GÉANT Data Protection Code of Conduct ("CoCo"), with the intend to comply with v2 GDPR version of the Code of Conduct
        ii. services to comply to the Research and Scholarship Entity Category
        iii. services to comply with and use Sirtfi
        iv. services to comply to the REFEDS Assurance Framework

    b. SCZ will check for certain things:
        i. the service to use a SSL certificate: as a rule of thumb, it should have at least a "B" rating on SSLLabs.com (but preferably better, of course). If you would like to test your server for configuration issues, you can use the Qualys SSL labs server test at: https://www.ssllabs.com/ssltest/
2. Technical: what is needed on the technical side depends on your situation. We have documented some common situations and relevant information in the child-pages of this page:
    - Connecting a web service to the SCZ environment via SAML
    - Connecting to the ldap
    - PAM Module
    - Supplied attributes
    - Sample user consent texts/AUPs/code of conduct
    - Connecting a service to the SCZ using OIDC
    - SSH PublicKeys in LDAP
    - Connect eduGAIN IdP's

After the above technical connection has been taken care of, a service needs to be connected to a CO in our Membership Management Service (MMS, for example COmanage) before receiving attributes stored in the MMS (enter the entityID of the SP for "Service URL" and "Entitlement URI" for the CO that needs access to that SP and specify 'Zone Provisioner' as provisioning target).

- For COmanage, as mentioned in End user documentation SCZ COmanage, a description is available of how to Make services available to users . Without this configuration, a service will receive no attributes about a user at all.

Some points of attention

- Attributes are not passed from the IdP of the user to the SP: the attributes received from the IdP are (partly) used for SCZ. SCZ will look up your account info in the MMS (COmanage) and use the attributes found internally to pass to the SP. So: while you might see attributes from the IdP, in case the configuration in SCZ/MMS isn't right, you might not receive attributes at the SP
- Before you receive attributes, at least the following needs to be catered for:
    - the SP needs to be connected to the SCZ
    - the IdP of the user needs to be connected to the SCZ
        - for Dutch IdP's, that means the SURFconext contactperson of the institution needs to connect their IdP to SCZ in the SURFconext dashboard
        - for eduGAIN:
            - you can lookup whether the IdP is published in eduGAIN (needs to be so)
            - the IdP needs to release R&S-attributes (check here)
    - in SCZ a CO needs to be created and a CO-admin needs to be enrolled
    - in SCZ a zone provisioner needs to be defined for your CO and SP
    - you will only receive attributes from identities that are member of your CO
    - the login proxy gets its data from a 'connection database' in which the CO attributes are provisioned. De relevant database table is updated whenever a new member is added to the CO while the ZoneProvisioner of the CO is set to "automatic". To provision all attributes to existing members, that existed before the ZoneProvisioner was configured, the "reprovision all" button needs to be clicked
    - you need to set up groups within your CO, maybe COU's, and define an enrolment for your CO, so people can register.
        - for COmanage, please consult the COmanage documentation
- See the underlying pages for specific cases, like for example with OIDC, you need to specifically request attributes

Questions?

When you can't find what you're looking for, please let us know via raoul.teeuwen@surfnet.nl .

Underlying pages

- Connecting a web service to the SCZ environment via SAML
- Connecting to the ldap
- PAM Module
- Supplied attributes
- Sample user consent texts/AUPs/code of conduct
- Connecting a service to the SCZ using OIDC
- SSH PublicKeys in LDAP
- Connect eduGAIN IdP's