7 -practical work

Topic: Familiarization and analysis of the process of working with SSO protocols

Objective: To gain knowledge about the workings of protocols used in implementing a single sign-on (SSO) system.

Theoretical part

SSO relies on establishing a trust relationship between an application known as a service provider and an access management system, such as OneID. This trust relationship is often based on the exchange of a certificate between the access management system and the service provider. Such a certificate can be used to authenticate the identity information sent from the access management system to the service provider, so that the service provider can know that the information is from a trusted source. In SSO, account information is in the form of tokens that contain identification values for user information, such as email or username.

The authorization procedure usually looks like this:

1. The user logs in to the application or site they want to access, i.e. the service provider.
2. The service provider sends a token containing user information (such as an email address) to the SSO system (also known as an access control system) as part of a request to authenticate the user.
3. First, the access control system checks whether the user has been authenticated up to this point. If so, it grants the user access to the service application, going directly to step 5.
4. If the user is not logged in, they must do so by providing the account credentials required by the access control system. This can be simply a username and password, or other types of authentication, such as a one-time password (OTP).
5. After the access control system validates the account information, it returns a token to the service provider confirming successful authentication.
6. This token is passed to the service provider through the user's browser.
7. The token received by the service provider is verified against the trust relationship established between the service provider and the access control system during initial setup.
8. The user is granted access to the service provider.

Practical part

The process of allowing a user to log in to the system by an SSO service provider is illustrated in the figure below.

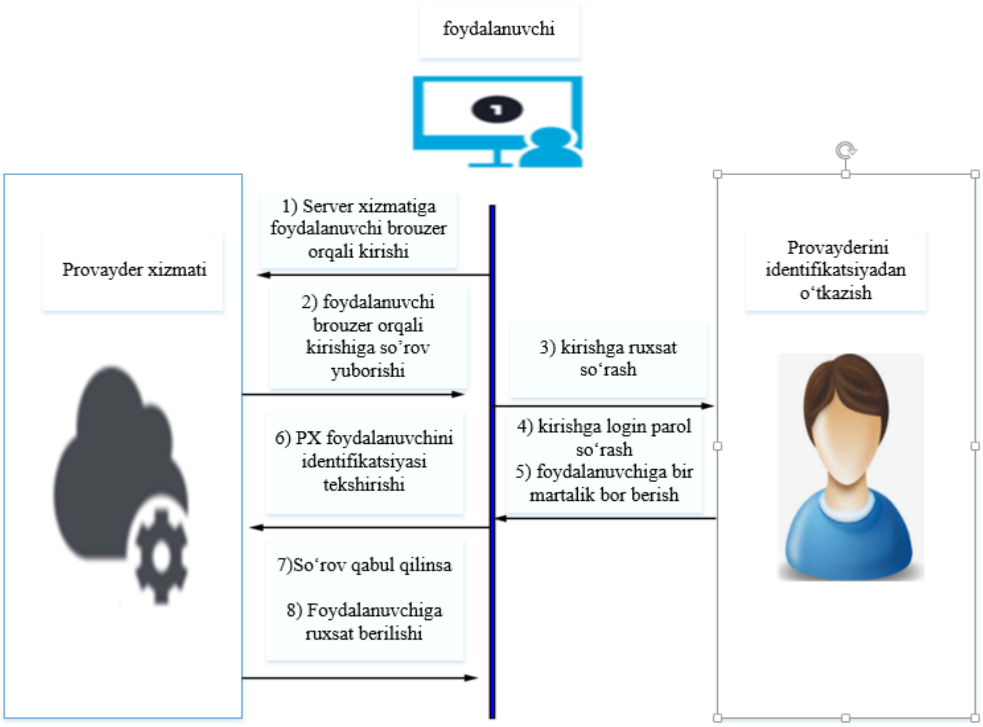
foydalanuvchi
Provayder xizmati
1) Server xizmatiga foydalanuvchi brouzer orqali kirishi
2) foydalanuvchi brouzer orqali kirishiga so’rov yuborishi
3) kirishga ruxsat so‘rash
Provayderini identifikatsiyadan o‘tkazish
4) kirishga login parol so‘rash
5) foydalanuvchiga bir martalik bor berish
6) PX foydalanuvchini identifikatsiyasi tekshirishi
7)So‘rov qabul qilinsa
8) Foydalanuvchiga ruxsat berilishi

Figure 8.1. User authentication

If a user tries to access another site, such a trust relationship must be configured according to the SSO method. In this case, the authentication process will also consist of the above steps.

A token is a piece of data or a set of data that is passed from one system to another during SSO. The data can be as simple as an email address and information about the system that sent the token. Tokens must be digitally signed so that the recipient can prove that they came from a trusted source. A digital signature certificate is provided during the initial setup phase.

There are several reasons to implement SSO. A single sign-on can simplify the login and password experience for both users and administrators. Users no longer have to remember all their account information, and they no longer have to remember just one more complex password. SSO allows users to access applications faster.

There are different types of SSO, which are as follows:

- Federated Identity Management (FIM);
- OAuth (OAuth 2.0 currently);
- OpenID Connect (OIDC);
- Security Access Markup Language (SAML);
- Single Sign On (SSO) .

In fact, SSO is part of a broader concept called Federated Identity Management , which is why SSO is sometimes referred to as Federated SSO. FIM simply refers to the trust relationship created between two or more domains or identity management systems. Single Sign-On (SSO) is a feature/feature available in the FIM architecture.

OAuth 2.0 is a specific software platform that is part of the FIM architecture and can be used to sign in. OAuth focuses on trust relationships by providing domains with user account information .

OpenID Connect (OIDC) is an authentication layer that is layered over the OAuth 2.0 framework to provide SSO functionality.

Security Access Markup Language (SAML) is an open standard that is also designed to provide SSO functionality.

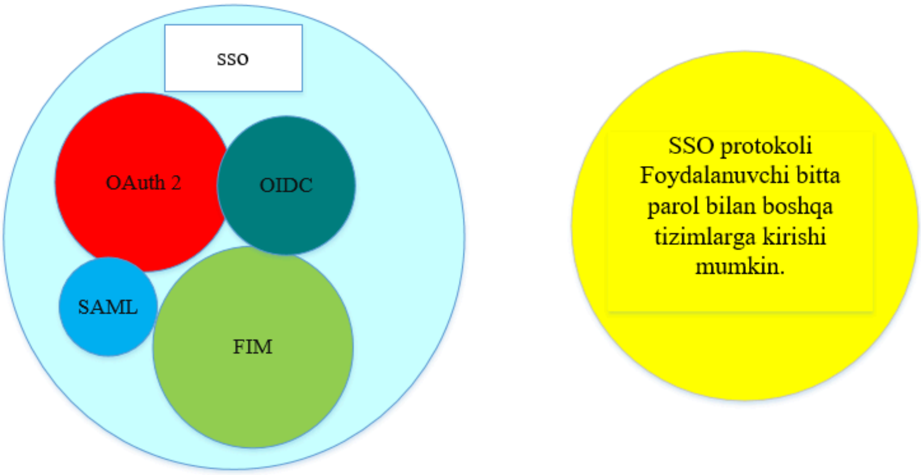
SSO
OAuth 2
OIDC
SAML
FIM
SSO protokoli Foydalanuvchi bitta parol bilan boshqa tizimlarga kirishi mumkin.

Figure 8.2. Types of SSO protocols

Single sign-on, often referred to as SSO, is not really a single sign-on because it does not imply a trust relationship between the parties being authenticated. It relies more on credentials that are replicated and transferred to other systems as needed. It is not as secure as any SSO solution.

SAML is an acronym used to describe the Security Assertion Language (SAML). Its primary role in online security is to allow access to multiple web applications using a single set of credentials. It works by transmitting authentication information in a specific format between two parties, typically an identity provider (idP) and a web application.

SAML is an open standard used for authentication. Based on the Extensible Markup Language (XML) format, web applications use SAML to transfer authentication information between two parties - an identity provider (IdP) and a service provider (XP).

SAML Benefits. SAML is becoming a popular enterprise solution for account authentication due to its many benefits. First, it improves the user experience because you only need to log in once to access multiple web applications. This not only speeds up the authentication process, but also means you only need to remember a single set of credentials for one account.

SAML works by exchanging user information, such as logins, authentication state, identifiers, and other relevant attributes, between an identity provider and a service provider. As a result, it simplifies and secures the authentication process because the user only needs to log in once with a single set of authentication credentials. So, when a user attempts to access a site, the identity provider passes the SAML authentication to the service provider, who then grants the user access. These processes are illustrated in Figure 8.3 below.

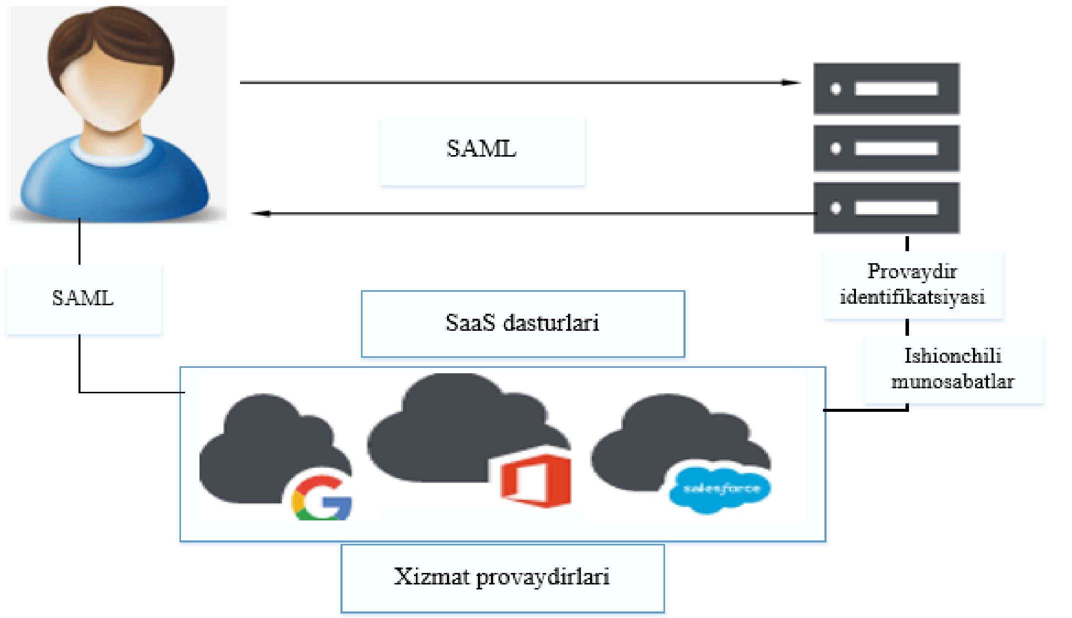

Figure 8.3. SAML working principle

SAML Single Sign-On is a mechanism that uses SAML to allow users to access multiple web applications after signing in to an identity provider. Because the user only needs to sign in once, SAML SSO provides a faster and more seamless user experience. The following figure shows a scenario for accessing web applications using SAML .

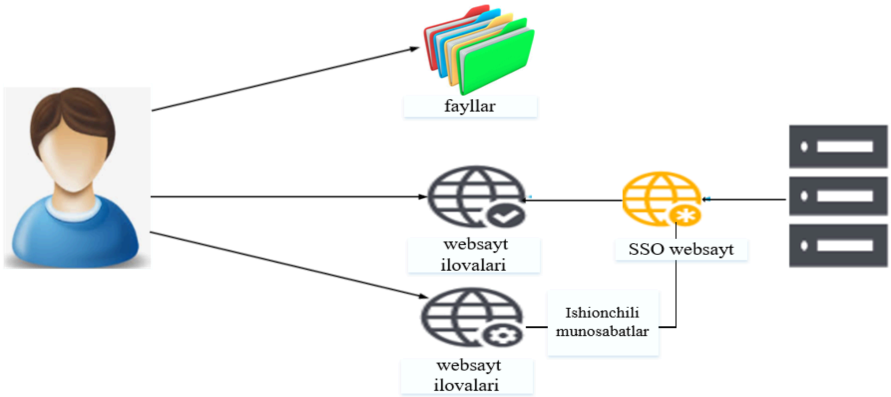

Figure 8.4. SAML protocol usage mechanisms

SAML SSO is easy to use and more secure from a user's perspective, as they only need to remember one user credential. It also provides a fast and seamless sign-in experience, as each application they access does not require them to enter a username and password. Instead, the user logs in to the identity provider and then logs in to the appropriate web application by clicking on its icon or navigating to the site via a URL.

OneLogin offers a set of SAML features that developers can use to enable SSO for their applications through an identity provider that offers SAML authentication. It also provides resources on how to add your application to the OneLogin catalog, how to code your application to provide SSO to users through OneLogin, as well as helpful best practices and frequently asked questions.

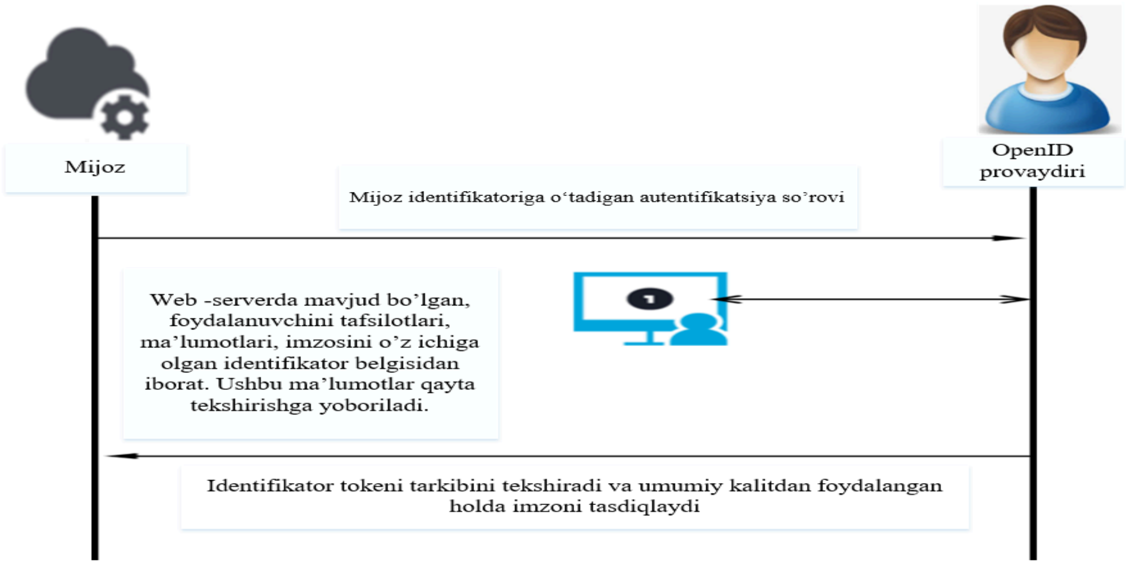
Mijoz
OpenID provaydiri
Mijoz identifikatoriga o'tadigan autentifikatsiya so'rovi
Web -serverda mavjud bo'lgan, foydalanuvchini tafsilotlari, ma'lumotlari, imzosini o'z ichiga olgan identifikator belgisidan iborat. Ushbu ma'lumotlar qayta tekshirishga yoboriladi.
1
Identifikator tokeni tarkibini tekshiradi va umumiy kalitdan foydalangan holda imzoni tasdiqlaydi

Figure 8.5. OISC protocol working mechanism

OIDC is simply a secure mechanism for an application to communicate with an identity service, retrieve user credentials, and securely return them to the application. The OIDC specification includes information about how the requested user credentials should be encoded and encrypted or signed, and how and when this is done.

Assignment

Analysis of systems that use different types of SSO such as FIM, OIDC, SMAL , Oauth .

Control questions

1. What is the function of the SSO protocol?
2. What types of SSO protocols are there?
3. Which systems currently use the SSO protocol?