SAML architecture

Introduction

SAML is the most complete, secure, and mature solution to get identity federation. SAML defines three main kinds of servers:

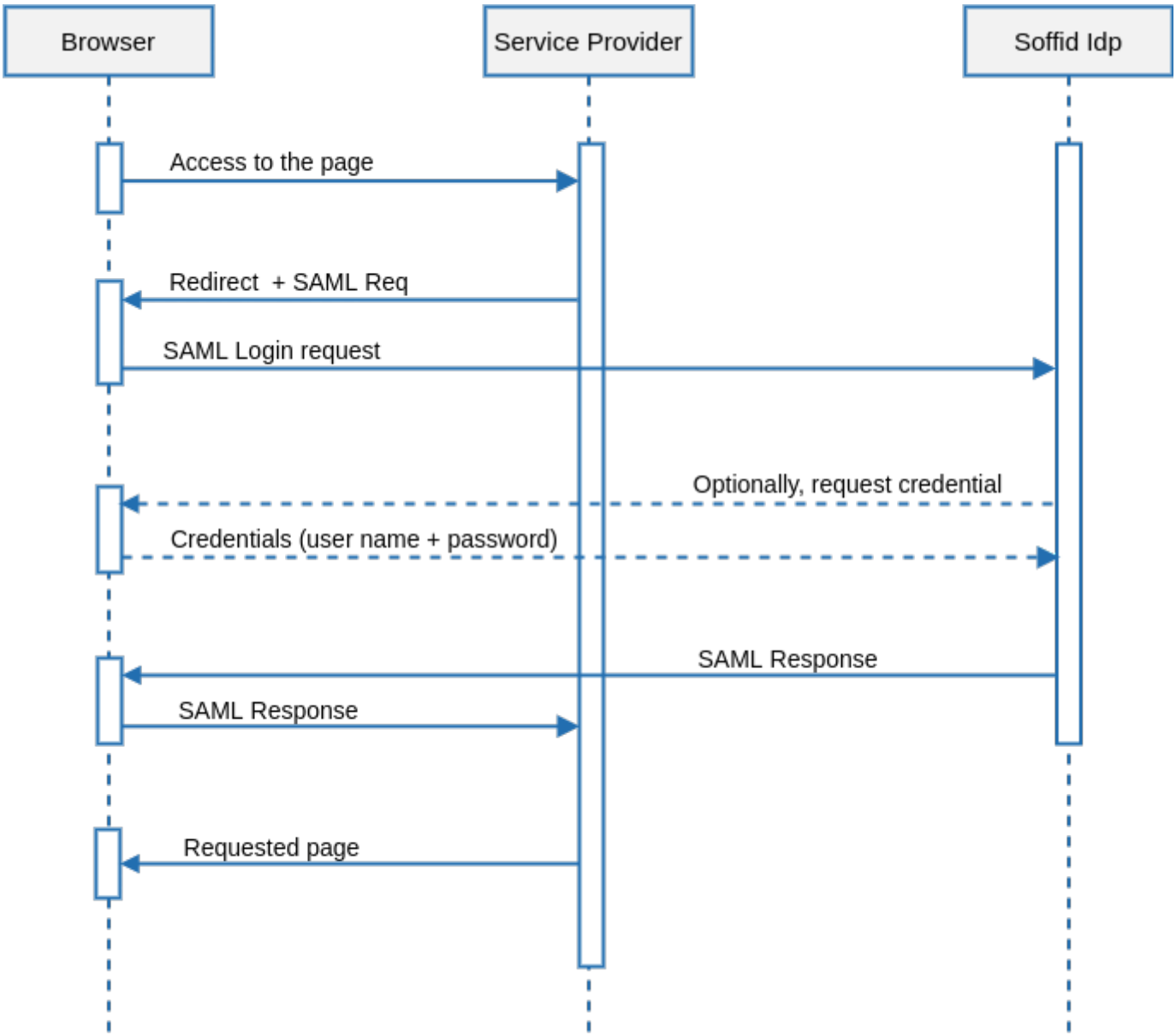
- Federation metadata server. Publishes information about the federation members, its protocols, and capabilities. Any federation member will only trust on other federation members.
- Identity providers are able to identify the user and publish its information to any application that requires it.
- Service providers are standard application servers that relay on identity providers to let users log in.

For now, we will focus on the **single log-in** and **single log-out** use cases, but be in mind that SAML defines much more use cases.

Communication is done through the browser

Single Log-in

The single log-in is usually initiated by the application server. The typical UML use case is as follows:



Description

1. The user's browser tries to get a web page from the service providers.

2. The service provider wants to authenticate the user identity. To get this, builds an AuthenticationRequest document. It is an XML document that includes the server name and time and date. This XML document is signed using its private key and optionally encrypted using the identity provider public key. Both keys are published by the federation metadata server.

3. The service provider generates an HTML page that automatically posts the AuthenticationRequest document to the identity provider.

4. The AuthenticationRequest is received by the identity provider. At this point, the identity provider verifies it is correct and safe.

Next, the identity providers checks if the user browser does have an active SSO session. In such a case, skip to step 6.

5. The identity providers ask for credentials to the user.

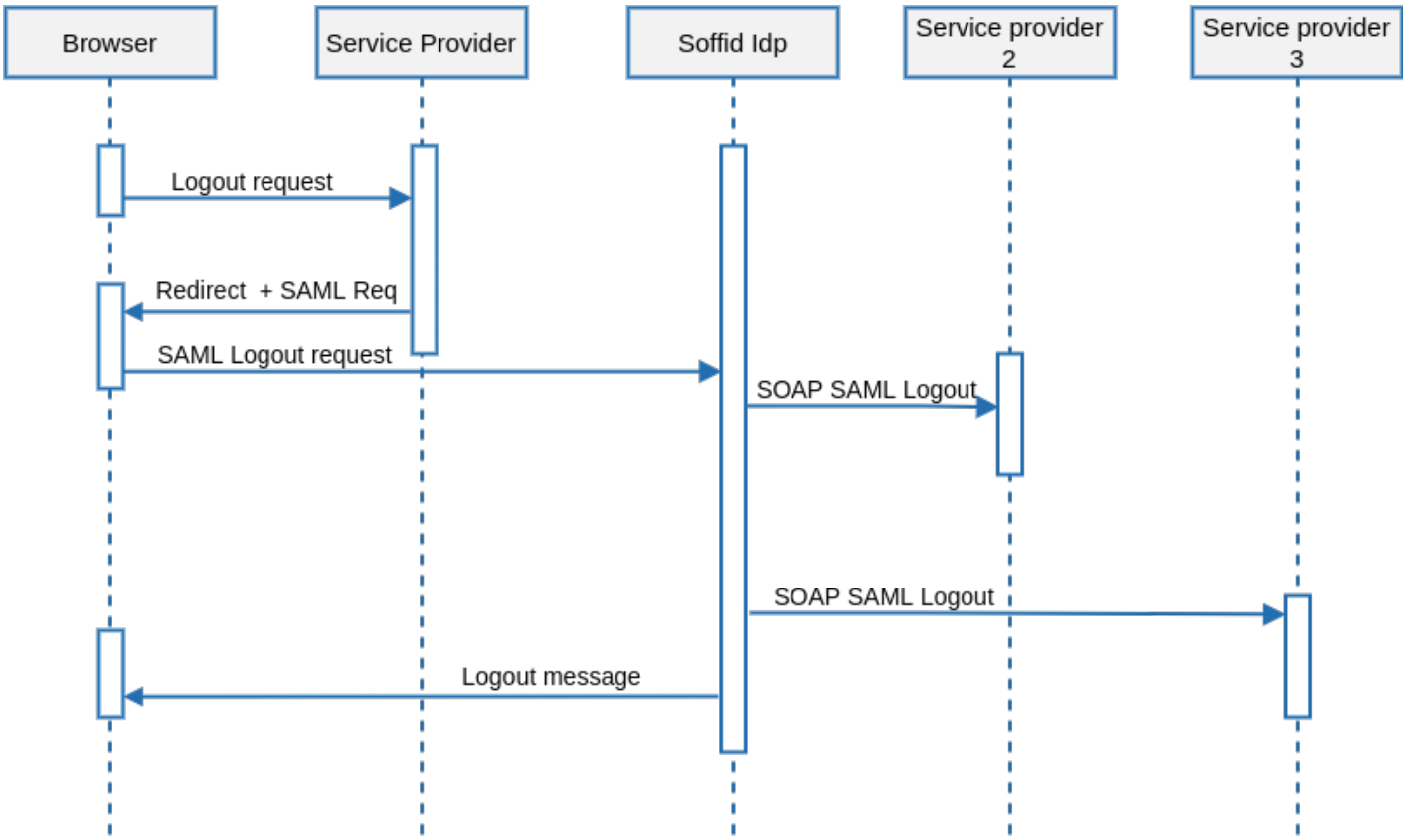
6. The user enters its credentials. At this time, the identity provider verifies the user name and password are correct, and creates a new SSO session.

7. The identity provider sends a SAML assertion to the service provider. This assertion is signed using its private key and optionally encrypted using the service provider public key. The SAML assertion contains some user attributes. The included attributes and its value can vary depending on the service provider that will receive it.
As previously seen in the authentication request, the assertion is always sent through the user's browser.

8. The service provider receives the SAML assertions, decrypts and verifies it, obtaining all the user attributes.

Single Log-out

The single log-out process follows the next UML diagram:



Description

1. The user requests to log out the application. At this point, the application (service provider) can give the user the chance to log out from any other application.

2. The service provider issues a global SAML logout request to the identity provider. The SAML logout request includes the user or session id. It is signed using its private key and optionally encrypted with the identity provider public key.

3. The identity provider sends a SOAP SAML logout request to any service provider with active sessions for this user. These logout requests are almost identical to the one sent from the service provider to the identity provider, but it is sent using SOAP rather than an HTTP URL.

4. After closing any active session, the user is informed about the logout progress, or optionally redirected to a farewell web page specified by the service provider.

The logout request must be signed, it is not mandatory to the login request.

Revision #19
Created 6 September 2021 09:56:25

Updated 4 November 2022 08:16:19