Science Collaboration Zone Home

Research is more and more about collaboration, also confirmed in the Dutch NWO 2019-2022-strategy. Researchers that want to collaborate (internationally) and providers of resources who want to offer research facilities to collaborative organisations therefor face the question: how to provide secure access to resources. The SCZ project (SCZ, FIAM for collaborating researchers) tries to solve a number of issues in the field of authentication, authorization and policies. On these pages we describe what the SCZ project is about.

Simplified: we provide an Authentication & Authorisation Infrastructure-as-a-Service focused on the needs of researchers, research projects and providers of resources for researchers. It takes care of user management.

In the European AARC-project (Authentication and Authorisation for Research and Collaboration) the specific identity and access challenges researchers face are addressed, and they made a clear video about the problem:

AARC crafted a blueprint architecture that addresses those challenges. SCZ is basically doing an implementation of that blueprint.

Why the SCZ project?

Researchers have typical access needs that aren't taken care of by the current solutions, and they have documented them in FIM4R-documents (Federated Identity Management for Research). We address a number of those problems in the SCZ-project:

- Providing access to invited people to the actual resources currently often takes a relatively long time (working with system admins of all resources, setting up 'account management', provisioning etc).
- You want to streamline the invitation process (**invites**, enrollment). When the collaboration grows, there is a need to manage collaboration **groups** (membership etc).
- Researchers often want access to '**non-web**' services (think of resources accessed via **SSH** or WebDAV): those are currently not tied to their institutional accounts, which makes access revocation a problem.
- Research is often **international** and providing people without an institutional account (eg from companies involved in the research project, '**guest-access**') secure access often is a problem.
- **Authorization** often is a problem. Group membership can be used to decide on authorization: what is a user allowed to do within a certain service? This requires a solution that can convert the group information into **attributes** that are subsequently consumed and interpreted by the resources to be shared (eg wikis, compute or data) for authorising users.

Currently, for every new research the wheel is reinvented to arrange for the things mentioned. Collaborations and research are delayed in the start-up phase because providing access takes time. What if there was a plug and play service?

How does SCZ provide a solution?

With the SCZ project, we:

- ensure that parties who want to share resources can do so by connecting the resource to the SCZ proxy (only once). The SCZ solution takes care, amongst others, of making the service available via **eduGAIN**.
- provide an environment where institutions and collaborative organisations can **quickly request a collaboration group, assign group managers and then manage that group themselves, invite people, etc**.
- provide a possibility to **manage specific attributes** per collaborative organisation.
- ensure that **people without an edu account** can also easily be invited and access the resources, where possible with a higher 'Level of Assurance' than with a social identity.
- ensure that **non-web resources like SSH and WebDav** can be approached via federated authentication (eg institutional account) (for the benefits of federated authentication see "Why federative"?).

- ensure that an institution only has to join the SCZ once in order to give all its researchers (via one or more collaborations) access to the participating services and resources.

To get an extra idea of what SCZ wants to offer, here we share the 'user stories' (in broad outline) for which we want to offer a solution with SCZ.

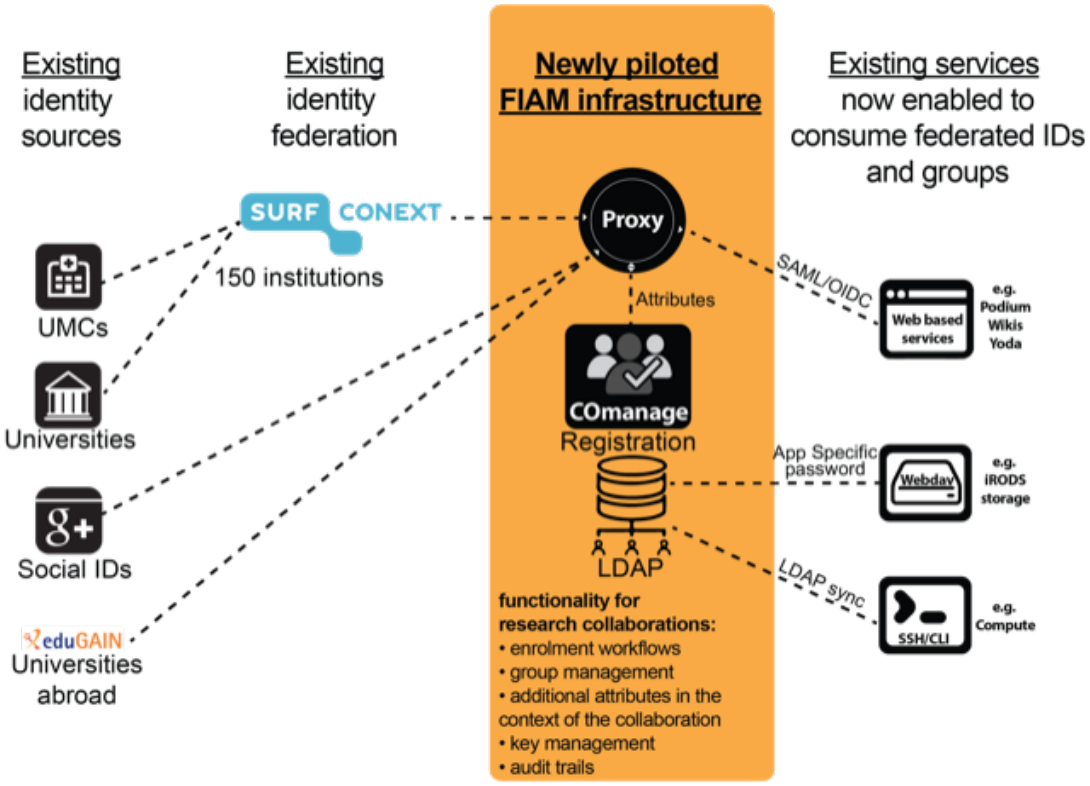
SCZ and Open Access / Open data

Open Access and access regulation mechanisms often go together. Possible scenario's:

- The research team has every intention to publish lots of data and results at some point, but at the start or during the research, access has to be limited. SCZ can provide for this.
- Certain data is available for open access, but for all kinds of reasons, certain other data is only available for authorised users (see for instance page 75, 13.2 and 13.4, in 'RDM Toolkit'. SCZ can provide for that as well.

Schematic overview of the SCZ solution

Schematically the SCZ can be drawn as follows:



The picture above shows that the research services are linked to the SCZ proxy: these services only have to make and maintain one link. The picture shows the features of the SCZ infrastructure:

- Connects with eduGAIN so that research services are accessible for researchers at institutions outside the Netherlands.
- Provides a mechanism (via COmanage) to invite users and manage groups and attributes (a so called 'Membership Management Service').
- Provides a solution for people without an edu account to use services (such as via Google and / or other social accounts).
- Link with SURFconext so that researchers at Dutch institutions can make use of the research services via SURFconext and the SCZ proxy.
- Provides a solution to securely unlock non-web services.

Video and demo you can try yourself

Wondering how a flow of inviting a user to access via SSH looks like? See the below video, but know this is just to get an idea as the environment is developing continuously (if the video doesn't start playing, try opening it full-screen via the icon in the top right corner. The cow-

sound at the start of the video is related to the name of the company involved in work on COmanage, Spherical Cow Group of which the name is based on the usage of spherical cow, a humorous metaphor for highly simplified scientific models of complex real life phenomena):

Another way of logging in is shown in a video at the bottom of PAM Module. We've made a connection to Azure AD VM's which we show in this video.

You can also try **a demo** yourself.

How SCZ aligns with GDPR/privacy

Many federated academic services require a few user attributes to successfully complete login, usually name, email, and a persistent user identifier (called the “R&S attribute bundle”). An international program called the Research & Scholarship Entity Category (R&S) was established to meet this need. This program enables federated services serving a research or scholarly purpose to request that their national R&E federation (as InCommon is for the US) “tag” them with the R&S entity category. It also specifies how R&E federation operators vet such requests to ensure that such tags are only applied to appropriate services.

The R&S program further provides a means by which an academic IdP can automatically release the R&S attribute bundle when users login to services that have been tagged R&S, and a corresponding R&S tag to be given to an IdP to signal that it participates in this global program. This is important because some R&S tagged services will only permit a login to proceed if the user’s IdP is also tagged R&S.

It’s worth noting that releasing R&S attributes under the R&S program contributes to good privacy practice under the European General Data Protection Regulation (GDPR). REFEDS, the international organization of Research and Education Federations, conducted a thorough analysis of how attribute release under the R&S Category addresses GDPR requirements to arrive at this conclusion.

SCZ only connects services in the R&S category. So IdP's can connect to our proxy, knowing they are compliant to the GDPR in regards to authentication (for processing personally identifiable information (PII) in services connected to our hub, the involved institutions might need extra contractual agreements, which normally are taken care of in the startup phase of research project).

Involved collaborations and institutions

We have a https://wiki.surfnet.nl/display/SCZ/Pilot+partners listing (a part of) the institutions piloting within our project and what is being piloted.

The institutions involved in pilots are expected to participate in meetings and allow the right people within the institution to test the pilot environment, provide feedback to SURF and participate in talks about new features and requirements.

Apart from pilots, we also frequently present about the project, like for the Health-RI event of Dec 8th 2017, where a poster was crafted to show the value of COmanage for collaborations like BBMRI. A generic version:

.

Which technical components are used?

Interested in the components used? See Technical overview of SCZ .

COmanage documentation

Curious about how you can get started in COmanage? We have organised and provide links to End user documentation SCZ COmanage .

Connecting services

Connecting Services to the SCZ environment describes how to services to the SCZ infrastructure. A list of connected services can be found at https://mdq.pilot.scz.lab.surf.nl/role/sp.html .

Why authenticate in a federated way?

Enabling a service / resource for federated authentication means users can 'login' (authenticate) with their institutional account: as soon as they want to access a service, they are automatically forwarded to the login screen of their institution (or other organisation where they have an account, if that can be used, such as a bank). Reasons to arrange this like this:

- It provides more reliability
    - As a service / resource you have certainty about the identity
    - If an employee leaves an organisation and may therefore no longer have access to a service / resource, federative authentication ensures that access is no longer possible.
- It ensures scalability
    - As a service / resource you have no / less work on creating an account, supporting users who forget their password etc
- It increases security
    - Users can use their (strong) settings institutional password and do not have 'another' account and password to manage
    - Users only have to enter their password on the institutional-login screen known to them (the fewer deviating screens ask for passwords, the less sensitive users are for phishing)
- It ensures user-friendliness
    - Users don't need to manage extra user accounts and passwords, they can re-use the already known institutional account

The European AARC-project has a training-module on what a identity federation is and what its advantages are: 1. AAI Overview.pdf. More information can be found at these websites: Federation-101 and Training for service providers. See also the advantages for IdP's, SP's and users as listed for SURFconext.

Why institutions need to connect

The SCZ can work without institutions releasing attributes; the researcher can use social accounts etc to sign in to the SCZ. But the value for all parties increases when an institution connects its IdP to a service in the SURFconext dashboard; this makes it so the researcher can use the credentials of their home institution, which provides more certainty for the research group and resource providers.

In many Dutch institutions it takes a long time between the request from a researcher to be able to sign in to a research resource with their institutional account and the time sign in is enabled. Sometimes it never happens. Often, the researcher doesn't want to wait that long, and chooses a different solution to get access, which often turns out to be less secure, more costly etc in the long run.

The reason why it often takes that long, is that the employees tasked with connecting a service, want to make sure privacy is protected, IPR is taken care of, whether any financial flows need to be available, whether usage of the service will increase helpdesk calls etc.

Some institutions have decided researchers can carry part of the mentioned responsibility. They have started using a 'light' procedure for connecting research services:

- The University of Amsterdam (UvA) is using a SURFconext feature, Autorisatieregels, to control who can access research services. You can read more about how the UvA is doing this on this Dutch language blog.
- The University of Utrecht is one of those institutions. On https://www.surf.nl/kennisbank/2018/best-practice-toegang-tot-nieuwe-diensten-hoeft-niet-altijd-lang-te-duren.html we've documented their way of working. Another

Will this be a SURF service?

SURF is conducting the pilots to also answer this question. In this way, after the pilots, we can draw conclusions about the functionalities: does the SCZ actually solve these problems? We also have a better idea of the feasibility to offer this centrally and if so including the costs (in equipment and people) that are needed to offer such a central infrastructure. In the summer of 2019 we will decide on this based on the experiences with the pilots. Naturally, the pilot partners have considerable influence on this process. Should it be decided not to offer the SCZ as a service, we will enter into a phase-out process with each pilot partner, for example SURF can help transfer the infrastructure to a local copy an institution can run locally.

As we're always looking for an efficient way to deliver services, we keep a close eye on international developments. Due to our international relations and activities, we know GÉANT is gearing up a new service, eduTEAMS. Both our teams have been sharing a lot of knowledge, and there are a lot of similarities. We will investigate whether and how we can use eduTEAMS. A nice feature is eduTEAMS also offers Hexaa and Per un as alternative Membership Management Services to COmanage (GÉANT has a comparison of the 3 systems).

Mailinglist

We have a mailing list for this project. Feel free to sign up for that list via https://list.surfnet.nl/mailman/listinfo/projectscz-fiam . An archive of previo usly shared messages can be found via https://list.surfnet.nl/mailman/private/projectscz-fiam . Interested? Questions? Suggestions? Mail with Raoul Teeuwen (raoul.teeuwen@surfnet.nl).

If you find the SURFnet SCZ mailinglist interesting, you might also be interested in the following:

> "*Following some community interest, a new (not COmanage specific) list has been established: cmp-discuss. This is a discussion group for any technologies, policies, or use cases associated with collaboration management platforms, and especially general (non-product specific) topics or topics crossing multiple technologies.*
>
> *You can join and manage your subscription here: https://groups.google.com/forum/#!aboutgroup/cmp-discuss*
>
> *(The list was set up as a Google Group to avoid associations with any particular project or community.)*"

Planning / timeline / status

In June 2017 phase 1 of the project was completed, and phase 2 started. In phase 1, use cases were drawn up and coordinated with a number of cooperative organisations, an architecture was drawn up and needs were assessed. Phase 2, which runs from until the 2nd quarter of 2010, is dedicated to realising the various components and gaining experience through pilots.

SCZ phase 2 focuses on:

- Building a largest-commoner service for use cases and pilots.
- Building the SCZ technical infrastructure
- Drafting the SCZ policy.
- Testing the SCZ technical infrastructure and policy on the described use cases.
- Acquiring experience with the SCZ through pilot projects with institutions
- Drafting a business case.

Schedule

- ~~Aug / Sep 2017 - Establish pilot environment~~
- ~~Oct / Nov 2017 - Connecting backend systems~~
- ~~Oct / Nov 2017 - Set up and test deployment flows~~
- ~~Oct-Dec 2017 - Set up and fine-tune access for external people / guests / etc~~
- Dec 2017 - Jun 2019 - Pilot with the pilot environment:
    - Access for "ordinary" (pilot) users
    - Finetuning flows
    - Connect more services
    - Develop the platform
- Jun 2019 - go / no go SCZ phase 3 (service development or realised controlled phasing out)
- Until the end of 2019 - Regardless of the decision (go or no go) pilot partners will be supported until the end of 2019.

More information

- SCZ Public Space
    - Pilot partners
    - Technical overview of SCZ
    - Userflow
    - End user documentation SCZ COmanage
        - COmanage Configuration Options
        - Configuring COmanage Enrollment Flows
        - Example invite flows
            - Example invite flow configuration
            - Example self signup configuration
            - PI distributes link for users to self-enroll
            - Example User enroll with non-edu account-flow
    - Connecting services to the SCZ-environment
        - Connecting a web service to the SCZ environment via SAML