FREE eBook

# LEARNING saml-2.0

Free unaffiliated eBook created from
**Stack Overflow contributors.**

#saml-2.0

# Table of Contents

# About

You can share this PDF with anyone you feel could benefit from it, downloaded the latest version from: saml-2-0

It is an unofficial and free saml-2.0 ebook created for educational purposes. All the content is extracted from Stack Overflow Documentation, which is written by many hardworking individuals at Stack Overflow. It is neither affiliated with Stack Overflow nor official saml-2.0.



Use the content presented in this book at your own risk; it is not guaranteed to be correct nor accurate, please send your feedback and corrections to info@zzzprojects.com

# Chapter 1: Getting started with saml-2.0

## Remarks

SAML2.0 is an open standard used for transferring authentication and authorization data between Service Providers and Identity Providers.

The most common usage is web based SSO, where SAML is what enabled a user to login to an application with credentials from another system, without having the need to have the two systems directly connect to each other during authentication.

## Examples

### The SAML2.0 authentication flow

SAML specifies three key roles:

- **The Identity Provider (IdP)**

  The party which provides and maintains the identity of the users. This can be a directory service like ADFS or a custom database solution.

- **The Service Provider (SP)**

  The Service Provider is the actual *service* which the user tries to login to. This can be a website, an application or any service a user ought to be required to login to.

- **The principal / the user**

  The actual user initiating the request, or trying to access a resource from the *Service Provider* (SP).

The main SAML use case is *Web Based SSO*, where the SAML process is conducted by a set of redirects within the users' browser, where the user acts as the token carrier between the IdP and SP.

There are two flows for *Web Based SSO* using SAML:

- **Identity Provider (IdP) Initiated**

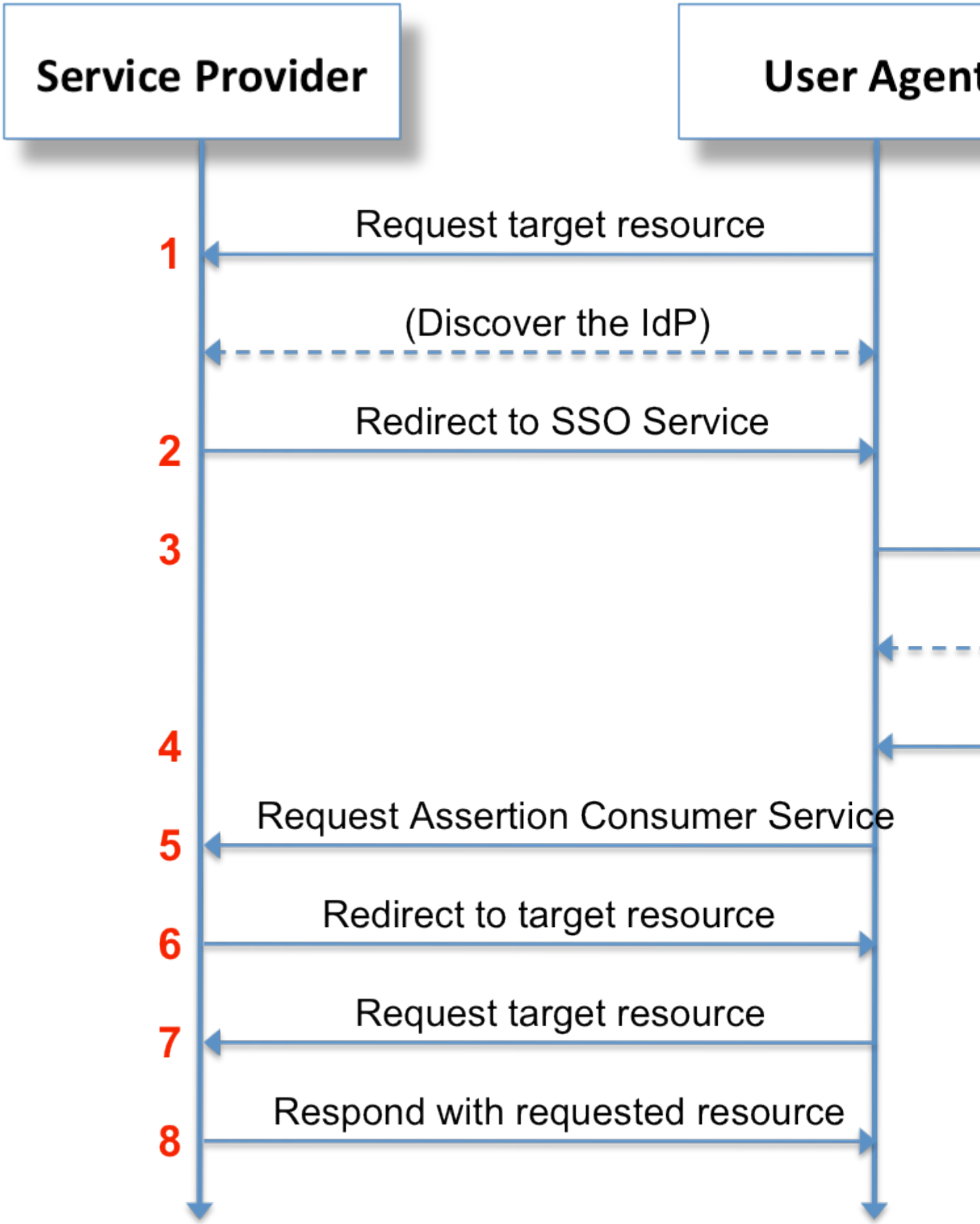
  The user logs into the IdP and is then forwarded to the SP of choice. E.g. a user logs into a corporate intranet and is presented with all available applications.

- **Service Provider (SP) Initiated**

  The user tries to login to an application, but is forwarded to the IdP to perform the actual authentication. E.g. a user tries to login to a remote SaaS application, but is forwarded to a

corporate IdP so the user can login with their corporate credentials into the remote application.

The SP initiated flow is visualized greatly by the workflow below:




Source: Wikipedia

1. A user tries to access a resource on a specific application or webpage
2. A user specifies (s)he tries to login using an external IdP. The SP will generate a SAML assertion, and will pass this along (usually through POST or GET variables) while forwarding you to the IdP
3. The user will authenticate itself against the IdP
4. The signed assertion and token are generated by the IdP
5. The signed assertion and token are forwarded back (again using POST or GET variables) to the SP and if successful a session is initiated on the SP
6. *and further* the user is able to request further resources from the SP while it has an active session with the SP (i.e. through cookies) so it does not have to authenticate with the IdP on every request.

## SAML Debugging tools

With all the requests and assertions going back and forth, it can be cumbersome to debug issues with your SAML claims and assertions.

As within SAML a core principle is not needing a direct connection between the IdP and the SP, the user's browser acts as a message carrier between the two. Because of this all communication - albeit encrypted - goes through your own browser.

Using various debug tools you can see the exact communication and requests being made, and forwarded between IdP and SP.

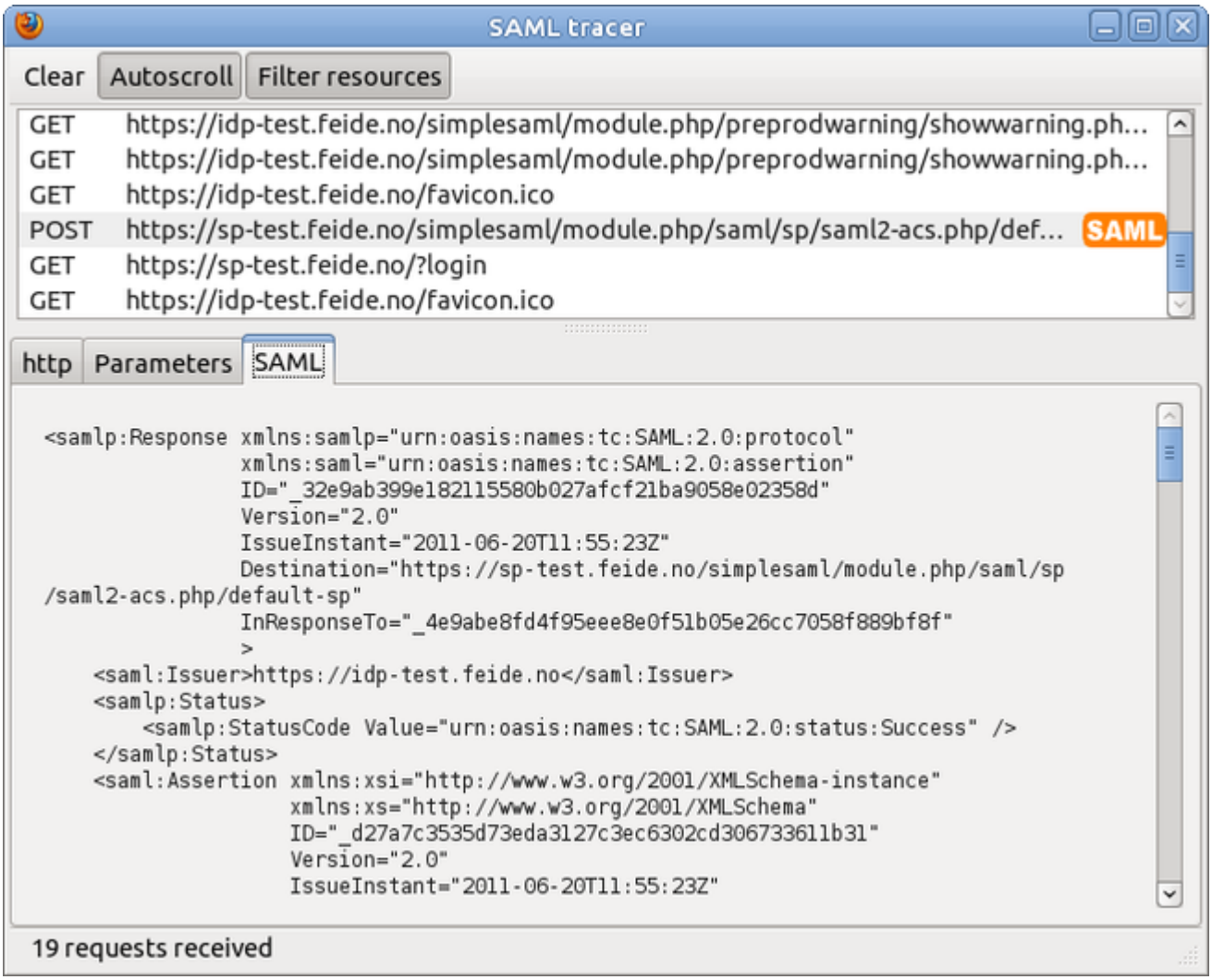
To get you started, here are a couple of tools for various browsers that should get you started:

**Chrome**

- SAML Chrome Panel
- SAML DevTools extension
- SAML Message Decoder

**Firefox**

- SAML Tracer
- SSO Tracer




*Using for example SAML Tracer you can see decoded SAML assertions and requests in real time while testing and debugging*

Read Getting started with saml-2.0 online: https://riptutorial.com/saml-2-0/topic/5634/getting-started-with-saml-2-0

# Credits

| S. No | Chapters | Contributors |
| --- | --- | --- |
| 1 | Getting started with saml-2.0 | Community, Rick |