isPassive

The isPassive feature can only be used with a SAML2 Service Provider. It allows to automatically log in a user on a web page **without any user interaction**. However, for this to work:

1. the user already needs to have a valid session at his Identity Provider and
2. the Discovery Service must be able to "guess" this Identity Provider for the user.

If this both is given, the user's attributes will be available automatically if he accesses a page that makes use of isPassive, e.g. using the script below.

In case one of the above-mentioned two requirements cannot be met, the Service Provider will throw an error. Therefore, a Service Provider administrator who wants to make use of the auto-login feature has to use a script like below that makes sure the user won't see that error.

The main requirement of implementing isPassive for SAML2 products is that there shouldn't be any user interaction when the user is at the Discovery Service or the Identity Provider. Therefore, the usage of isPassive should only work with authentication systems and other authentication related tools, that obey this requirement.

Note:
External authentication systems like CAS and Pubcookie won't obey isPassive most likely.

In order to use the script, try the following:

- Add the script below to a page (#THIS PAGE#) where you want to have auto-login, e.g. a portal's home page.
- In your Service Provider 2.x shibboleth2.xml file, add redirectErrors="#THIS PAGE#" to the Errors element.
    - As of SP 2.2 you can set the `ignoreNoPassive on your AssertionConsumerService, e.g.:`

      ```
      <md:AssertionConsumerService Location="/SAML2/POST" index="
      1"
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
      POST"
          conf:ignoreNoPassive="true" />
      ```

    - If you don't have an <AssertionConsumerService> but only an <SSO> element (new simplified configuration), it is enough to add a **conf: ignoreNoPassive="true"** attribute to it.
- Make sure #THIS PAGE# is protected with a lazy session (no Shibboleth session is enforced but attribute are made available to application in case a user has a session)

Sample JavaScript that can be used to have an auto-login in case a user already has a session at an IdP

```
<!-- START: isPassive script-->
<script type="text/javascript" language="javascript">
<!--
// Written by Lukas Haemmerle <lukas.haemmerle@switch.ch>, SWITCH
/*
This isPassive script will automatically try to log in a user using the SAML2
isPassive feature.
In case a user already has an authenticated session at his Identity Provider and
given the Discovery Service can guess the user's Identity Provider, the user will
eventually be on the exact same page this script is embedded in but logged in
(= Shibboleth attributes are available and user has a valid session with the
Service Provider on the same host).
The user page also will be requested with the same GET arguments than the initial request.

Requirements:
- Only works if a Service Provider 2.x is installed on the same host
- JavaScript must be enabled. Otherwise the script won't have any effect.
- The script must be able to set cookies (required for Shibboleth Service Provider as well)
- In the shibboleth2.xml there must be defined a redirectErrors="#THIS PAGE#" in
  the <Errors> element. #THIS PAGE# must be the relative/absolute URL of the page
  this script is embedded in.
- It also makes sense to protect #THIS PAGE# with a lazy session in order to use
  the Shibboleth attribute that should be available after authentication.
*/

// Check for session cookie that contains the initial location
if(document.cookie && document.cookie.search(/_check_is_passive=/) >= 0){
        // If we have the opensaml::FatalProfileException GET arguments
        // redirect to initial location because isPassive failed
        if (
                window.location.search.search(/errorType/) >= 0
                && window.location.search.search(/RelayState/) >= 0
                && window.location.search.search(/requestURL/) >= 0
        ) {
                var startpos = (document.cookie.indexOf('_check_is_passive=')+18);
                var endpos = document.cookie.indexOf(';', startpos);
                window.location = document.cookie.substring(startpos,endpos);
        }
} else {
        // Mark browser as being isPassive checked
        document.cookie = "_check_is_passive=" + window.location;

        // Redirect to Shibboleth handler
        window.location = "/Shibboleth.sso/Login?isPassive=true&target=" + encodeURIComponent(window.location);
}
//-->
</script>
<!-- END: isPassive script-->
```

Note:
In case the Discovery Service guesses that a user's Identity Provider is a SAML1 IdP, this IdP won't obey the requirements of isPassive not to interact with the user. Therefore, it still could occur that the user is asked to authenticate at the IdP.
If a user already has a session with a SAML1 IdP, things should work as expected unless there are any other tools installed at the IdP that won't obey isPassive.