skolfederation.se
info@skolfederation.se

Trust and usability with Skolfederation

skolfederation.se
info@skolfederation.se

Skolfederation – for easy and safe access to services

Teaching in Swedish schools is moving into the digital world. In order to better exploit the potential of digital services, there is need for a well-functioning login solution to be in place for students and staff. The login solution must preserve privacy but still be simple, secure, cost-effective, easily administered and possible to develop. With a well-functioning login solution in place for students and staff, more focus can be placed on teaching practice and on digital services that the school would like to use.

The purpose of Skolfederation is to:

Facilitate the Swedish education sector's use of digital services

Provide a common identity and access federation to make services easily accessible to students and techers in the country's schools

Protect user privacy while offering a secure service for members

Skolfederation has emerged from dialogue and collaboration in the education sector around the use of digital services in school. In 2011, work was pushed within the SIS (Swedish Standards Institute) project *IT-standarder för lärande* (IT standards for learning) to start Skolfederation. A model for, and background to the formation of an identity federation, is the identity federation Swamid within universities and higher education. Like other federative initiatives, Skolfederation aims to follow *Svensk e-legitimation* (Swedish E-identification). Skolfederation was developed under the guidance of SIS, and is now run by IIS (The Internet Foundation in Sweden).

Stakeholders
In 2012 stakeholders collaborated to create a service that corresponds to the needs of members. In 2013 members began connecting and the production of the service stabilised. Now, more than one hundred stakeholders are engaged in the work of Skolfederation, either as members or interested persons. Many of the service providers requested by principal organisers of the schools have already joined and many more are about to join. Service providers predict that in three years digital resources will be used as much as traditional teaching materials and a common login service is considered important or crucial for the use of digital services in teaching.

Collaboration and development
Collaboration helps to increase the understanding of the federation and facilitates the work of its members through the exchange of experiences, opportunities to see the service and use of demo schools, as well as highlighting various good examples.

Based on members' wishes, development is ongoing in order to handle higher security with an enhanced level of assurance between principal organisers of the school and online services. Development is also made to facilitate the administration of the members' metadata.

Background in the SIS project – IT standards for learning

Skolfederation emerged as the result of a larger project, IT standards for learning, powered by SIS (Swedish Standards Institute) in SIS TK 450. The purpose was to make it easier for schools to use digital services and content by using common standards.

Common open standards
The SIS project does not seek to create any new standards because there are already appropriate ones in use. Instead, the goal is to create common guidelines, and practices on how they should be applied, as well as spreading knowledge and awareness of how to use them.

If providers and municipalities can work with solutions based on common and open standards, instead of creating custom solutions for the integration of content, conditions for the school's use of digital resources will be improved.

The SIS project set up a number of impact goals:
- The use of digital learning resources increases in school.
- An increased use of digital resources should provide the students with opportunities to improve their performance.
- Both municipal schools and independent schools use compiled guidelines for ordering digital resources.
- Service providers use the guidelines when producing digital learning resources and services.
- New suppliers are established and the market is expanding, both within and outside Sweden.

Skolfederation – the service

Skolfederation is a collaboration between principal organisers of the school and online service providers. The service is targeted at the principal organisers and those suppliers of digital services that can become members. Skolfederation is an identity federation whose members trust each other's user identification.

Skolfederation provides an infrastructure for login that facilitates access to digital resources, protects user privacy and provides a secure service for members. It is fundamental that the identification made by the principal organisers, which is used in school, can also be used for logging into the services of service providers.

Agreement and rules
To allow members to use and rely on each other's identities and credentials, all members need to follow the regulations of Skolfederation.

The federation operator (IIS, The Internet Foundation in Sweden) manages the operating activities in Skolfederation, such as membership management, metadata management, operation and development of the common infrastructure, management of contracts and legal frameframework and information to members.

Additional service for access to wireless networks
A partnership between Skolfederation and Sunet gives students and teachers in Swedish schools access to Wi-Fi in about 7,000 locations via eduroam. That includes more than 500 locations in Sweden. The Wi-Fi is available at universities, but also in public places such as train stations, restaurants and cafes. eduroam has previously only been available to universities and colleges, but is now also available for primary and secondary schools as part of Skolfederation.

Interconnection agreements
eduroam (education roaming), which is available in 54 countries, is a collaboration in the research and education community to take advantage of each other's Wi-Fi. Skolfederation and Sunet, that is responsible for the Swedish connection to eduroam, have a roaming agreement that allows for the principal organisers of schools that are members of Skolfederation to also become members in the global eduroam collaboration.

Members of Skolfederation

The service is aimed at principal organisers of school and service providers in the education sector. The specific conditions of the education sector, such as regulatory requirements, market needs, market trends and the different stakeholders involved, set the framework for the service.

The following stakeholders can be members of Skolfederation:

- A principal organiser of the school for any of the types of schools listed in *Skollagen 2010:800* (Swedish Education Act), that provides education, under public or private administration. It is acceptable to have separate agreements for different school units.
- A Swedish government agency that works in a field concerning school.
- A provider of digital services who has been recommended by a principal organiser of a school.

Learning material and administration
The principal organisers of the school are Sweden's municipalities and *friskolor*, independent schools that receive public funding but are independent of the municipal local school authority. Service providers include providers of educational software, various media, learning management systems and administrative services such as schedule, student records, planning, monitoring; text, speech, image and video processing services, publishing and storage.

Other stakeholders involved that will need to provide support for the use of Skolfederation are suppliers to the principal organisers and service providers, such as product providers, system integrators and consultants.

Federation directory
To become a member, a stakeholder can begin with an expression of interest. Then they make a membership application by signing an agreement and make a metadata registration where the member leaves metadata checked and uploaded in the federation directory. There are two different member agreements, one for principal organisers and one for service providers. They consist of a membership agreement with attachments for technical requirements, safety, attributes, prices and glossary. To promote the use, the service has a simple and predictable pricing structure, with a fixed volume dependence annual membership fee.

Benefits for members

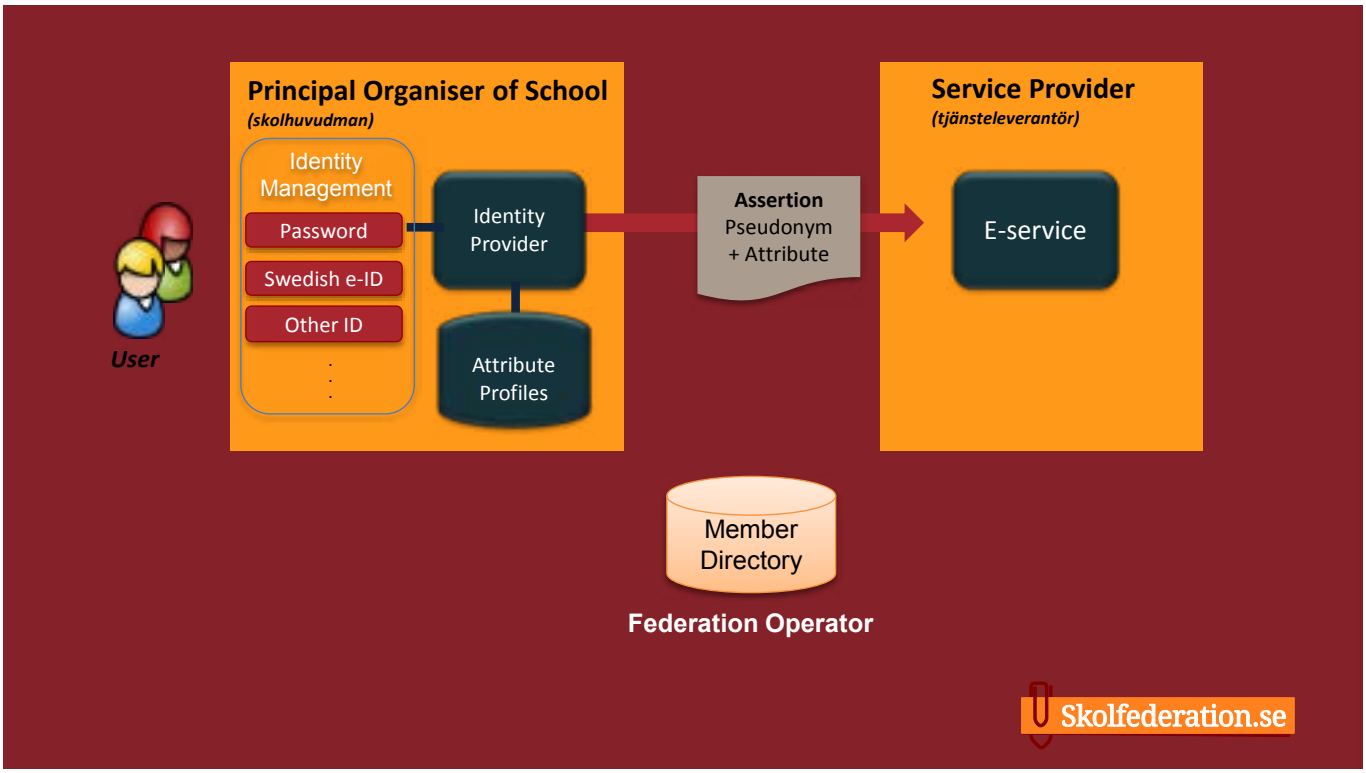
A single login to the school for access to both internal and external services reduces time-consuming administration of accounts and passwords to numerous services. Schools can feel more confident in giving access to different services when the use of sensitive data can be limited and only the information necessary for access to the service needs to be provided.

Reduced need for integration makes it easier to connect more services for use in schools. Once a school is connected to Skolfederation, no further technical integration is needed for additional service providers (who also are affiliated with Skolfederation).

Standardised interface
Login methods may change without affecting connected services. Skolfederation provides a standardised interface for exchanging information between principal organisers and service providers. The regular login to the school takes place in the first step, before releasing information to the service provider. In this way, methods for login can change without interfaces to service providers being affected.

Reduces integration costs
Those that offer web based services to schools, get access to a secure, standardised login service that all connected schools can use with Skolfederation. Supplier's integration costs can be lowered when they only need to adapt their systems once to work in the federation. Thus, they do not have to administer their own user directory. Service providers can therefore easily make their services accessible to schools, teachers and students, which facilitate access to more services, emergence of new services and combinations of content.

Federation structure



Skolfederation is an identity federation which means that an association of organisations have agreed to trust each other's electronic identities in their respective IT systems.

Principal organiser of school – *skolhuvudman*
The basic concept of an identity federation is that the authorisation of users should be as close to the source as possible, preferably when the student or teacher log into the school's internal network.

Once a member, the principal organiser becomes an identity provider in Skolfederation. When a user is authenticated by logging into the school's internal IT system, an electronic identity assertion confirms that the user is known and accepted by the school. The identity assertion can have attributes of different types added, such as name or in which school the student is registered.

Personal details
The identity assertion does not need to contain any personal details. It is sent to the service that the user wants to log in to, without additional login. For many schools it is easy to join Skolfederation. They already have the technical environment needed and only need to activate the function.

Service provider
An online service provider who becomes a member will only need to integrate its login system once with the identity federation. It still needs to sign agreements with each school for access to services. Through Skolfederation, service providers get access to a secure, standardised login service that all connected schools can use.

Impartial authentication – federation operator
Skolfederation also has a federation operator who approves and documents all members, coordinates their use and conformation to standards and provides essential services to them. It is IIS (The Internet Foundation in Sweden) that has this role. The most important function of the federation operator is to manage a directory of all members through which the identity assertions are verified in an impartial and secure way.

Trust
The trust in the identities and attributes used within Skolfederation is of great importance. If a party neglects its handling it can lead to confidence deteriorating in all members' identities and attributes. In order to ensure a high level of trust in the identities and attributes within Skolfederation all members must follow the safety precautions specified in the membership agreement.

The importance of privacy

Being able to identify a person is an important feature but it is also important to take into account personal privacy. Therefore, only the necessary information is sent to online service providers affiliated to Skolfederation.

A fundamental requirement of Skolfederation is that all parties comply with *Personuppgiftslagen 1998:204* (Swedish Personal Data Protection Act). It is the responsibility of the member of Skolfederation to ensure that the requirements stipulated in *personuppgiftslagen* are met and followed.

Members shall only process personal data necessary for the service.

Pseudonyms for added privacy

Skolfederation upholds and promotes privacy and we strive after identifying the users with "pseudonyms" instead of a *personnummer* (Swedish national identity number). This ensures that the real identity of the user is not normally visible to the online service provider but that the real identity can be traced, if needed, for example in cases of abuse.

New pseudonyms

There are two types of pseudonyms – persistent (resistant) and transient (temporary).

- With persistent pseudonyms, a user is assigned to one and the same pseudonym for an online service, but different pseudonyms are used for different online services.
- With transient pseudonyms a user is never given the same pseudonym. Instead the user gets a new pseudonym for each new occasion they use an online service.

Attributes

The basis of an identity system is determining if a person really is who he or she claims to be. But when it comes to providing access to digital learning material it is, for reasons of privacy, an advantage if authorisation is based on attributes such as school, grade and so on, rather than on the user's *personnummer*.

Because Skolfederation upholds and promotes privacy, the goal is that the user should only have to share the information which is necessary in any given situation.

Should a user, for example, book a ticket with student discount on a website, then the company that sells the ticket does not need to know your *personnummer*. It should suffice that you log in to Skolfederation and your school certifies that you are a student without sending your *personnummer*.

Local maintenance

The responsibility for maintaining these user data (attributes) is with each principal organiser. They are expected to update when students change school or when staff quit or get new work tasks. The attributes are therefore expected to be retrieved from the primary source of the municipal school or independent school which may be a directory (AD, eDirectory) or a database.

Attributes of Skolfederation

One of Skolfederation's objectives is to minimise the exposure of personal information. In the agreement between the school principal organisation and the service provider it is decided which attributes are made available to the service provider. It is the school principal organisation who is responsible for what is made available and to whom. It is important to point out that not all services are entitled to all attributes but a minimalist principle applies.

Technology

The technical infrastructure of Skolfederation has been built to the same standards that are already used for the Swedish federation for higher education SWAMID (Swedish Academic Identity). Skolfederation is similar to other federative initiatives' (such as *Svensk e-legitimation* – Swedish E-identification) aim to use the following SAMLv2 profiles:

- Implementations profile eGov2 (describing required SAML abilities)
- Deployment profile saml2int (describing how SAML abilities should be used)

Stakeholder requirements

Service provider (SP) ***tjänsteleverantör***, Skolfederation's service providers should have the ability to process identity assertions.

Identity provider (IdP) ***huvudman***, Skolfederation's principal organisers should have the ability to identify and authenticate users, for example students, and as a result be able to provide an identity assertion.

Federation operator, the federation operator should provide digitally signed aggregated SAML metadata which can be considered the core of Skolfederation – the essential trust.

General technical infrastructure

SAML metadata (MD, metadata)
In order for the members of Skolfederation to be able to trust each other's identity assertions, an exchange of the public keys in each stakeholder's key pair is needed to verify the signature of the identity assertion. Exchange is done by aggregating the local SAML metadata, which describes a stakeholder's attributes, abilities and public keys, to the federation operator who digitally signs and publishes the aggregated SAML metadata, which thus contains all of the stakeholder's attributes, abilities and public keys.

In saml2int it is described how SAML metadata shall be presented. The format of the SAML metadata is regulated in OASIS SAML V2.0 metadata specification [SAML2Meta] and the handling of SAML metadata is regulated in OASIS Metadata Interoperability Profile [MetaIOP]. All joining stakeholders in Skolfederation shall support these.

Validation of metadata
Before the stakeholder sends in metadata to the federation they can themselves validate it against Skolfederation. It can be done by uploading a file or entering the URL in the following location:
https://fed.skolfederation.se/validator/

Publication of metadata
Skolfederation's aggregated and signed metadata is published here: https://fed.skolfederation.se/prod/md/skolfederation-3_0.xml

The federation operator's public key to verify the metadata can be found here:
https://www.skolfederation.se/certifikat-for-metadata-skolfederation/

Each constituent stakeholder should verify the SAML metadata with signature towards at least one key source at each change.

Authentication request
If a user, such as a student who wishes to use a service, is unidentified, he or she becomes prompted to authenticate oneself. The request that the service creates in this scenario is an authorisation request which the user brings back to the identity provider (IdP).

Skolfederation has chosen to use saml2int as the deployment profile, which clearly describes how the SAML V2.0 Web Browser SSO Profile [SAML2Prof] should be used, which in turn reflects on the authentication request. The authentication response may be due to an authentication request, but it can also be an authentication response with no previous authentication request.

Pseudonyms
Skolfederation upholds and promotes privacy. Therefore, it is important that all joining parties can manage pseudonyms as subject of identification. The following two formats, which are part of SAML2Core5, should be supported:
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent urn:oasis:names:tc:SAML:2.0:nameid-format:transient

The property of persistent pseudonyms is that they always map a user to the same pseudonym for that service. That is, different services provide different pseudonyms.

Transient pseudonyms never use the same pseudonym for a user, but the user gets a new pseudonym for each occasion and for every service.

Discovery service (DS) *anvisningstjänst*

In the scenario where an unidentified user wants to use a service, he or she is being prompted to authenticate themselves. In a two-part relation, the service knows which identity provider (IdP) they should direct the user to. In a federation like Skolfederation, with over one hundred identity providers, a function is required to assign the user to "their" identity provider. This function is called discovery service (DS). It should be emphasized that a central discovery service is not a necessity but the service provider may choose to implement a function for local directing based on SAML metadata.

It should also be noted that there is opportunity for a scenario with unsolicited identity assertions (unsolicited response) where the user first connects to its identity provider (IdP) through a parameter in the call, which is then used to direct the user to the correct service (SP).

Handling of discovery service is regulated by the OASIS Identity Provider Discovery Service Protocol Profile [IdPDisco]. All joining members of Skolfederation shall support this.

Skolfederation's discovery service can be found here: https://fed.skolfederation.se/prod/ds/

Single logout

Skolfederation initially has no requirement that joining members should support single logout. Skolfederation does not, however, put up any infrastructural obstacles to the implementation of single logout.

Attribute service (AA, Attribute Authority)

Skolfederation's stakeholders have initially not identified any common attribute services (AA, Attribute Authority). Skolfederation does not, however, put up any infrastructural obstacles to the implementation of attribute service.

Collaboration – the development and opportunities

Skolfederation has evolved thanks to good cooperation between the principal organisers and service providers. Fundamental is the collaboration on Skolfederation as the common login service for the education sector so it corresponds to the needs of members and facilitates access to digital services in school.

Within the framework of Skolfederation there is also room for dialogue and exchange of experiences and needs regarding the development of the use of digital services in school, a development to which Skolfederation opens up possibilities. Skolfederation has a reference group that advises in policy issues relating to the service, which is open for all who may become members: the principal organisers, service providers and government agencies.

Basic condition

Skolfederation is a fundamental prerequisite for access to digital services in school. With a well-functioning login solution in place for students and staff, more focus can be placed on teaching practices and on the digital services that the school would like to use.