EBook Gratis

APRENDIZAJE saml-2.0

Free unaffiliated eBook created from
Stack Overflow contributors.

#saml-2.0

Tabla de contenido

Acerca de 1

Capítulo 1: Empezando con saml-2.0 2

Observaciones 2

Examples 2

El flujo de autenticación SAML2.0 2

Herramientas de depuración SAML 5

Creditos 7

Acerca de

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

Capítulo 1: Empezando con saml-2.0

Observaciones

SAML2.0 es un estándar abierto utilizado para transferir datos de autenticación y autorización entre los proveedores de servicios y los proveedores de identidades.

El uso más común es el SSO basado en la web, donde SAML es lo que permitió al usuario iniciar sesión en una aplicación con credenciales de otro sistema, sin tener la necesidad de que los dos sistemas se conecten entre sí directamente durante la autenticación.

Examples

El flujo de autenticación SAML2.0

SAML especifica tres roles clave:

- **El proveedor de identidad (IdP)**

  La parte que proporciona y mantiene la identidad de los usuarios. Esto puede ser un servicio de directorio como ADFS o una solución de base de datos personalizada.

- **El Proveedor de Servicios (SP)**

  El proveedor de servicios es el *servicio* real en el que el usuario intenta iniciar sesión. Puede ser un sitio web, una aplicación o cualquier servicio al que se le deba solicitar a un usuario que inicie sesión.

- **El principal / el usuario**

  El usuario real que inicia la solicitud o intenta acceder a un recurso del *Proveedor de servicios* (SP).

El principal caso de uso de SAML es el *SSO basado en la Web* , donde el proceso SAML se realiza mediante un conjunto de redirecciones dentro del navegador de los usuarios, donde el usuario actúa como portador de token entre el IdP y el SP.

Hay dos flujos para el *SSO basado en la Web* usando SAML:

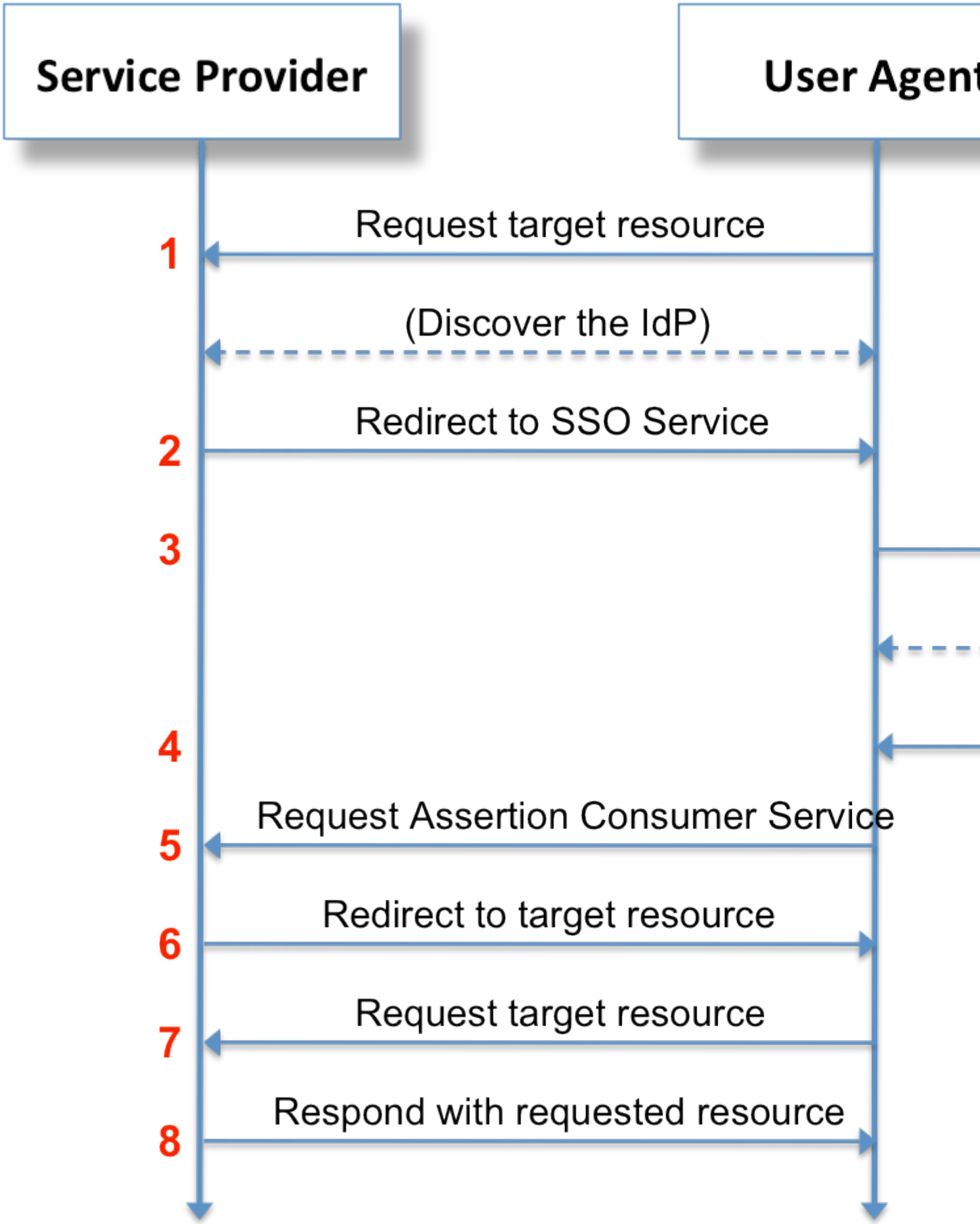
- **Proveedor de identidad (IdP) iniciado**

  El usuario inicia sesión en el IdP y luego se reenvía al SP de su elección. Por ejemplo, un usuario inicia sesión en una intranet corporativa y se presenta con todas las aplicaciones disponibles.

- **Proveedor de servicios (SP) iniciado**

El usuario intenta iniciar sesión en una aplicación, pero se reenvía al IdP para realizar la autenticación real. Por ejemplo, un usuario intenta iniciar sesión en una aplicación SaaS remota, pero se reenvía a un IdP corporativo para que el usuario pueda iniciar sesión con sus credenciales corporativas en la aplicación remota.

El flujo iniciado por SP se visualiza en gran medida mediante el siguiente flujo de trabajo:



Fuente: Wikipedia

1. Un usuario intenta acceder a un recurso en una aplicación o página web específica
2. Un usuario especifica que intenta iniciar sesión utilizando un IdP externo. El SP generará una aserción SAML y la pasará (generalmente a través de las variables POST o GET) mientras lo reenvía al IdP
3. El usuario se autenticará contra el IdP.
4. La aserción y el token firmados son generados por el IdP
5. La aserción firmada y el token se reenvían (nuevamente utilizando las variables POST o GET) al SP y, si tienen éxito, se inicia una sesión en el SP
6. *y además,* el usuario puede solicitar recursos adicionales del SP mientras tiene una sesión activa con el SP (es decir, a través de cookies) para que no tenga que autenticarse con el IdP en cada solicitud.

Herramientas de depuración SAML

Con todas las solicitudes y aseveraciones que van y vienen, puede ser complicado depurar los problemas con sus afirmaciones y afirmaciones de SAML.

Como dentro de SAML, un principio central no necesita una conexión directa entre el IdP y el SP, el navegador del usuario actúa como un mensajero entre los dos. Debido a esto, todas las comunicaciones, aunque encriptadas, pasan por su propio navegador.

Usando varias herramientas de depuración, puede ver la comunicación exacta y las solicitudes que se realizan y se reenvían entre IdP y SP.

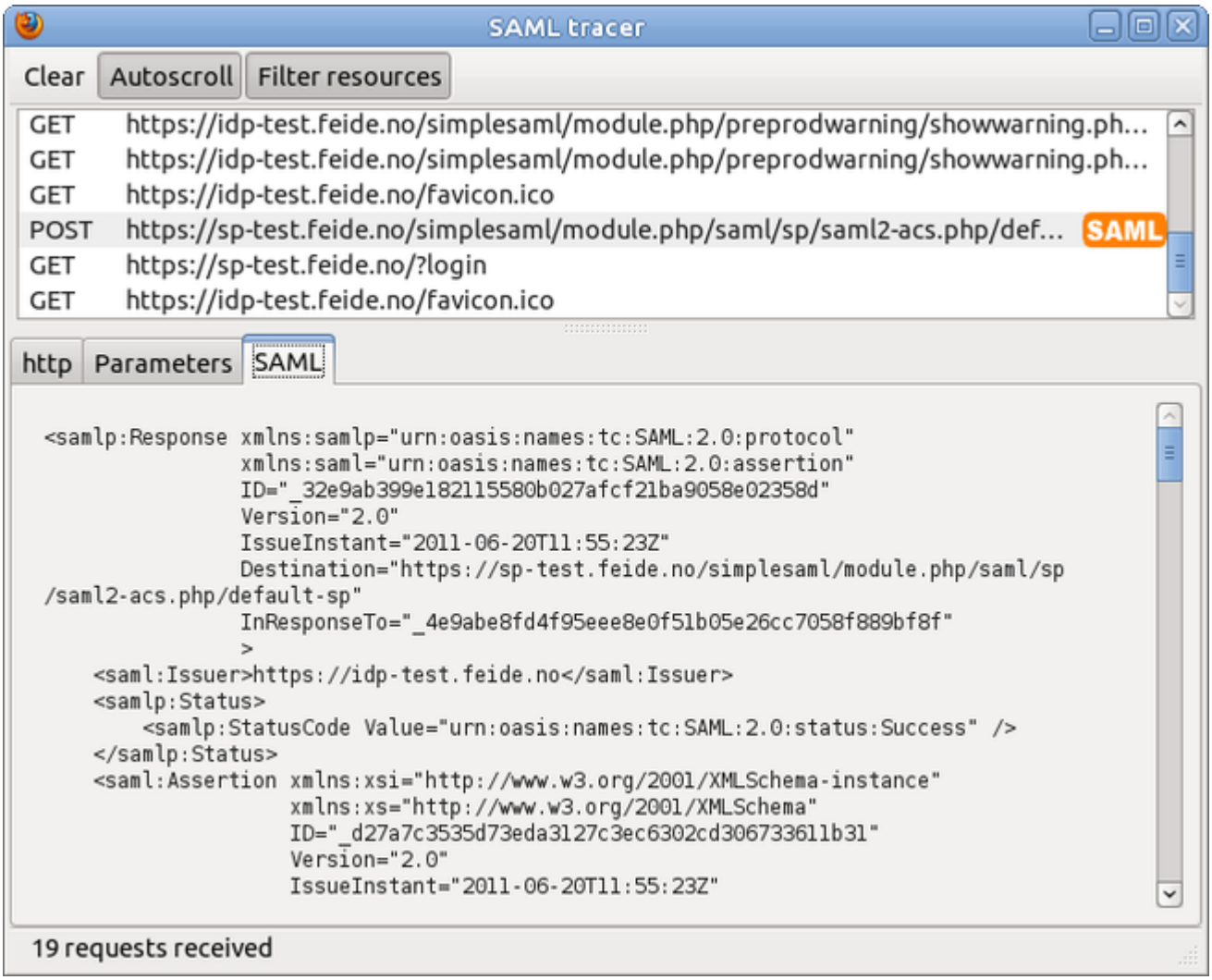
Para comenzar, aquí hay un par de herramientas para varios navegadores que deberían comenzar:

Cromo

- Panel de cromo SAML
- Extensión SAML DevTools
- Decodificador de mensajes SAML

Firefox

- SAML Tracer
- SSO Tracer



Al usar, por ejemplo, SAML Tracer , puede ver aserciones y solicitudes SAML descodificadas en tiempo real mientras prueba y depura

Lea Empezando con saml-2.0 en línea: https://riptutorial.com/es/saml-2-0/topic/5634/empezando-con-saml-2-0

Creditos

S. No	Capítulos	Contributors
1	Empezando con saml-2.0	Community, Rick