IdP juhend SimpleSAMLphp paigaldamiseks, seadistamiseks ja ühendamiseks TAATiga.

1. Laadige alla SimpleSAMLphp lehelt http://simplesamlphp.org/download ning pakkige arhiiv lahti oma veebiserverisse.
2. Veenduge, et serveri konfiguratsioon (vhost) võimaldaks võimaldaks ligipääsu installatsioonikausta.
   Kui on kasutusel Suhosin, siis on vaja see seadistada lubama pikemaid GET parameetrite väärtuseid. Debiani puhul failis */etc/php5/apache2/conf.d/suhosin.ini*
   ```
   suhosin.get.max_value_length = 2048
   ```
3. Navigeerige installatsioonikausta ja kopeerige kaustast *config-templates/* failid *config.php* ja *authsources.php* kausta *config/* ning *metadata-templates/* kaustast fail *saml20-idp-hosted.php* kausta *metadata/* :
   ```
   cp config-templates/config.php config-templates/authsources.php config
   cp metadata-templates/saml20-idp-hosted.php metadata
   ```
4. Muutke failis *config/config.php* järgmised read:
   - `'baseurlpath' => 'minuinstallatsioonikaust/',` - juurkataloogi puhul tuleb installatsioonikaustaks määrata *'/'*
   - `'enable.saml20-idp' => 'true',`
   - `'secretsalt' => 'suvalinesümbolijada',` - sümbolijada genrereerimiseks võib kasutada koodi kommentaarides olevat juhendit või sisestada see ise.
   - ```
     'auth.adminpassword' => 'administraatoriparool',
     'technicalcontact_name' => 'tehnilise kontaktisiku nimi',
     'technicalcontact_email' => 'tehnilise kontaktisiku e-postiaadress',
     ```
   - `'timezone' => 'Europe/Tallinn',`
5. Leidke samas failis authproc.idp plokk (kõige all), kommenteerige sisse rida mille alguses on „10 =>“ ning muutke see järgmiseks:
   ```
   100 => array(
     'class' => 'core:AttributeMap', ''name2urn''
   ),
   ```
6. Failis *config/authsouces.php* kommenteerige välja kõik autentimisallikad, mida te ei kasuta ning eemaldage kommentaarid sellelt, mida kasutate (olgu selleks siis SQL andmebaas, LDAP või midagi muud). Testimiseks sobib kõige paremini *exampleauth:UserPass*.
7. Konfigureerige valitud autentimisallikas vastavalt oma autentimissüsteemile, arvestades, et väljastama peate atribuudid, mis on nõutud TAAT Tehnoloogilises profiilis (http://taat.edu.ee/main/dokumendid/).
   NB! Kui autentimine toimub ühes süsteemis (nt LDAP) ning vajalikke andmeid võetakse teisest (nt SQL andmebaasist), siis selleks on olemas eraldi atribuutide koguja moodul: https://forja.rediris.es/svn/confia/attributecollector/
8. Aktiveerige valitud autoriseerimisallika moodul:
   ```
   touch modules/exampleauth/enable
   ```
9. Muutke failis *metadata/saml20-idp-hosted.php* järgmised read:
   ```
   'certificate' => 'server.crt',
   'privatekey' => 'server.pem',  - sertifikaadiandmed vastavalt enda poolt kasutatud
   sertifikaatidele
   'auth' => 'example-userpass',  - autentimisallikas, mida kasutate
   ```
   ning lisage järgmised:
   ```
   'sign.logout' => TRUE,        // sign logout messages sent from this IdP
   'validate.authnrequest' => TRUE,  // require signatures on authentication requests sent
   to this IdP
   'validate.logout' => TRUE,    // require signatures on logout messages sent to this IdP
   'redirect.sign' => TRUE,      // sign logout requests and responses sent from this IdP
   'redirect.validate' => TRUE,  // validate logout requests and responses sent to this IdP
   ```
   ```

10. Looge fail *metadata/saml20-sp-remote.php* ning kopeerige sinna kahe TAATi jaoturi SP metaandmed, mis on leitavad aadressidel:

    https://reos.taat.edu.ee/module.php/saml/sp/metadata.php/TAAT?output=xhtml
    https://sarvik.taat.edu.ee/module.php/saml/sp/metadata.php/TAAT?output=xhtml

    Ärge unustage failis alustada php-d.
    Näide:

```
<?php
$metadata['https://reos.taat.edu.ee/module.php/saml/sp/metadata.php/TAAT'] = array (
  'AssertionConsumerService' =>
'https://reos.taat.edu.ee/module.php/saml/sp/saml2-acs.php/TAAT',
  'SingleLogoutService' =>
'https://reos.taat.edu.ee/module.php/saml/sp/saml2-logout.php/TAAT',
  'certData' =>
'MIIDUDCCAjgCCQDNqOA94B8faTANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQGEwJFRTERMA8GA1UECBMIVGFydHVt
YWExDjAMBgNVBAcTBVRhcnR1MQ4wDAYDVQQKEwVFRU5ldDENMAsGA1UECxMEVEFBVDEZMBcGA1UEAxMQcmVvcy50Y
WF0LmVkdS5lZTAeFw0xMzAzMDQxMTQ1NTFaFw0xNjAzMDMxMTQ1NTFaMGoxCzAJBgNVBAYTAkVFMREwDwYDVQQIEw
hUYXJ0dW1hYTEOMAwGA1UEBxMFVGFydHUxDjAMBgNVBAoTBUVFTmV0MQ0wCwYDVQQLEwRUQUFUMRkwFwYDVQQDExB
yZW9zLnRhYXQuZWR1LmVlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5VBwvMzbOzT8oyJTk4P7p6gM
9hOIe9P6G18ztgegyJZ+TFa+TaU8EXDndvAF5kuBGEtIMgTNujsKgqAyM5W7uZO+Aa6WKZU0JH8z0uNHKtxJT49Up
44G6047GkwpRH/VUT/GUw2wzQJhCEgPFAdnkiUE4eZ+gksrslvREPg4MDOBAlvQd5hejEYlBmDIMLhKiDLgdVVzUO
VLBcJmV+VVMnmsIAbJGkWrhpvkpNS95hl0CpnV+jyP48VDFSbuT8RjucJlbvjOdTUodF3P2yjfzbBHr15uDIGL25Z
wX7zjrOudNsp4VPzwlTuoEtnGgtK+MevisI9uVeoaxJ8+BwuCIQIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQAn4XgA
YULlrw0Aoxm7DtqiP2yNcK44WE97WeIfbq4XY1NqM+E5mA4pepbFOG1REvIzOG1G0MRGQdxgf8gVKSAHTkDusu2Ga
2suuuw/60X8DoT72qw934JXZcCw3XKZgqK/ZHyWgmBwdMVuYsIGZ1d4ZUvByldZ1e80R7IlesrLYGVev6vlnu+s04
IafjAJxy8ic0SO7C1lbtPrE7hE9uuO86ICN6os3VKsBrgas6R7pBCtSLTiF06jmmquFHWoqj06HRRBNvI7ymjGzOb
1KU2KhI3zQvKEpitX5gSNk2KmO3CFzQhmmydzpo2cGoFhPhBSSCRGE85li2oF+aRoRqTq',
);
```

11. Tehke kasutaja JANUSesse aadressil https://taeva.taat.edu.ee/module.php/janus/index.php
12. Lisage JANUSesse uus ühendus („Create connection“), kus ID on „entity id“, mis on leitav teie oma SimpleSAMLphp installatsioonilehel menüüst „Federation“ ning ühenduse tüübiks on „SAML 2.0 IdP“. XML-i ei ole vaja kopeerida.
13. Valige loodud ühendus ja minge lehele „Import metadata“. Kopeerige oma metaandmete XML või link, mille leiate oma SimpleSAMLphp installatsioonilehet „Federation“ vahelehelt „show metadata“ klõpsates.
14. Vahelehel „Metadata“ lisage metaandmed, mis on nõutud TAAT Tehnoloogilises profiilis (http://taat.edu.ee/main/dokumendid/).
15. Testige sisselogimist TAAT testlehel https://eitja.taat.edu.ee/
    NB! Jaoturite andmeid uuendatakse kord 5 min jooksul. Kui teie ühendus kohe ei toimi, oodake 5 minutit ja proovige uuesti.