Best Practice:
WAYFless Access to Resources

Configuring on a Service
and Using in a Portal

v1.0

Prepared by:
Rhys Smith (Cardiff University & JANET(UK))
and John Murison (SDSS, EDINA)

Table of Contents

Executive Summary

- A WAYFless URL, which is specific to an institution with associated users and to a web-based service or resource, enables a user from that institution to gain federated access to the service or resource in a way that bypasses the 'Where Are You From' (WAYF) or Discovery Service step. Since a WAYF can be confusing and unpleasant to negotiate, bypassing it represents an improved end-user experience; this in turn can help organisations ensure that their users get best use of the services and resources that they provide.
- A WAYFless URL comes in two forms:
  1. SP-side WAYFless URL: this must be supported by the service in question, but represents the most flexible and reliable type of WAYFless URL.
  2. IdP-side WAYFless URL: this does not require to be supported by the service, but requires the inclusion within the URL of service-related components that may change, without notice and beyond the control of the institution, and can thus break easily.
- It is recommended that services support SP-side WAYFless URLs, by implementing session initiators. Optionally (but strongly recommended) these session initiators should follow a common format.

Recommendation 1 – for Service Providers

Providers of services should implement a Session Initiator. If the service uses the Shibboleth SP software, this is already built in and requires little additional work.

Recommendation 2 – for Service Providers

When implementing Session Initiators, in order to facilitate access by institutions, services should follow the recommended naming convention, namely:

`https://yourhost/start-session?entityId=X&target=Y`

(*Italicised* items are placeholders, described below.)

- Organisations wishing to make use of WAYFless URLs should use an SP-side WAYFless URL for a service if that service provides a session initiator, and an IdP-side WAYFless URL otherwise.

Recommendation 3 – for Institutions

Institutions should use WAYFless URLs (for example in their organisational portals) to make access to services and resources easier for their users.

If a service supports SP-side WAYFless URLs, by providing session initiators, the institution should use this form. If it does not, the institution should construct an IdP-side WAYFless URL and use it instead, until the service supports the SP-side form.

1. Introduction

WAYFless URLs are a method of allowing an organisation to build links, e.g. for use in an institutional portal, that enable a user from that organisation to connect to a service or resource using federated access management, without the user having to negotiate a 'Where Are You From' service (WAYF, now known as a 'Discovery Service'). This reduces the number of steps that the user must go through in order to gain access to the service, and so represents a better end-user experience.

1.1. Intended Audience

This report is intended for:

- Management and technical staff at Service Providers wishing to understand and enable WAYFless access to their services.
- Management and technical staff at organisations wishing to use WAYFless URLs to give improved service access for their organisation's end users.

1.2. Structure of Report

Section 2 is for both service provider and institutional audiences, and describes in detail the problem that WAYFless URLs address, and how they work.

Section 3 is for service providers, and describes how they can enable access to their services or resources via WAYFless URLs.

Section 4 is for organisations with end users, and describes how to deploy WAYFless URLs in an institutional portal or similar.

2. The Discovery Problem

A problem currently inherent in using federated access technologies – and one that WAYFless URLs try to solve – is commonly known as the 'Discovery Problem'. The essence of the Discovery Problem is as follows:

Each time an end-user starts his or her web browser and tries to gain access to a web-delivered service or resource, that service or resource needs to establish which organisation provides credentials for the user, in order to determine whether the user is entitled to use the service.

In technical terminology, the task for the service is to establish the 'identity provider' (IdP) for this user. Thus, in order to deal with a request for service from a user, the 'service provider' (SP) needs to establish which IdP to communicate with. This is the 'Discovery Problem'.

2.1. Possible Solutions to the Discovery Problem

2.1.1. The WAYF

Conceptually, the simplest solution to the Discovery Problem is to show a list of all possible IdPs to the user, and ask the user to choose one: this is the 'WAYF' (where are you from?) question.

This may mean that the user is faced with having to select their home organisation from a – potentially very large – list of options, which results in a confusing end-user experience, especially on first use. Bear in mind also that while some institutions have their own IdP, so that the institution and its IdP can be regarded as synonymous, in other cases an institution may outsource its user identity provision, so the IdP to be selected may represent several institutions. This is particularly common in the schools sector, where a Regional Broadband Consortium or Local Education Authority may run a single IdP for all the schools in its region. This makes the choice of IdP for an end-user even more difficult, since the user's own organisation will not appear in the list of IdPs: instead the user needs to be told in advance what name to select.

Once the choice has been made, however, the user is redirected to the IdP and is asked to log in. This will prove that they are associated with an institution represented by the selected IdP. There is then normally a behind-the-scenes exchange between the SP and the IdP to determine whether the user is authorised to use the service and, if all is well, the user is given access.

2.1.2. Improving the WAYF

Can the WAYF process be made easier? There may be ways of ameliorating the choice to be made: for example it may be possible, by exploiting the user's IP address, current geographical location or previous behaviour, to deduce which IdP they may be associated with, and present that as the most likely choice. However, a much better solution would be to find a way of removing the need for the user to choose an IdP at all. Can this be done?

2.1.3. WAYFless URLs

The discovery problem arises when the user tries to gain access to a service by navigating to the service and then requesting access (perhaps by clicking a "login" link). If the user were instead to be provided with a special URL to use in their browser which in some way contained the correct answer to the discovery problem for that user, then the service would immediately know which IdP to communicate with, and the WAYF question would not have to be asked.

The actual value for the URL will depend on the appropriate IdP for the end-user's institution. This leads directly to the notion of an institution providing what could be referred to as a 'portal': that is, a web page containing a collection of these special URLs (one per service) which end-users from the institution can use in order to gain 'WAYFless' access to services which the institution is licensed to use.

The user experience when invoking a service is then:

1. User goes to institutional portal. Often there is a login challenge at this point.
2. User finds the service that they wish to access from the list of available resources, and clicks that service's link.
3. User gains access to the service, assuming that they are entitled to do so by the terms of the licence that the institution holds for the service.

This is clearly superior to asking the user to choose from a very large list of IdPs.

2.2. Types of WAYFless URL

There are two forms of WAYFless URL:

- those that point to a specific location on an SP – an SP-side WAYFless URL
- those that point to a specific location on an IdP – an IdP-side WAYFless URL

2.2.1. SP-side WAYFless URLs

An SP-side WAYFless URL points to a specific location on the SP designed to initiate a session with a particular IdP, by including the unique *entityID* of the IdP in the URL; it may also include a target URL to redirect the user to once authorised.

SP-side WAYFless URL format

```
https://SPHOSTNAME/SESSION_INITIATOR_LOCATION?
        entityID=YOUR_IdP&
        target=RESOURCE_LOCATION
```

SP-side WAYFless URL example with a target specified

```
https://sp.example.com/start-session?
        entityID=https://idp.example.com/idp/shibboleth&
        target=https://sp.example.com/some/webpage.html
```

Note that these forms of WAYFless URL do not contain any hard-coded web service URLs within the chosen IdP's site, which means that technical changes at the IdP will not affect the validity of the SP-side WAYFless URL.

2.2.2. IdP-side WAYFless URLs

An IdP-side WAYFless URL points directly to the authentication web service URL of the IdP, and contains additional parameters that tell the IdP where on the SP to send the authentication assertion.

IdP-side WAYFless format

```
https://IDPHOSTNAME/SSO_LOCATION?target=RESOURCE_LOCATION&
        shire=ACS_LOCATION&
        providerId=PROV_ID
```

IdP-side WAYFless URL example with a target specified

```
https://idp.example.com/idp/profile/Shibboleth/SSO?target=https%3A%2F
%2Fsp.example%2Fcom%2Fsome%2Fwebpage.html&shire=https%3A%2F%2Fsp.exam
ple.com%2FShibboleth.sso%2FSAML%2FPOST&providerId=https%3A%2F%2Fsp.ex
ample.com%2Fshibboleth-sp
```

2.2.3. Which type is better?

IdP-side WAYFless URLs work perfectly well, but are more 'brittle' than SP-side WAYFless URLs since they contain hard-coded web service locations within the IdP site; whereas, as we have seen, SP-side WAYFless URLs only contain that IdP's unique entityID. For this reason SP-side WAYFless URLs are preferable, if the service in question supports them.

3. For Service Providers: Configuring WAYFless Access

To provide for SP-side WAYFless access to your service, you need to configure what is known as a "Session Initiator". A session initiator essentially defines a web service location that can be invoked as an SP-side WAYFless URL.

3.1. Configuring a Session Initiator

Conceptually, a session initiator is a way of configuring how sessions should be started on your service: that is, whether a user without a current session should be sent directly to a particular IdP, to a WAYF service or to a Discovery Service; it requires the technical details to enable this decision.

How easy or difficult this is to do depends on the federated access software you are using.

3.1.1. …natively with the Shibboleth SP

If you are using the Shibboleth 2 SP, session initiators are built in to the software, and are very likely to be configured already. These are configured in the shibboleth2.xml file and are of the form:

Example Discovery Service Session Initiator

```
<SessionInitiator type="Chaining" Location="/DS" id="DS"
                  relayState="cookie">
    <SessionInitiator type="SAML2" acsIndex="1"
                      template="bindingTemplate.html"/>
    <SessionInitiator type="Shib1" acsIndex="5"/>
    <SessionInitiator type="SAMLDS"
                      URL="https://ds.example.org/DS"/>
</SessionInitiator>
```

Shibboleth session initiators allow the entityID of the IdP to be specified, and optionally a target to redirect the user to after successful authentication, for deep linking. (See Section 2.2.1 above.)

3.1.2. …natively with other software

If you are using software other than Shibboleth, you will either have to consult the vendor/developers of the software you are using to see if they natively support the idea of session initiation, or else build your own service that performs this function.

3.2. Using the recommended format

If using session initiators, you can optionally (but highly recommended!) adopt a standard format by having a session initiator at a predefined URL at your site. This URL is as follows:

```
https://yourhost/start-session?entityID=X[&target=Y]
```

Where:

- *yourhost* is the hostname of your service
- *X* is the entityID of the IdP as supplied by the organisation that configured the link
- *Y* is the URL to redirect the user to after successful authorisation.

Typically, session initiators live under the Handler URL of the software, e.g. `/Shibboleth.sso/Login`. If this is the case, there are several ways of enabling access to these session initiators while using the standard URL format. These are now discussed.

3.2.1. ...by mapping directly to a session initiator

You can use mod_rewrite, HTTP redirects, etc., to map requests from the standard URL format of `/start-session?foo` to `/handlerurl/sessioninitatorname?foo`.

Apache/IIS mod_rewrite example

```
RewriteEngine On
RewriteRule ^/start-session /Shibboleth.sso/WAYF [L,R]
```

Apache Redirect example

```
RedirectMatch /start-session$ /Shibboleth.sso/WAYF
```

3.2.2. ...by passing information to a Session Initator

An alternative to directly implementing the HTTP redirect within the web server would be to create a script that sits at the standard location (`/start-session`) which accepts the two parameters of `entityID` and `target` and constructs a redirect to return to the client that sends them to the actual session initiator.

Example Perl Script

```
#!/usr/bin/perl


use CGI;
$query=CGI->new;

# Get the entityID and target as passed to this script
$entityID = $query->param('entityID');
$target = $query->param('target');


# Create a URL to redirect to, which will be the Session Initiator
# with entityID as a query string parameter, and also ‘target’ if
# it was specified when calling this script.
$url =
"https://sp.example.com/Shibboleth.sso/WAYF?entityID=$entityID";
if ($target) { $url = $url . "&target=" . $target; }


# Redirect
print $query->redirect($url);
```

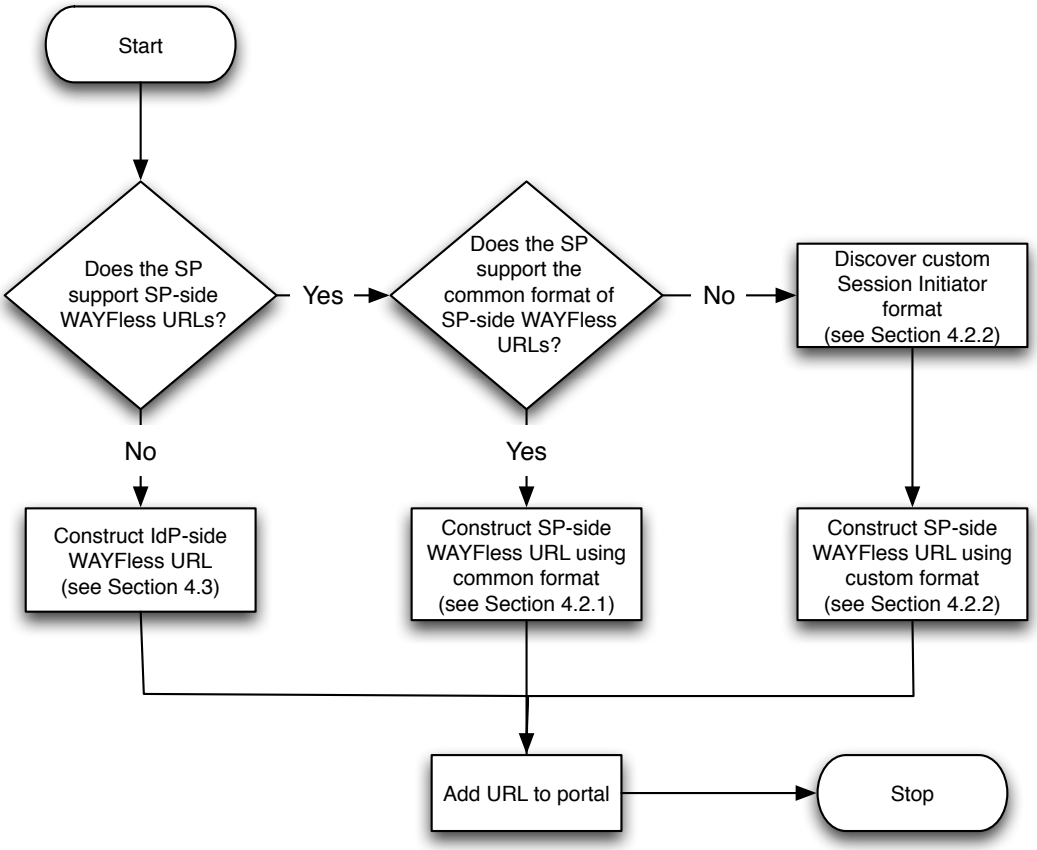
4. For Identity Providers: Using WAYFless Links

Those who wish to use WAYFless links in an institutional portal must first create the link and then add it to the portal. Creating the link is unfortunately not a simple task; there are several formats in which this WAYFless URL can exist, ranging from more to less preferred:

1. SP-side WAYFless URL using a common recommended format is most preferred
2. SP-side WAYFless URLs using its own format is next preferred
3. IdP-side WAYFless URL can be used where the first two options are not available.

4.1. How to know which style of WAYFless URL to use

When constructing a WAYFless URL for a particular service, follow the process specified in the flowchart below to figure out which style of WAYFless URL to use. Once you have calculated that, follow the relevant instructions in Section 4.2/4.3 to construct that type of URL.



4.2. Constructing SP-side WAYFless URLs

4.2.1. …in the common format

If the SP in question has implemented Session Initiators and adopted the recommended format, then you simply have to construct a URL in the following format:

```
https://SPHOSTNAME/start-session?entityID=X[&target=Y]
```

Where:

- *SPHOSTNAME*: is the hostname of the SP. This will usually (but not always) be the main hostname of the service itself.
- *X*: is the entityID of your IdP.
- *Y*: is optional and indicates where the user should be redirected to after successful authentication. If not specified the user will be redirected to a default URL as specified by the SP's configuration.

Example SP-side WAYFless URLusing the common format.

```
https://www.example.com/start-session?
  entityID=https://idp.example.com/idp/shibboleth
  &target=https://www.example.com/somejournal/somepage.html
```

4.2.2. …not in the common format

If the SP in question has implemented Session Initiators, but not adopted the common format, then you can perform the following steps:

1. Take a guess – most Shibboleth SP installations use the same Session Initiator configuration, as shown below. Construct a link in this format and see if it works. If so, use this URL. If not, proceed to step 2.

   ```
   https://SPHOSTNAME/Shibboleth.sso/Login?entityID=X[&target=Y]
   ```

   Where the parameters are the same as discussed in Section 4.1.1.

2. Check the SP's entry on the Services section of the UK federation website to see if their custom Session Initiator is recorded there. If so, follow the guidance on there to construct the WAYFless URL. If this information is not present, proceed to step 3.
3. Contact the SP to ask them what the URL to their Session Initiator is, and follow their guidance to construct the WAYFless URL.

Example SP-side WAYFless URL not in the common format.

```
https://www.example.com/Shibboleth.sso/Login?
  entityID=https://idp.example.com/idp/shibboleth
  &target=https://www.example.com/somejournal/somepage.html
```

4.3. Constructing IdP-side WAYFless URLs

If SP-side WAYFless URLs are not available for an SP, you will have to construct and IdP-side WAYFless URL for use until such time as the SP supports them.

An IdP-side WAYFless URL has the following format:

```
https://IDPHOSTNAME/SSO_LOCATION?
  target=RESOURCE_LOCATION&
  shire=ACS_LOCATION&
  providerId=PROVIDER_ID
```

Where:

- *IDPHOSTNAME:* is the hostname of your IdP
- *SSO_LOCATION:* is the SAML 2 or Shibboleth 1 SSO endpoint of your IdP
- *Target:* indicates where the user should be redirected to after successful authentication
- *Shire:* is the SAML 2 or SAML 1 web service location of the SP's AssertionConsumerService that the IdP's authentication responses should be sent to
- *providerId*: is the entityID of the SP

Note that all URLs must be suitably URL-encoded.

To construct an IdP-side WAYFless URL you must collect each item of information indicated above and put them together in the form indicated above. The *IDPHOSTNAME* and *SSO_LOCATION* will almost always be the same within a particular IdP, but the *Target*, *Shire*, and *ProviderId* will be different for every SP. These latter pieces of information can only be gathered by asking the SP to provide this information to you, or manually through finding that entity in the appropriate metadata file and discovering this information for yourself.

IdP-side WAYFless URL example

```
https://idp.example.com/idp/profile/Shibboleth/SSO?
  target=https%3A%2F%2Fsp.example%2Fcom%2Fsome%2Fwebpage.html&
  shire=https%3A%2F%2Fsp.example.com%2FShibboleth.sso%2FSAML%2FPOST&
  providerId=https%3A%2F%2Fsp.example.com%2Fshibboleth-sp
```

5. Conclusions and Recommendations

5.1. Recommendations for Service Providers

- Implement a session initiator on your service. If you are using the Shibboleth SP software, these are already built in and will require very little work.
- Follow the recommended naming convention to allow access to your session initiator – that of:

```
https://yourhost/start-session?entityID=X&target=Y
```

5.2. Recommendations for Organisational Portal Developers

- Use WAYFless URLs in your organisation's portal to make access to resources easier for your users.
- If the service supports SP-side WAYFless URLs in the form of session initiators, use those. If they do not, construct IdP-side WAYFless URLs instead as a temporary measure until the service supports the SP-side form.