SP 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/* :
   ```
   cp config-templates/config.php config-templates/authsources.php config
   ```
4. Muutke failis *config/config.php* järgmised read:
   - `baseurlpath' => 'minuinstallatsioonikaust/',` - juurkataloogi puhul tuleb installatsioonikaustaks määrata *'/'*
   - `'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:
   ```
   10 => array(
     'class' => 'core:AttributeMap', ''urn2name''
   ),
   ```
6. Failis *authsources.php* muutke default-sp nimi vastavaks oma teenuse nimega ning lisage read:
   ```
   '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 fromthis SP
   'sign.logout' => TRUE,       // sign logout messages sent from this SP
   'validate.logout' => TRUE,   // validate signature of logout messages sent to this SP
   ```
7. Kaustas *cert/* peab olema kehtiv sertifikaat. Self-signed sertifikaadi saab genereerida nii:
   ```
   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. Looge fail *metadata/saml20-idp-remote.php* ning kopeerige sinna kõigi kahe TAATi jaoturi IdP metaandmed, mis on leitavad aadressidel:

   https://reos.taat.edu.ee/saml2/idp/metadata.php?output=xhtml (vajalik ainult test staatuses)
   https://sarvik.taat.edu.ee/saml2/idp/metadata.php?output=xhtml

   Ärge unustage failis alustada php-d.
   Näide:

   ```
   <?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' =>
'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',
'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. Tehke kasutaja JANUSesse aadressil https://taeva.taat.edu.ee/module.php/janus/index.php
10. 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 SP“. XML-i ei ole vaja kopeerida.
11. Valige loodud ühendus ja minge lehele „Import metadata“. Kopeerige oma metaandmete XML või link, mille leiate oma SimpleSAMLphp installatsioonilehet „Federation“ vahelehelt „show metadata“ klõpsates.
12. Vahelehel „Metadata“ lisage metaandmed, mis on nõutud TAAT Tehnoloogilises profiilis (http://taat.edu.ee/main/dokumendid/).
13. Vahelehel “Connection” valige endale ARP ehk atribuutide väljastamise poliitika. Tõenäoliselt on teil vaja luua uus “New”. Nimetage oma ARP nii, et nimi sisaldaks teie asutuse domeeninime ja ARP lisamise/muutmise kuupäeva ning valige atribuudid, mida soovite TAATi kaudu vastu võtta. Atribuudid peavad klappima hiljem sõlmitud lepingus oleva atribuutide nimistuga. Ärge unustage ka muudatusi salvestada.
14. Testige sisselogimist TAAT test-idp andmetega, mille leiate lehelt 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.