Ghid pentru instalare IdP (identity provider) în baza simpleSAMLphp

Prefaţă

Schema generalizată a funcţionării federaţiei LEAF (figura 1) conţine entităţi şi legături. Printre entităţi se enumeră:

- IDSI IdP – prestator de identitate
- e-mail SP – prestator de serviciu
- LEAF – serviciu de management a entităţilor şi partajare a metadatei
- eduGAIN – serviciu de management a metadatelor
- serviciu extern – prestator de serviciu din exteriorul federaţiei

Printre legături se enumeră:

- săgeți cu linii continue – flux de metadate pentru managementul entităţilor
- săgeți cu linii continue (SAML date) – flux de metadate pentru autentificare/autorizare
- săgeți cu linii întrerupte – flux de date pentru înregistrarea entităţilor în federaţie

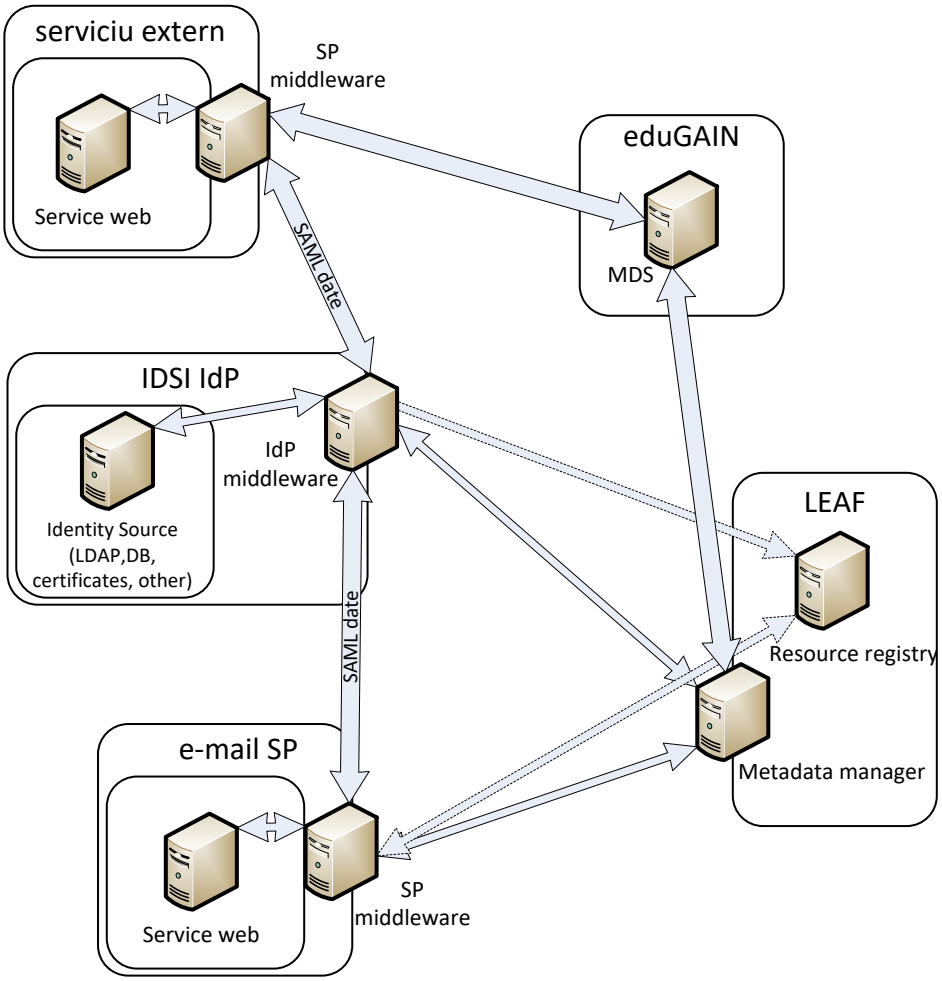

Figura 1. Schema generalizată a funcţionării federaţiei

Accesul către servicii are lor conform următoarei scheme:

1. utilizatorul accesează pagina web al serviciului
2. utilizatorul selectează autentificarea prin SSO
3. utilizatorul este redirecționat la pagina unde va fi selectat prestatorul de identitate
4. utilizatorul este redirecționat la pagina web al prestatorului de identitate unde va trebui sa se autentifice(SAML date)
5. in caz de succes utilizatorul este redirecţionat la pagina cu serviciul

Pentru lansarea unui element IdP nu este necesar un element de calcul separat. IdP middleware, care în cazul acestui ghid este simpleSAMLphp, poate fi instalat direct pe unitatea unde se afla şi sursa de identificare(baze de date, certificate, LDAP, altele). Componenta soft instalată va utiliza resurse doar în momentul autentificării şi actualizării metadatelor.

Instalare IdP

Pentru descrierea procesului de instalare nu vor fi specificate instrucţiunile necesare spre rulare în sistemul operaţional. Va fi specificat doar rezultatul care trebuie sa fie obţinut. Pentru problemele apărute consultaţi manualul sistemului operațional sau persoana de contact al operatorului federaţiei.

Instalarea se va începe cu copierea si verificarea funcţionării middleware.

1. Conform recomandărilor de pe pagina https://simplesamlphp.org/docs/1.15/simplesamlphp-install efectuaţi instalarea şi testarea iniţială a aplicaţiei, şi anume:
   a. verificaţi minimul necesar pentru instalare:
      - *server pentru rularea PHP*
      - *PHP version >= 5.4.0.*
      - *Suport pentru următoarele extensii PHP:*
        1. *date, dom, hash, libxml, openssl, pcre, SPL, zlib, json, curl*
        2. *pentru autentificare LDAP: ldap*
        3. *pentru autentificare RADIUS: radius*
        4. *pentru utilizarea sesiilor PHP: session*
        5. *pentru pastrarea informatiei din sesie în memcache: memcache*
        6. *pentru utilizarea bazelor de date:*
           a. *PDO*
           b. *Database driver: (mysql, pgsql, ...)*
   b. copiaţi şi instalaţi simpleSAMLphp
   c. configuraţi web serverul pentru accesul corect la middleware
   d. efectuaţi configurările de bază în *config.php*
   e. verificați accesul corect la pagina de start al simpleSAMLphp
2. Conform recomandărilor de pe pagina https://simplesamlphp.org/docs/stable/simplesamlphp-idp efectuaţi configurarea şi testarea a aplicaţiei pentru funcţionarea în calitate de IdP
   a. modificaţi *config.php* pentru funcţionare în calitate de IdP *'enable.saml20-idp' => true,*
   b. Selectaţi şi configuraţi modulul de autentificare modificând *authsources.php* pentru utilizarea modului de autentificare becesar
   c. Generaţi şi instalaţi un certificat pentru semnarea metadatelor
   d. Configuraţi informația despre IdP, care va fi prezentă în metadate, modificînd `saml20-idp-hosted.php`. Exemplul de configurare:

```
////////////////////////////////  inceput
<?php
$metadata['https://gidp.federations.renam.md'] = array(
        'host' => '__DEFAULT__',
/////////////////////////  certificat  pentru semnarea metadatelor
        'privatekey' => 'gidpnew.key',
        'certificate' => 'gidpnew.pem',
        'privatekey_pass' => 'mystrongpass',
/////////////////////////////  modul de autentificare utilizat
        'auth' => 'renam-ldap',
/////////////////////////////  bloc informatie despre entitate
         'RegistrationInfo' => array(
        //// autoritatea d einregistrare
     'authority' => 'http://federations.renam.md/',
        //// politici de activare
 'policies' => array(
                    'ro' => 'http://federations.renam.md',
                    'en' => 'http://federations.renam.md',
                    'ru' => 'http://federations.renam.md'
                    ),
                    ),
        //// determinare prezentare atribute
        'userid.attribute' => 'uid',
        'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
        'name' => array(
       'ro' => 'GIDP-RENAM',
```

```
            'en' => 'GIDP-RENAM',
           'ru' => 'GIDP-RENAM',
        ),

            'UIInfo' => array(
            'DisplayName' => array(
                    'ro' => 'GIDP-RENAM',
                    'en' => 'GIDP-RENAM',
                    'ru' => 'GIDP-RENAM',
                                ),
            'Description' => array(
                    'ro' => 'GIDP-RENAM - prestator de servicii de identitate utilizat de RENAM',
                     'en' => 'GIDP-RENAM - identity provider used by RENAM',
                    'ru' => 'GIDP-RENAM - сервис для идентификации сотрудников RENAM',
                                ),
                        'InformationURL' => array(
                    'ro' => 'https://gidp.federations.renam.md',
                    'en' => 'https://gidp.federations.renam.md',
                    'ru' => 'https://gidp.federations.renam.md',
                                ),
            //// logo organizatie este obligatoriu link https
    'Logo' => array(
            array(
              'url'    => 'https://gidp.federations.renam.md/renam.jpg',
              'height' => 121,
              'width'  => 205,
            ),
        ),
      ),

            'OrganizationName' => array(
            'ro' => 'RENAM',
                    'en' => 'RENAM',
                    'ru' => 'RENAM',
                                            ),
            'OrganizationDisplayName' => array(
            'ro' => 'RENAM',
                    'en' => 'RENAM',
                    'ru' => 'RENAM',
                                            ),
            'OrganizationURL' => array(
            'ro' => 'http://renam.md',
                    'en' => 'http://renam.md',
                    'ru' => 'http://renam.md',
                                            ),
    );
    ///////////////// final bloc de configurare
```

Configurarea prezentată este suficientă pentru initializarea IdP. Pentru funcţionarea normală este necesar de configurat modulul *metarefresh* şi modulul *cron*.

e. Configurarea *metarefresh* poate fi consultată pe https://simplesamlphp.org/docs/1.15/simplesamlphp-automated_metadata

Mai jos este prezentat un exemplu de configurare al modulului metarefresh si anume al fişierului *config-metarefresh.php*

```
<?php
$config = array(
        'sets' => array(
////    masivul cu date pentru configurarea sursei de metadate  locale
'moldova' => array(
                        'cron'              => array('daily'),
```

```
                'sources'          => array(
                array(

        /////  adresa pentru prelucrarea metadatelor din cadrul federatiei
        'src' => 'https://manage.federations.renam.md/signedmetadata/federation/LEAF-MD/metadata.xml',
                                        'template' => array(
                                        'tags'     => array('moldova'),
                                        ),
                                ),
                ),
                'expireAfter'      => 60*60*24*4, // Maximum 4 days cache time.
                'outputDir'        => 'metadata/federation/moldova/',
                'outputFormat' => 'flatfile',
            ),
        ////    masivul cu date pentru configurarea sursei de metadate  edugain
        'edugain' => array(
                'cron'             => array('daily'),
                'sources'          => array(
                        array(
                                'src' => 'http://mds.edugain.org/',
                                'template' => array(
                                        'tags'     => array('edugain'),
                                        'authproc' => array(
                                        51 => array('class' => 'core:AttributeMap', 'oid2name'),
                                        ),
                                ),
                        ),
                ),
                'expireAfter'      => 60*60*24*4, // Maximum 4 days cache time.
                'outputDir'        => 'metadata/federation/edugain/',
                'outputFormat' => 'flatfile',
            ),
        ),
    );
```

Aceasta configurare va citi metadatele din sursele specificate si le amplasa in mapele pe calea specificata. Citirea va fi efectuata conform unui orar setat cu ajutorul modulului cron.

f. Configurati modulul cron utilizînd https://simplesamlphp.org/docs/1.15/cron:cron

Odată ce este finisata configurarea ea trebuie testată. In acest sens trebuie populată metadata. Pentru popularea fişierelor cu metadate trebuie rulata:

curl -k "https://myidentityprovider.md/module.php/cron/cron.php?key=coolestkeyvalue&tag=daily"

La îndeplinirea acestei instrucțiuni va fi populata meta cu condiția ca web serverul are configurata limita de memorie cashe și timp de aștepare suficiente. Pentru testarea funcţională este necesar ca un prestator de serviciu să conțină metadatele IdP–ului configurat recent. Pentru testarea funcțională adresaţi-vă operatorului federației sau purcedeţi la setarea unui SP.

Odată ce setarea IdP este finalizată si testată adresaţi-vă la operatorului federației pentru a efectua teste de interoperabilitate în cadrul federației.