

Drupal SSO Using SAML

Will Hartmann

Goals

- Learn a bit about SSO using SAML
- Understand SSO customization possibilities
- Open discussion

Who am I?

- Will Hartmann
- “PapaGrande”
- 9 years working with Drupal, since 4.7
- Back-end dev building sites that interact with external systems
- Disclaimer

What is SSO?

- Single-Sign On
- Authenticating on one site to be able to log into another
- e.g. using Facebook, Google, Twitter, etc. account to log into a site

Terminology

SAML

- Security Assertion Markup Language
- An XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
—Wikipedia

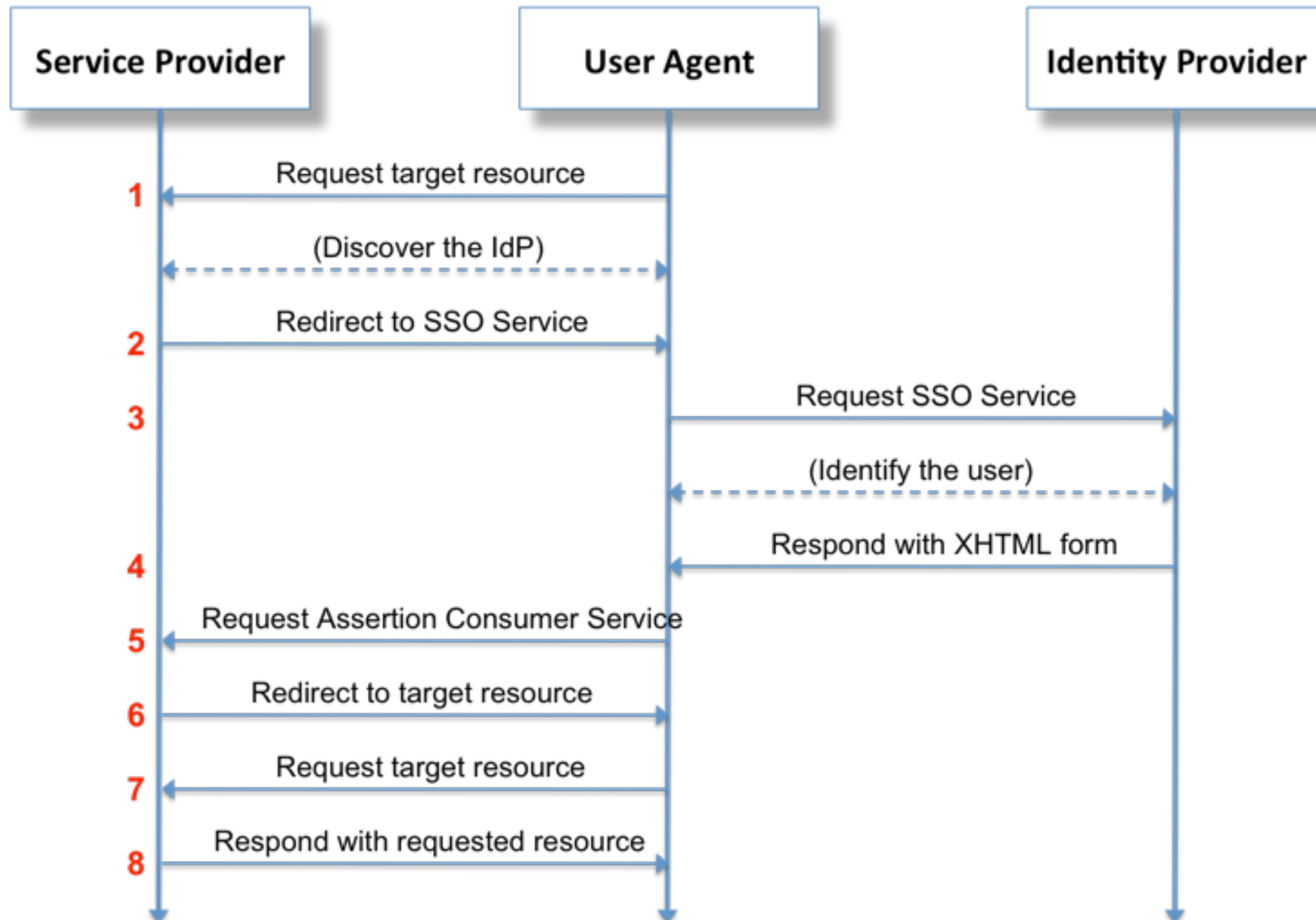
Identity Provider (IdP)

- Authenticates the user

Service Provider (SP)

- The website the user is accessing

How it works



Required Tools

- Library: simplesamlphp
 - <https://simplesamlphp.org/>
- Module: simplesamlphp_auth
 - https://www.drupal.org/project/simplesamlphp_auth

Setup #1 - Installation

1. Install library

1.1.sites/all/libraries/simplesamlphp

2. Create symlink in Drupal root:

```
2.1.ln -s sites/all/libraries/  
simplesamlphp/www simplesaml
```

3. Install module

```
3.1.drush dl simplesamlphp_auth
```

Setup #2 - Configuration

1. Configure simplesamlphp lib

1.1. sites/all/libraries/simplesamlphp/config/config.php

```
'auth.adminpassword' => 'setnewpasswordhere',  
'secretsalt' => 'randombytesinsertedhere',  
'technicalcontact_name' => 'insertName',  
'technicalcontact_email' => 'insertEmail',  
'timezone' => 'America/Los Angeles', (set your desired timezone)
```

1.2. Generate keys (in Linux)

```
1.2.1. tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd  
bs=32 count=1 2>/dev/null; echo
```

1.3. Change store to 'sql' or 'sqlite'

1.4. Trick for SQL: Add to top of file to keep db credentials separate

```
include(__DIR__ . '/../..../default/settings.php');
```

2. Test

2.1. <http://yoursite.com/simplesaml>

Setup #3 - Key Generation

1./sites/all/libraries/simplesamlphp/config/authsources.php

```
'impact-dev' => array(  
    'saml:SP',  
    'privatekey' => 'saml.pem',  
    'certificate' => 'saml.crt',  
    'idp' => 'https://stage.projectoutcome.org/saml',  
),
```

2.cd /sites/all/libraries/simplesamlphp/cert

```
2.1.openssl req -newkey rsa:2048 -new -x509 -  
days 3652 -nodes -out saml.crt -keyout saml.pem
```

Setup #4 - Key Sharing

1. Go to <https://youridp.org/saml/metadata>
 - 1.1. Get metadata in XML
 - 1.2. Copy XML
2. Go to <http://yoursite.com/simplesaml/admin/metadata-converter.php>
 - 2.1. Paste XML
3. open <sites/all/libraries/simplesamlphp/metadata/saml20-idp-remote.php>
 - 3.1. Paste in metadata

Setup #5 - Configure SimpleSAMLphp_auth Module

1. Check Activate authentication via SimpleSAMLphp
2. Set Authentication Source (as set in authsources.php - ex:drupal-prod)
3. Which attribute from simpleSAMLphp should be used as user's name
 - 3.1. displayName
4. Which attribute from simpleSAMLphp should be used as unique identifier for the user
 - 4.1. mail
5. Which attribute from simpleSAMLphp should be used as user mail address
 - 5.1. mail

Setup #5.1 - Configure SimpleSAMLphp_auth Module

6. Check Register users

7. Check Allow authentication with local Drupal accounts

8. Which ROLES should be allowed to login with local accounts?

9. administrator, authenticated user, or specific role

10. Click Save configuration

11. Trick: Save site-specific variables to settings.php per server

UX Demo

What's happening?

- Redirects in the browser from SP to IdP & back to SP
- Cookies written for SP & IdP sessions

Underneath the Drupal Covers

- authmap table
- simpleSAMLphp tables

Customizations

- Registration
- Login

Useful Hooks

- `hook_user_presave()`
- `hook_user_insert()`
- `hook_user_login()`

Custom Code

Drupal 8

- Not sure, but there is a dev version of `simplesamlphp_auth`

Resources

- Comparison of Single Sign On (SSO) Modules
 - <https://groups.drupal.org/node/182004>
- <https://simplesamlphp.org/>
- https://www.drupal.org/project/simplesamlphp_auth

Recap

- SSO & SAML Basics
- SimpleSAML Setup
- Registration & Login Customization

Questions