SP manual for the installation, configuration of SimpleSAMLphp and connection with TAAT

1. Download SimpleSAMLphp from http://simplesamlphp.org/download and unpack the archive in your webserver.

2. Make sure the server configuration (*vhost*) allows access to the installation directory.

   If you are using Suhosin then you need to change the configuration to allow for longer GET parameter values. In the case of Debian change the file */etc/php5/apache2/conf.d/suhosin.ini*:

   ```
   suhosin.get.max_value_length = 2048
   ```

3. Navigate to the installation directory and copy the following 2 files from *config-templates/* to *config/* directory:

   ```
   cp config-templates/config.php config-templates/authsources.php config
   ```

4. Edit the following lines in the file *config/config.php*:

   - `baseurlpath' => 'myinstallationdirectory/',` - use '/' in case of root directory.
   - `'secretsalt' => 'randomsymbolstring',` - you can use the guide in the comments of the code for the generation of the symbol string or enter it yourself.
   - `'auth.adminpassword' => 'adminpsswd',`
     `'technicalcontact_name' => 'name of the technical contact',`
     `'technicalcontact_email' => 'e-mail of the technical contact,`
   - `'timezone' => 'Europe/Tallinn',`

5. Locate the authproc.idp block (at the bottom) within the same file, comment the line that starts with „10 =>“ and modify it in the following way:

   ```
   10 => array(
    'class' => 'core:AttributeMap', ''urn2name''
   ),
   ```

6. In the file *authsources.php* modify the default-sp name to correspond with the name of your service and add the following lines:

   ```
   'certificate' => 'server.crt',
   'privatekey' => 'server.pem',
   'redirect.sign' => TRUE, // sign authn requests, logout requestsand responses sent
   from this SP
   'redirect.validate' => TRUE, // validate signature of authn requests, logout
   requests and responses sent to this SP
   'sign.authnrequest' => TRUE, // sign authentication requests sent from this SP
   'sign.logout' => TRUE, // sign logout messages sent from this SP
   'validate.logout' => TRUE, // validate signature of logout messages sent to this SP
   ```

7. A valid certificate must be stored in the */cert* directory. You can generate a self-signed certificate like this:

   ```
   rm server*
   openssl req -nodes -new -keyout server.pem -newkey rsa:2048 > server.csr
   openssl x509 -req -days 1095 -in server.csr -signkey server.pem -out server.crt
   chgrp www-data server.*
   chmod o-r server.pem
   ```

8. Create the file *metadata/saml20-idp-remote.php* and copy there the Idp metadata of both TAAT hubs. The metadata is available here:

   https://reos.taat.edu.ee/saml2/idp/metadata.php?output=xhtml (necessary for *test* status)
   https://sarvik.taat.edu.ee/saml2/idp/metadata.php?output=xhtml

   Don't forget to start the file with php declaration. Example:

```
<?php
$metadata['https://reos.taat.edu.ee/saml2/idp/metadata.php'] = array ('metadata-
set' => 'saml20-idp-remote',
'entityid' => 'https://reos.taat.edu.ee/saml2/idp/metadata.php',
'SingleSignOnService' => 'https://reos.taat.edu.ee/saml2/idp/SSOService.php',
'SingleLogoutService' =>
'https://reos.taat.edu.ee/saml2/idp/SingleLogoutService.php',
'certData' =>
'MIIDUDCCAjgCCQDNqOA94B8faTANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQGEwJFRTERMA8GA1UECBMIVG
FydHVtYWExDjAMBgNVBAcTBVRhcnR1MQ4wDAYDVQQKEwVFRU5ldDENMAsGA1UECxMEVEFBVDEZMBcGA1UEA
xMQcmVvcy50YWF0LmVkdS5lZTAeFw0xMzAzMDQxMTQ1NTFaFw0xNjAzMDMxMTQ1NTFaMGoxCzAJBgNVBAYT
AkVFMREwDwYDVQQIEwhUYXJ0dW1hYTEOMAwGA1UEBxMFVGFydHUxDjAMBgNVBAoTBUVFTmV0MQ0wCwYDVQQ
LEwRUQUFUMRkwFwYDVQQDExByZW9zLnRhYXQuZWR1LmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
KCAQEA5VBwvMzbOzT8oyJTk4P7p6gM9hOIe9P6G18ztgegyJZ+TFa+TaU8EXDndvAF5kuBGEtIMgTNujsKg
qAyM5W7uZO+Aa6WKZU0JH8z0uNHKtxJT49Up44G6047GkwpRH/VUT/GUw2wzQJhCEgPFAdnkiUE4eZ+gksr
slvREPg4MDOBAlvQd5hejEYlBmDIMLhKiDLgdVVzUOVLBcJmV+VVMnmsIAbJGkWrhpvkpNS95hl0CpnV+jy
P48VDFSbuT8RjucJlbvjOdTUodF3P2yjfzbBHr15uDIGL25ZwX7zjrOudNsp4VPzwlTuoEtnGgtK+MevisI
9uVeoaxJ8+BwuCIQIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQAn4XgAYULlrw0Aoxm7DtqiP2yNcK44WE97W
eIfbq4XY1NqM+E5mA4pepbFOG1REvIzOG1G0MRGQdxgf8gVKSAHTkDusu2Ga2suuuw/60X8DoT72qw934JX
ZcCw3XKZgqK/ZHyWgmBwdMVuYsIGZ1d4ZUvByldZ1e80R7IlesrLYGVev6vlnu+s04IafjAJxy8ic0SO7C1
lbtPrE7hE9uuO86ICN6os3VKsBrgas6R7pBCtSLTiF06jmmquFHWoqj06HRRBNvI7ymjGzOb1KU2KhI3zQv
KEpitX5gSNk2KmO3CFzQhmmydzpo2cGoFhPhBSSCRGE85li2oF+aRoRqTq',
'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',
'OrganizationName' =>
array (
 'et' => 'Teaduse Autentimise ja Autoriseerimise Taristu',
 'en' => 'Research Authentication and Authorization Infrastructure',
),
'OrganizationDisplayName' =>
array (
 'et' => 'TAAT',
 'en' => 'TAAT',
),
'OrganizationURL' =>
array (
 'et' => 'http://taat.edu.ee',
 'en' => 'http://taat.edu.ee',
),
);
```

9. Create a user in in JANUS at the address https://taeva.taat.edu.ee/module.php/janus/index.php

10. Add a new connection to JANUS („Create connection") with the ID that corresponds to the "entity id". The latter can be found in your SimpleSAMLphp installation page, under the menu "Federation" and the connection type is "SAML 2.0 SP". You don't need to copy the XML.

11. Select the created connection and go to the page “Import metadata”. Copy the XML or the link to your metadata. You can find this on your SimpleSAMLphp installation page - on the “Federation” page click on “show metadata”.

12. On the page “Metadata” add the metadata that is required in the TAAT Technological Profile: http://taat.edu.ee/main/documents/?lang=en

13. On the page “Connection” select ARP (attribute release policy). Most likely you need to create a new one (“New”). Name your ARP so that it includes the domain name of your institution, the creation/modification date of ARP and select the attributes that you would like to receive from TAAT. These attributes must correspond to the list of attributes to be listed in the future contract. Don’t forget to save the changes.

14. Test your TAAT authentication with test-idp data, available at https://reos.taat.edu.ee/

    NB! Data in our hubs is refreshed every 5 minutes. If your connection does not work initially, wait for 5 minutes and try again.