REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO
DIREKTORAT ZA INFORMATIKO IN E-STORITVE

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski socialni sklad

CENTRALNI APLIKACIJSKI GRADNIK

VARNOSTNA SHEMA

sistem za upravljanje z uporabniki in njihovimi pravicami

VARNOSTNA SHEMA

Tip dokumenta	SPECIFIKACIJA
Avtor	ComTrade, d.o.o
Različica dokumenta	1.0
Datum	07. NOVEMBER 2018

Kazalo

1 UVOD

Centralni aplikacijski gradnik Varnostna shema (v nadaljevanju Varnostna shema - VS) zagotavlja administracijo uporabnikov in njihovih vlog na posameznih aplikacijah. Poleg avtentikacije uporabnikov se v sklopu Varnostne sheme upravljajo tudi avtorizacije uporabnikov. Sistem ima vgrajeno SSO funkcionalnost. SSO je mehanizem za enkratno prijavo uporabnika v vse aplikacije, do katerih ima nastavljene pravice, s čimer se izognemo prijavi v vsako aplikacijo posebej. Posamezne aplikacije imajo možnost nastavitve, da se eksplicitno od uporabnika zahteva ob prijavi tudi geslo. SSO izvede avtentikacijo uporabnikov.

Dokument opisuje seznam vmesnikov za integracijo zunanjih aplikacij z Varnostno shemo. Namenjen je razvijalcem, ki želijo integrirati svojo rešitev z omenjenim sistemom. Za integracijo z Varnostno schemo, se lahko izbira med tremi programskimi vmesniki, in sicer:

1. vmesnik, ki je podmnožica protokola CAS 2.0 z nekaj razširitvami.
2. vmesnik podoben prvega, ki poteka preko spletnih storitev (*web service*).
3. vmesnik (*UserInfo*), ki je od omenjenih neodvisna spletna storitev, ki aplikacijam omogoča poizvedovanje po podatkih uporabnikov in njim dodeljenih vlog in pravicah ter vpis prošenj za dodelitev pravic/vlog uporabniku.

Aplikacija lahko uporabi enega ali drugega ali jih kombinira, odvisno o zahtev in okoliščin.

2 ZNAČILNOSTI SISTEMA VARNOSTNE SHEME

Klučne vsebinske lastnosti sistema Varnostne sheme so nasljednje:

1. Varnostna shema je sistem za enotno upravljanje z uporabniki in njihovimi pravicami. Omogoča nadzor dostopa do aplikacij in njihovih funkcionalnosti.
2. Varnostna shema zagotavlja avtentikacijo in avtorizacijo, izključno z uporabo digitalnih potrdil.
3. Uporabniki se lahko prijavijo s katerimkoli veljavnim kvalificiranim digitalnim potrdilom. Pri tem so motenj pri izteku in zamenjavi certifikatov nevtralizirane. Omogočeno je še dodatno varovanje z geslom.
4. Tipična skupina uporabnikov so administratorji.
5. Uporabniki lahko pripadajo eni ali večim institucijam hkrati.
6. Vgrajen je sistem za upravljanje z institucijami (hierarhičen register institucij), na enem mestu so zbrani glavni podatki o vsaki vključeni instituciji.
7. Isti uporabnik ima lahko pri različnih institucijah različne pravice za različne aplikacije.
8. Uporabnik sam zaprosi za pravice, potrdi mu jih odgovorni nadzornik.
9. Z varnostno shemo upravljajo nadzornik institucije, nadzornik tipa institucije in vrhovni nadzornik.
10. Varnostna shema ima podporo za fizične uporabnike in za sistemske uporabnike (aplikacije oz. sistemi).
11. Funkcionalnosti so dostopne preko GUI in preko API vmesnikov.
12. Vgrajena je SSO funkcionalnost oz. vse aplikacije, ki uporabljajo ta modul, imajo omogočen prenos prijave.

2.1 KONCEPTI VARNOSTNE SHEME

Za razvijalce, ki bodo svojo rešitev integrirali z Varnostno shemo je ključno poznavanje osnovnih entitet v Varnostni shemi:

- Uporabniki
    - Certifikati
- Krovne aplikacije
    - Aplikacije
        - Vloge
        - Skupine pravic
        - Pravice
- Tipi organizacij
    - Organizacije
- Kandidati

2.1.1 Aplikacije, vloge in pravice

Aplikacije se delijo v krovne in podrejene. Pod eno krovno aplikacijo se združijo sorodne aplikacije. Vsaka aplikacija ima lahko definirane razne pravice, ki urejajo možnosti uporabnikov pri delu s to aplikacijo. Pravice so grupirane v skupine pravic. Vloge so skupek pravic, ki se lahko dodelijo uporabnikom. Vloga pripada določeni aplikaciji in vsebuje izbrane pravice ali skupine pravic te aplikacije. Če vloga pripada krovni aplikaciji, lahko vsebuje tudi pravice podrejenih aplikacij.

Krovno aplikacijo lahko ustvari vrhovni nadzornik VS, podrejene pa tudi nadzornik krovne aplikacije.

2.1.2 Oraganizacije in tipi oraganizacij

V VS so vpisani tipi organizacij in organizacije teh tipov. Tipe in organizacije lahko vpisujejo nadzorniki VS.

2.1.3 Uporabniki, vloge in organizacije

Uporabnikom se lahko dodelijo vloge. Posamezna vloga se načeloma podeli za določeno organizacijo (npr. vloga »Nadzornik_organizacije« za organizacijo »Upravna enota Celje«), za katero potem veljajo te pravice. Nekatere vloge pa se ne navezujejo na organizacije, zato je možno tudi dodeliti vlogo uporabniku brez izbrane organizacije. Vloga se uporabniku lahko dodeli:

- ročno s strani nadzornika v spletnem vmesniku VS
- uporabniku se avtomatsko podelijo vlog
- uporabnik odda prošnjo za dodelitev pravic na spletnem vmesniku VS (v tem primeru je določitev organizacije obvezna)
- aplikacija odda prošnjo za dodelitev pravic uporabniku prek WS (metoda *FirstLogin* ali *submitUserRegistrationRequest*)

Zadnja dva primera oddata prošnjo, katero potrdi ali zavrne nadzornik v VS.

3 INTEGRACIJA SPLETNIH APLIKACIJ PREKO SSO

Spletna aplikacija, ki želi uporabljati SSO (single sign-on) rešitev od Varnostne sheme, lahko izbira med tremi programskimi vmesniki. Prvi je podmnožica protokola CAS 2.0 z nekaj razširitvami, drugi pa zelo podoben postopek, ki poteka preko spletnih storitev (*web service*). Tretji (UserInfo) je od omenjenih neodvisna spletna storitev, ki aplikacijam omogoča poizvedovanje po podatkih uporabnikov in njim dodeljenih vlog in pravicah ter vpis prošenj za dodelitev pravic/vlog uporabniku. Aplikacija lahko uporabi enega ali drugega ali jih kombinira, odvisno o zahtev in okoliščin. Posamezni postopki so opisani v nadaljevanju.

3.1 PREDPOGOJI NA VARNOSTNI SHEMI

Preden lahko aplikacija začne uporabljati SSO Varnostne sheme (v nadaljevanju VS), je potrebno izpolniti nekaj pogojev, ki so opisani v sledečem besedilu.

3.1.1 Registracija aplikacije v VS

Pred uporabo SSO s strani aplikacije je potrebno le to registrirati v VS, kar opravi vrhovni nadzornik na VS (MJU) ali nadzornik (krovne) aplikacije, ki je lahko npr. razvijalec ali skrbnik aplikacije.

Ključen podatek za vpis nove aplikacije v VS in ga pripravi razvijalec aplikacije je servisni URL (v smislu CAS protokola). Vpiše se v obliki *regex* vzorca. V različnih načinih komunikacije z VS le ta primerja dejansko uporabljen servisni URL (parameter *service*, ki ga kot URL parameter pošlje aplikacija) z vzorcem in tako identificiral aplikacijo. Primerjava ne upošteva razlik med velikimi in malimi črkami (case-insensitive). Uporaba vzorca omogoči, da lahko aplikacija po potrebi na uporabljen servisni URL pripne dodatne parametre za lastno uporabo in podobno, VS pa še vedno prepozna aplikacijo. Med postopkom prijave VS preusmeri uporabnikov brskalnik na podano vrednost servisnega URL (podrobnejši opis pod »3.2.1 CAS avtentikacija spletnih aplikacij preko spleta«).

Prav tako je v tej točki za potrebe administracije aplikacije v VS potrebno skrbniku aplikacije posredovati podatek ali bo aplikacija uporabila dodatno zaščito z uporabo gesla (izbira »Vstopno geslo«). VS namreč omogoča prijavo v aplikacije z uporabo enega ali več kvalificiranih digitalnih potrdil ter dodatno uporabo gesla. Uporaba le gesla za prijavo uporabnikov v aplikacijo, ki je integrirana na VS, ni možna.

3.1.2 Registracija sistemskega uporabnika s certifikatom

Če bo aplikacija klicala *web service* na strani VS, potrebuje za to registriranega uporabnika v VS.

Klici w*eb* service so potrebni za vse oblike postopka prijave razen po metodi »3.2.1 CAS avtentikacija spletnih aplikacij preko spleta« v primeru da je aplikacija zadovoljna s številčnim ID certifikata uporabnika kot rezultatom. To je na primer če so podatki o uporabnikih iz VS vnaprej uvoženi v aplikacijo ali so ji dostopni na kaki drug način.

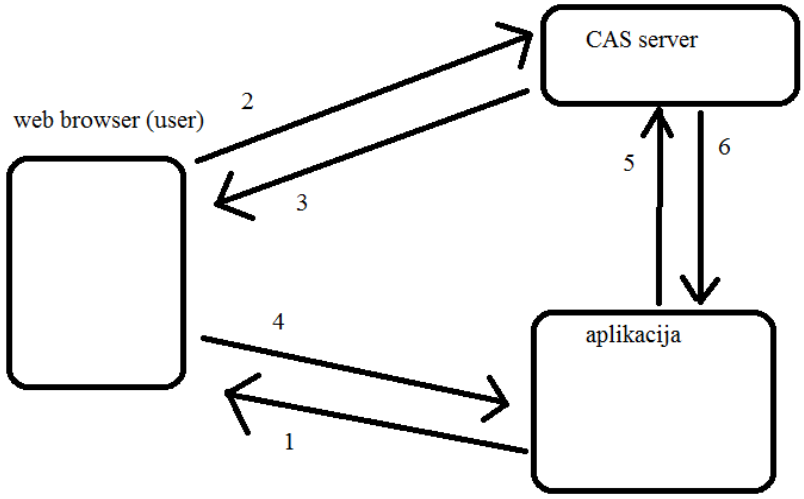
Za uporabo spletnih servisov VS se zahteva avtentikacija in avtorizacija. Za ta namen mora nadzornik (vrhovni nadzornik VS ali nadzornik aplikacije) v VS kreirati **sistemskega** uporabnika, ki se mu uvozi javni del certifikata, s katerim se bo aplikacija avtenticirala pri klicih (*HTTPS SSL/TLS client certificate*) *web service* metod. Prav tako se takemu uporabniku dodeli vloga (recimo VS_aplikacija_<ime_app>), ki omogoča dostop do podatkov o uporabnikih in organizacijah vezanih na aplikacijo.

3.2 RAZLIČNI POSTOPKI SSO

3.2.1 CAS avtentikacija spletnih aplikacij preko spleta

Aplikacija pri tem načinu za začetek postopka prijave uporabnika (pre)usmeri na naslov https://vs.gov.si/VS.web/login?service=*{servisni URL}*. Varnostna shema bo preverila ali je uporabnikovo digitalno potrdilo prijavljeno v VS. Nato bo vrnjen SSO žeton s katerim bo aplikacija lahko pridobila podatke o uporabniku in njegove pravice na tej aplikaciji. Vrednost žetona se bo aplikaciji vrnila preko redirecta na *{servisni URL}*.

V primeru, ko certifikat še ni prijavljen v VS, bo VS najprej poskusila prirediti certifikat obstoječemu uporabniku na podlagi uporabnikove davčne številke. Za podrobnosti glej poglavje »Prepoznava in prirejanje neznanih certifikatov«. Če se certifikat uspešno poveže z obstoječim uporabnikom, se naredi, kot da je certifikat bil že prej znan (postopek v prejšnjem odstavku). V nasprotnem primeru se bo prikazala stran za prvo prijavo (prošnja za dodelitev pravic), kjer bo lahko uporabnik vnesel svojo kandidaturo za uporabo aplikacij registriranih v VS. Po potrditvi kandidature s strani skrbnika aplikacije bo prijava v naslednjem poskusu potekala na zgoraj opisan način.



Slika 1. Postopek SSO CAS avtentikacije aplikacije preko spletnih strani

Podrobnejši opis korakov za izvedbo postopka SSO CAS avtentikacije v spletnih aplikacijah preko spletnih strani:

1. Aplikacija (pre)usmeri (redirect) uporabnika na spletni naslov CAS login (https://vs.gov.si/VS.web/login?service=https%3A%2F%2Fapp.example.com%2Fimpl%2Fapp1%2FprijavaReturn), pri čemer poda kot parameter svoj servisni URL, ki služi kot identifikacija aplikacije za VS ter obenem URL kamor se bo preusmeril uporabnik po uspešni prijavi.
2. Uporabnik se identificira na prijavni spletni strani VS s svojim certifikatom in po potrebi (odvisno od nastavitev za aplikacijo v VS) z vpisom svojega gesla. Če je že avtenticiran (s kako prejšnjo prijavo), VS ne bo zahtevala ponoven vpis gesla ampak bo nadaljevala postopek z naslednjo točko.
3. Po uspešni avtentikaciji uporabnika na strani VS se uporabnik preusmeri na podan servisni URL z dodanim parametrom *ticket* (*service ticket*, žeton): https://app.example.com/impl/app1/prijavaReturn?ticket=ST-1-0MiOi5JeHcdheqLCmC4f-vs.gov.si (oblika *service ticket*-a je v skladu s CAS)

   V tem koraku se na uporabnikov brskalnik shrani tudi *ticket-granting cookie*, ki mu omogoči avtomatsko prijavo na aplikacije, brez ponovnega vnašanja gesla.

4. Uporabnikov brskalnik zahteva od aplikacije dokument za URL iz prejšnje točke.
5. Aplikacija prejeti *service ticket* iz URL validira na CAS serverju s klicem URL https://vs.gov.si/VS.web/serviceValidate?service=https%3A%2F%2Fapp.example.com%2Fimple%2Fapp1%2FprijavaReturn&ticket=ST-1-0MiOi5JeHcdheqLCmC4f-vs.gov.si

   Vrednost parametra *service* mora biti enaka vrednosti iz prve točke!
6. VS vrne kot response XML datoteko, ki predstavlja uspešno/neuspešno avtentikacijo. V primeru, da je le-ta uspešna, vsebuje na primer *<cas:user>12345</cas:user>,* v celoti:

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
    <cas:authenticationSuccess>
        <cas:user>${certificate.id}</cas:user>
    </cas:authenticationSuccess>
</cas:serviceResponse>
```

   ${certificate.id} predstavlja identifikator za uporabnika, je celo število. Bolj točno, gre za ID številko uporabnikovega certifikata, ki ga je uporabil za prijavo. Med certifikati in uporabniki velja relacija N:1, t.j. en uporabnik ima lahko več certifikatov. V primeru neuspešne validacije je odgovor XML z vsebino:

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
  <cas:authenticationFailure code='INVALID_TICKET'>
         ticket not recognized
  </cas:authenticationFailure>
</cas:serviceResponse>
```

   V obeh primerih aplikacija odgovori na HTTP zahtevo uporabnika iz točke 4 (npr. vrne spletno stran z besedilom »uspešno ste se prijavili« oziroma »prijava ni uspela«).

S tem je prijava zaključena. Velja opomniti, da je protokol CAS namenjen samo za avtentikacijo in ne tudi avtorizacijo (preverjanje vlog/pravic), ki jo je potrebno v tem primeru reševati drugače. Če aplikacija potrebuje še druge podatke o uporabniku, je potrebno le-te pridobiti s kakim drugim postopkom (npr. batch import) ali preko spletnega servisa *vsAdmin* ali *UserInfo*, kot opisano spodaj. Lahko pa se uporabi tudi kombinirana metoda opisana v točki »3.2.3 Kombiniran postopek – CAS avtentikacija aplikacij preko spleta in spletnih storitev«.

Podatke o uporabniku lahko aplikacija preprosto pridobi z metodo *getUserInfo* storitve UserInfo ali z zaporedjem klicev naslednjih metod storitve vsAdmin, ki je starejša in bolj zapletena možnost:

- ***listCertificate:*** vhodni parameter je en element EntityFilter z fieldName="certificateId" in fieldValue="<id iz CAS metode serviceValidate>"

  vrne se polje (array) z enim objektom tipa *Certificate*, ki vsebuje med drugim podatek *userId*
- ***listUser:*** vhodni parameter je en element EntityFilter z fieldName="userId" in fieldValue="<id iz WS metode listCertificate>"

  vrne se polje (array) z enim objektom tipa *User*, ki vsebuje podatke uporabnika (ime, email), razen spiska vlog (element *roles*)
- ***listAllUserRoleNames:*** vhodni parameter sta dva elementa EntityFilter z fieldName="userId" in fieldValue="<id iz WS metode listCertificate>" ter z fieldName="applicationId" in fieldValue="<id aplikacije>". Id aplikacije pove, vloge od katere aplikacije zanimajo klicatelja. To bo ponavadi aplikacija, ki izvaja klic. Vrednost id se dodeli pri registraciji aplikacije v VS (glej odstavek »Registracija aplikacije v VS«).

  vrne se polje (array) z objekti tipa String, ki so imena vlog, ki so dodeljena uporabniku.

3.2.2 CAS avtentikacija aplikacij preko spletnih storitev

Ta način je podoben prej opisanemu s to razliko, da se vsa komunikacija med aplikacijo in VS odvija preko spletnih storitev, uporabnik (oziroma njegov spletni brskalnik) pa ne pride v stik z VS. Potek in logika sta sicer enaka. Spletna storitev je UserLogin (glej poglavje »Vmesnik spletne storitve VS za aplikacije - UserLogin«).

Pregled postopka prijave uporabnika po korakih:

1. Aplikacija ugotovi da uporabnik še ni prijavljen, pridobi njegov certifikat in po potrebi še geslo, nato izvede klic metode *AutenticateUser* in poda uporabnikov certifikat, svoj servisni URL ter po potrebi geslo. Pri tem aplikacija dobi nazaj SSOToken, ki vsebuje *granting ticket*.
2. Aplikacija z dobljenim *granting ticket*-om SSOToken pokliče metodo *GrantUserService* in poda dva parametra: servisni URL ter prej dobljeni SSOToken. Kot rezultat dobi nov SSOToken, ki predstavlja *service ticket.*
3. Aplikacija preko *GetValidatedUserInfo* (ali *GetValidatedUserInfo2*) in parametrov servisni URL (*service*) ter service ticket (*token*) potrdi service ticket in kot rezultat dobi User objekt, ki vsebuje vse potrebne podatke o prijavljenem uporabniku (podatki o uporabniku samem, kot tudi spisek dodeljenih mu vlog od aplikacije).
4. Za logout se poklice metoda *LogoutUser* s parametrom granting ticket.

Ta način avtentikacije je primeren za tiste aplikacije, ki ne želijo svojih uporabnikov preusmerjati na stran od Varnostne sheme in nazaj na aplikacijo. Uporabnik na ta način ne zapusti okolja aplikacije, kjer želi opraviti neko storitev ipd.

Če aplikacija za svoje potrebe ne uporablja pravice definirane v sistemu VS ampak upošteva le vloge (torej na VS se za aplikacijo definirajo vloge, brez da bi vsebovale pravice), potem se naj uporabi metoda *GetValidatedUserInfo2*, ker metoda *GetValidatedUserInfo* vrača le spisek efektivno dodeljenih pravic uporabniku, ki jih v takih primerih ni.

3.2.3 Kombiniran postopek – CAS avtentikacija aplikacij preko spleta in spletnih storitev

Možna pa je tudi kombinacija opisanih postopkov avtentikacije in sicer se postopek avtentikacije preko spleta (3.2.1 CAS avtentikacija spletnih aplikacij preko spleta) uporabi od začetka do vključno točke 4 in se potem namesto *serviceValidate* kliče metoda *getValidatedUserInfo* (ali *GetValidatedUserInfo2*) spletnega servisa UserLogin (točka 3 iz 3.2.2 CAS avtentikacija aplikacij preko spletnih storitev).

4 VMESNIK SPLETNE STORITVE VS ZA APLIKACIJE - USERLOGIN

Na strani VS je za potrebe integracije novih aplikacij v VS implementiran spletni servis za pridobivanje podatkov o uporabnikih in njegovih pravicah: **UserLogin**.

Klicatelj se avtenticira s svojim certifikatom (*HTTPS SSL/TLS client certificate*), ki mora biti registriran v VS (glej odstavek »3.1.2 Registracija sistemskega uporabnika s certifikatom«).

Metode, ki jih ponuja spletna storitev, so opisane v interni dokumentaciji.

5 VMESNIK SPLETNE STORITVE ZA ADMINISTRACIJO UPORABNIKOV – VSADMIN

Na strani VS je implementirana spletna storitev, ki je namenjena administraciji VS preko drugih aplikacij. Ta spletni servis se za integracijske namene aplikacij praviloma ne uporablja in je zgolj na voljo v primeru, če bi neka aplikacija morala izvajati tudi "naprednejše" operacije, kot so dodajanje in spreminjanje uporabnikov, organizacij in podobno.

Metode, ki jih ponuja spletna storitev, so opisane v interni dokumentaciji.

6 VMESNIK SPLETNE STORITVE USERINFO

Spletna storitev *UserInfo* omogoča z metodo *getUserInfo* poizvedovanje po podatkih določenega uporabnika za potrebe integriranih aplikacij, z metodo *submitUserRegistrationRequest* pa registracijo novega uporabnika oziroma oddajo prošnje za dodelitev pravic. Klicatelj se avtenticira s svojim certifikatom (*HTTPS SSL client certificate*), ki mora biti registriran v VS (glej »3.1.2 Registracija sistemskega uporabnika s certifikatom«).

Vhodni in izhodni parametri metod so opisani v interni dokumentaciji.

6.1 METODA GETUSERINFO

Metoda *getUserInfo* prejme kot vhodne parametre identifikacijo uporabnika, o katerem se poizveduje, ter aplikacije za katero se iščejo podatki. Izhodni parametri so podatki o uporabniku ter spisek mu dodeljenih vlog (iz nabora vlog specificirane aplikacije). Vrnjeni so samo podatki, do katerih ima klicatelj dostop (na podlagi njemu dodeljenih vlog oziroma pravic v VS). Bolj podrobno: Iskani uporabnik ima vlogo (eno ali več) iz specificirane aplikacije in klicatelj ima pravice nad to aplikacijo oziroma organizacijo, na katero se veže uporabnikova vloga.

6.2 METODA SUBMITUSERREGISTRATIONREQUEST

Metoda omogoča funkcionalnost začetka postopka registracije novega uporabnika v smislu poglavja Vložitev prošnje za dodelitev pravic iz metode *FirstLogin*, poglavje »Vmesnik spletne storitve VS za aplikacije - UserLogin«.

Klic metode zapiše v VS podatke o novem uporabniku/kandidatu (davčna številka, ime, priimek, email naslov in opcijsko telefonska številka) ter vlogah, ki bi jih naj imel. V primeru, da v VS kandidat z enako DŠ že obstaja, se obstoječemu le dodajo podane vloge (če že ne obstajajo tudi). Vloge se podajajo v parih (vloga, organizacija).

6.3 PRIMERI KLICEV METODE GETUSERINFO

Sledi nekaj primerov klicev metode *getUserInfo* storitve UserInfo.

Uspešen klic z davčno številko (podana je davčna številka uporabnika in servisni URL aplikacije NM.web):

- klic:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:user="http://userinfo.vs.mju.si/">
   <soapenv:Header />
   <soapenv:Body>
      <user:getUserInfo>
         <userIdentifier>
            <idName>TAX_NUMBER</idName>
            <idValue>12347890</idValue>
         </userIdentifier>
         <serviceURL>https://nm-sola.gov.si:443/NM.web/j_spring_cas_security_check
         </serviceURL>
         <extraParameters>
            <idName>is_ignored</idName>
            <idValue>xxx</idValue>
         </extraParameters>
      </user:getUserInfo>
   </soapenv:Body>
</soapenv:Envelope>
```

- odgovor:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
   <soap:Body>
      <ns2:getUserInfoResponse xmlns:ns2="http://userinfo.vs.mju.si/">
         <userInfoPackage>
            <user>
               <userId>2143</userId>
               <firstname>Primernik</firstname>
               <lastname>Janez</lastname>
               <phone>010001234</phone>
               <email>primer@example.org</email>
               <isSystem>true</isSystem>
            </user>
            <role>
               <roleId>20</roleId>
               <roleName>AM_Monitor</roleName>
               <roleDescription>Dostop do monitor podatkov AM</roleDescription>
               <applicationId>13</applicationId>
               <applicationName>NM.web</applicationName>
               <applicationDescription>AM Nadzorni modul - web
GUI</applicationDescription>
               <applicationParentId>10</applicationParentId>
               <organizationUnit>
                  <organizationUnitId>1000</organizationUnitId>
                  <orgUnitTypeId>1000</orgUnitTypeId>
                  <orgUnitTypeName>Javna uprava</orgUnitTypeName>
                  <orgUnitTypeDescription>Javna uprava</orgUnitTypeDescription>
                  <orgUnitName>Ministrstvo za javno upravo</orgUnitName>
                  <taxId>80696937</taxId>
                  <registrationNumber>2041421000</registrationNumber>
                  <address>Tržaška 21</address>
                  <postCity>1000 Ljubljana</postCity>
               </organizationUnit>
               <permission>
                  <permissionId>51</permissionId>
                  <permissionName>AM_Monitor</permissionName>
```

```
                <permissionDescription>Pravica za AM_Monitor</permissionDescription>
                <applicationId>13</applicationId>
                <applicationName>NM.web</applicationName>
                <applicationDescription>AM Nadzorni modul - web
GUI</applicationDescription>
                <applicationParentId>10</applicationParentId>
             </permission>
          </role>
       </userInfoPackage>
    </ns2:getUserInfoResponse>
 </soap:Body>
</soap:Envelope>
```

Uspešen klic z davčno številko – VS_API_LEVEL 1 (podana je davčna številka uporabnika in servisni URL aplikacije NM.web ter VS_API_LEVEL 1, kar povzroči vrnitev tudi podatka User.taxID):

- klic:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:user="http://userinfo.vs.mju.si/">
   <soapenv:Header />
   <soapenv:Body>
      <user:getUserInfo>
         <userIdentifier>
            <idName>TAX_NUMBER</idName>
            <idValue>12347890</idValue>
         </userIdentifier>
         <serviceURL>https://nm-sola.gov.si:443/NM.web/j_spring_cas_security_check
         </serviceURL>
         <extraParameters>
            <idName>VS_API_LEVEL</idName>
            <idValue>1</idValue>
         </extraParameters>
      </user:getUserInfo>
   </soapenv:Body>
</soapenv:Envelope>
```

- odgovor:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
   <soap:Body>
      <ns2:getUserInfoResponse xmlns:ns2="http://userinfo.vs.mju.si/">
         <userInfoPackage>
            <user>
               <userId>2143</userId>
               <firstname>Primernik</firstname>
               <lastname>Janez</lastname>
               <taxID>12347890</taxID>
               <phone>010001234</phone>
               <email>primer@example.org</email>
               <isSystem>true</isSystem>
            </user>
            <role>
               <roleId>20</roleId>
               <roleName>AM_Monitor</roleName>
               <roleDescription>Dostop do monitor podatkov AM</roleDescription>
               <applicationId>13</applicationId>
               <applicationName>NM.web</applicationName>
               <applicationDescription>AM Nadzorni modul - web
GUI</applicationDescription>
```

```
                <applicationParentId>10</applicationParentId>
                <organizationUnit>
                   <organizationUnitId>1000</organizationUnitId>
                   <orgUnitTypeId>1000</orgUnitTypeId>
                   <orgUnitTypeName>Javna uprava</orgUnitTypeName>
                   <orgUnitTypeDescription>Javna uprava</orgUnitTypeDescription>
                   <orgUnitName>Ministrstvo za javno upravo</orgUnitName>
                   <taxId>80696937</taxId>
                   <registrationNumber>2041421000</registrationNumber>
                   <address>Tržaška 21</address>
                   <postCity>1000 Ljubljana</postCity>
                </organizationUnit>
                <permission>
                   <permissionId>51</permissionId>
                   <permissionName>AM_Monitor</permissionName>
                   <permissionDescription>Pravica za AM_Monitor</permissionDescription>
                   <applicationId>13</applicationId>
                   <applicationName>NM.web</applicationName>
                   <applicationDescription>AM Nadzorni modul - web
GUI</applicationDescription>
                   <applicationParentId>10</applicationParentId>
                </permission>
             </role>
          </userInfoPackage>
       </ns2:getUserInfoResponse>
    </soap:Body>
</soap:Envelope>
```

6.4 PRIMERI KLICEV METODE SUBMITUSERREGISTRATIONREQUEST

Sledijo primeri klicev metode submitUserRegistrationRequest.

Uspešen klic (podani so obvezni podatki za kandidata in dve želeni vlogi):

- klic:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
       xmlns:user="http://userinfo.vs.mju.si/">
       <soapenv:Header />
       <soapenv:Body>
             <user:submitUserRegistrationRequest>
                   <userIdentifier>
                         <idName>TAX_NUMBER</idName>
                         <idValue>22334466</idValue>
                   </userIdentifier>
                   <userRole>
                         <organizationUnitId>1020</organizationUnitId>
                         <roleId>10</roleId>
                   </userRole>
                   <userRole>
                         <organizationUnitId>991720</organizationUnitId>
                         <roleId>10</roleId>
                   </userRole>
                   <extraParameters>
                         <idName>USER_FIRST_NAME</idName>
                         <idValue>test01</idValue>
                   </extraParameters>
```

```
                    <extraParameters>
                          <idName>USER_LAST_NAME</idName>
                          <idValue>Testen</idValue>
                    </extraParameters>
                    <extraParameters>
                          <idName>USER_EMAIL</idName>
                          <idValue>testing@example.org</idValue>
                    </extraParameters>
              </user:submitUserRegistrationRequest>
       </soapenv:Body>
</soapenv:Envelope>
```

- odgovor:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
   <soap:Body>
      <ns2:submitUserRegistrationRequestResponse xmlns:ns2="http://userinfo.vs.mju.si/">
         <candidateId>993841</candidateId>
      </ns2:submitUserRegistrationRequestResponse>
   </soap:Body>
</soap:Envelope>
```

7 SAML 2.0 VMESNIK ZA POTREBE NAPREDNE AVTENTIKACIJE IN AVTORIZACIJE

7.1 PODPORA STANDARDOM

Varnostna shema podpira tudi SAML 2.0 protokol. Implementirani vmesniki s katerimi je mogoče uporabnika avtenticirati in avtorizirati so naslednji:

- WS Trust 1.3

Varnostna shema za podporo SAML 2.0, WS Trust 1.3 uporablja JBoss komponento PicketLink. Komponenta skrbi za manipulacijo podatkov posameznih standardov. Varnostna shema se povezuje s PicketLink knjižnico preko predvidenih vmesnikov, ki skrbijo za pridobivanje podatkov o uporabniku vključno z njegovimi pravicami.

7.2 VMESNIKI

7.2.1 WS-Trust 1.3 in SAML 2.0

Za potrebe avtorizacije in avtentikacije web servisov se lahko za integracijo z Varnostno shemo uporabi WS-Trust 1.3 in je implementiran po specifikaciji http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html. Uporabnik pred klicem web servisa pokliče spletni servis WS-Trust na Varnostni shemi, ki mu nato vrne podpisan SAML 2.0 response. Vsebina SAML 2.0 vsebuje identifikacijo uporabnika, ter njegove pravice (permissions).

Parametri zahtevka so:

client certificate	Certifikat uporabljen identifikacijo klienta, ki je klicala metodo spletne storitve, na nivoju SSL/TLS (client certificate) Se uporabi z identifikacijo uporabnika, razen če je v zahtevku podan tudi parameter *OnBehalfOf*.

AppliesTo/ EndpointReference/ Address (obvezen)	Identifikacija aplikacije, na katero se nanaša zahtevek, v obliki servisnega URL. Vrnile se bodo le pravice in vloge uporabnika za podano aplikacijo.
OnBehalfOf/ UsernameToken/ Username (neobvezen) UsernameToken Id je lahko "TAX_NUMBER" ali "CLIENT_CERT"	Če je podan, se podatki vrnejo za uporabnika s podano davčno številko (v primeru Id="TAX_NUMBER") oziroma za uporabnika, ki je v VS registriran s podanim certifikatom (v primeru Id=" CLIENT_CERT"; parameter mora biti base64 kodiran javni certifikat).

V odgovoru so naslednji atributi uporabnika:

taxNumber	Davčna številka uporabnika.
email	Naslov elektronske pošte uporabnika.
name	Priimek in ime uporabnika, ločena s presledkom.
permission	Spisek pravic uporabnika. (samo imena pravic - PermissionName)
role	Spisek vlog uporabnika. (samo imena vlog - RoleName)

roleOnOrgs	Spisek vlog uporabnika s spiskom organizacij, za katere so te vloge dodeljene oziroma veljavne.
	Za vsako vlogo je vrnjen atribut oblike, primer:
	`<Role roleName="AM_Referent" roleId="10">`
	`<Organization>1021</Organization>`
	`<Organization>1021</Organization>`
	`<Organization>1021</Organization>`
	`</Role>`

permissionOnOrgs	Spisek pravic uporabnika s spiskom organizacij, za katere so te pravice dodeljene oziroma veljavne.
	Za vsako pravico je vrnjen atribut oblike, primer:
	`<Permission permissionName="ENQUIRY_ORGUNIT_VIEW" permissionId="10">`
	`<Organization>1021</Organization>`
	`<Organization>1000</Organization>`
	`</Permission>`

Primer SAML zahtevka brez parametra OnBehalfOf:

- klic:

```
<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header />
    <soap:Body>
        <wst:RequestSecurityToken
            xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512" Context="default-context">
            <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
            <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
            <wst:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey</wst:KeyType>
            <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
                <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
                    <wsa:Address>https://am-test.gov.si:443/AM.web/j_spring_cas_security_check</wsa:Address>
                </wsa:EndpointReference>
```

```
            </wsp:AppliesTo>
         </wst:RequestSecurityToken>
      </soap:Body>
</soap:Envelope>
```

- odgovor:

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
   <env:Header/>
   <env:Body>
      <wst:RequestSecurityTokenResponseCollection xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
         <wst:RequestSecurityTokenResponse Context="default-context">
            <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
            <wst:Lifetime>
               <wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">2015-12-02T16:26:43.111Z</wsu:Created>
               <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">2015-12-03T16:26:43.111Z</wsu:Expires>
            </wst:Lifetime>
            <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
               <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
                  <wsa:Address>https://am-test.gov.si:443/AM.web/j_spring_cas_security_check</wsa:Address>
               </wsa:EndpointReference>
            </wsp:AppliesTo>
            <wst:KeySize>128</wst:KeySize>
            <wst:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey</wst:KeyType>
            <wst:RequestedSecurityToken>
               <saml:Assertion ID="ID_b0fd0f6b-9402-4c03-916e-e5c2dfb31ccd" IssueInstant="2015-12-02T16:26:43.111Z"
Version="2.0" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml:Issuer>VS-STS</saml:Issuer>
                  <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
                     <dsig:SignedInfo>
                        <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments"/>
                        <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <dsig:Reference URI="#ID_b0fd0f6b-9402-4c03-916e-e5c2dfb31ccd">
                           <dsig:Transforms>
                              <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                              <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                           </dsig:Transforms>
                           <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                           <dsig:DigestValue>bktjfdLqN1Qby5Up093Mw6UIDgg=</dsig:DigestValue>
                        </dsig:Reference>
                     </dsig:SignedInfo>

<dsig:SignatureValue>jllRp3AL+QeEJJy/mZpcN6avfN31t97CR253Wm+005hEMjLBfV+PgsTp27ohWVYtDvJFOtVMNNlZ+lvi/ZNjjxvKoRWLZeHAd
uxqZqqhM+HtG0KiCfhuN7ZOXdL2Qtzh8W1eURGgmzff72IWCDqku5bTMreTRT5rIAyYeLhjW5k=</dsig:SignatureValue>
                     <dsig:KeyInfo>
                        <dsig:KeyValue>
                           <dsig:RSAKeyValue>

<dsig:Modulus>reZRBVj/a/GYfMhxNh8JPEowCpc8Zflstekf1fUH96MW4z39avCMKS50qDJC3dqEnXXA9CfS8dFcHP03xWXbh1Ax0yYSAWn/7iSoMkzy
hd5goK3NoJGOjvUaUd6gSc3pZcJYSlhAYseiUQdc7fzVR4rB1VlCXxevwi4wRXSbbZ0=</dsig:Modulus>
                              <dsig:Exponent>AQAB</dsig:Exponent>
                           </dsig:RSAKeyValue>
                        </dsig:KeyValue>
                     </dsig:KeyInfo>
                  </dsig:Signature>
                  <saml:Subject>
                     <saml:NameID NameQualifier="urn:picketlink:identity-federation">56458956</saml:NameID>
                     <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
                        <saml:SubjectConfirmationData>
                           <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                              <ds:X509Data>

<ds:X509Certificate>MIIFZTCCBE2gAwIBAgIEQLLkNTANBgkqhkiG9w0BAQUFADA+MQswCQYDVQQGEwJzaTEbMBkGA1UE
ChMSc3RhdGUtaW5zdGl0dXRpb25zMRIwEAYDVQQLEwlzaXRlc3QtY2EwHhcNMTEwNjA3MDcyNTQ1
WhcNMTYwNjA3MTQ1MTIzWjCBhzELMAkGA1UEBhMCc2kxGzAZBgNVBAoTEnN0YXRlLWluc3RpdHV0
aW9uczESMBAGA1UECxMJU0lURVNULUNBMRkwFwYDVQQLExBjZXJ0aWZpY2F0ZXMtd2ViMSwwFAYD
VQQDEw1NSlUgVk5hbU1hdGVqMBQGA1UEBRMNMTA2MjAxMTAwMDAwMjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAOEYOTM0BKuyFujCy203cEzOgz+gITSTfnY9EBR7LO2/5tUUatW55Cbb
U1zd1uZ6T/neqmn/Bha6ssexLIcSgav4UiSWfrUJzqsvw1paxvs8KwR2wu9W+aGYH9+Fka8kBRQW
GonTqW1rwTocmxlut3DmZL9h2d1U/rq91Cahg05PfJwMbpQwxNA0F0WjYQH/MRStYN+aqveRouCN
Nn65+8J1/kTkT6xYx/j485AkCSM84EV5AAhS58pV/GB9kB28wb689GwQBXMtv++1FCSq7+SLeKX2
tRlUCZ23nPHW/rdRn2lmH4aGTG9G5mmWFcpchGNbm5a1exhglvGGmsmDlBkCAwEAAaOCAh8wggIb
MA4GA1UdDwEB/wQEAwIFoDBLBgNVHSAERDBCMDYGCysGAQQBr1kCAQECMCcwJQYIKwYBBQUHAgEW
GWh0dHA6Ly93d3cuY2EuZ292LnNpL2Nwcy8wCAYGBACLMAECMBgGCCsGAQUFBwEDBAwwCjAIBgYE
AI5GAQEwFgYDVR0RBA8wDYELdGVzdEBnb3Yuc2kwgfYGA1UdHwSB7jCB6zBVoFOgUaRPME0xCzAJ
BgNVBAYTAnNpMRswGQYDVQQKExJzdGF0ZS1pbnN0aXR1dGlvbnMxEjAQBgNVBAsTCXNpdGVzdC1j
YTENMAsGA1UEAxMEQ1JMMzCBkaCBjqCBi4ZYbGRhcDovL3g1MDAuZ292LnNpL291PXNpdGVzdC1j
YSxvPXN0YXRlLWluc3RpdHV0aW9ucyxjPXNpP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFz
ZYYvaHR0cDovL3d3dy5zaWdlbi1jYS5zaS9jcmwvc2l0ZXN0L3NpdGVzdC1jYS5jcmwwKwYDVR0Q
BCQwIoAPMjAxMTA2MDcwNzI1NDVagQ8yMDE2MDYwNzE0NTEyM1owHwYDVR0jBBgwFoAUVEkHRofP
HYmdyq5yp6igoGm3IecwHQYDVR0OBBYEFNd6/zl01x25DvPAMrZoU8pAdHs1MAkGA1UdEwQCMAAw
GQYJKoZIhvZ9B0EABAwwChsEVjcuMQMCA6gwDQYJKoZIhvcNAQEFBQADggEBADo6NK+OzLoNnpPr
1T7qt7q4T1aLyH/WV1/uQt8UXb0vqNWdLeTI6fQNiPRgJ+ugGK1pRNMSEsqBy2EC18CqMK23mWuP
PYgt8BkEkfVr1SfOrMGvgH7AsmsI70EHqS+ah1E3fwFz8nCPd0f/Aw8Nhql247FPRc0HanqhykIs
YqMPHONKsEVZrZ8MMX+H2JNDOp4QuFsEb7vjA5wbGlsNPvTjcH6VYlTkoQzy09EtF1hg79+pPKKr
TpgxkMQKFSG9RVgYzihBNCcU2dUQYJFzet+JGykrCNfuXQnrRvmUdWBQ4YqMpYoodtxBUomRAd2f
```

```
ZBnJxEpYZuqdK2AXiZylSD8=</ds:X509Certificate>
                              </ds:X509Data>
                           </ds:KeyInfo>
                        </saml:SubjectConfirmationData>
                     </saml:SubjectConfirmation>
                  </saml:Subject>
                  <saml:Conditions NotBefore="2015-12-02T16:26:43.111Z" NotOnOrAfter="2015-12-03T16:26:43.111Z">
                     <saml:AudienceRestriction>
                        <saml:Audience>https://am-test.gov.si:443/AM.web/j_spring_cas_security_check</saml:Audience>
                     </saml:AudienceRestriction>
                  </saml:Conditions>
                  <saml:AuthnStatement AuthnInstant="2015-12-02T16:26:43.111Z">
                     <saml:AuthnContext>
                        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key</saml:AuthnContextClassRef>
                     </saml:AuthnContext>
                  </saml:AuthnStatement>
                  <saml:AttributeStatement>
                     <saml:Attribute Name="taxNumber">
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">56458956</saml:AttributeValue>
                     </saml:Attribute>
                     <saml:Attribute Name="email">
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">sandi@hermes.si</saml:AttributeValue>
                     </saml:Attribute>
                     <saml:Attribute Name="name">
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">VNamMatej MJU</saml:AttributeValue>
                     </saml:Attribute>
                     <saml:Attribute Name="permission">
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">ENQUIRY_ORGUNIT_EDIT</saml:AttributeValue>
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">ENQUIRY_ORGUNIT_VIEW</saml:AttributeValue>
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">VIEW_ENQUIRY_TYPE_ORGUNIT_AM</saml:AttributeValue>
                     </saml:Attribute>
                     <saml:Attribute Name="role">
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">AM_Referent</saml:AttributeValue>
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">AM_Testna_vloga</saml:AttributeValue>
                     </saml:Attribute>
                     <saml:Attribute Name="roleOnOrgs">
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><![CDATA[<Role roleName="AM_Referent"
roleId="10"><Organization>1021</Organization><Organization>1021</Organization><Organization>1021</Organization></Role>
]]></saml:AttributeValue>
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">&lt;Role roleName="AM_Testna_vloga"
roleId="2520">&lt;Organization>1000&lt;/Organization>&lt;/Role></saml:AttributeValue>
                     </saml:Attribute>
                     <saml:Attribute Name="permissionOnOrgs">
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">&lt;Permission permissionName="ENQUIRY_ORGUNIT_EDIT"
permissionId="11">&lt;Organization>1021&lt;/Organization>&lt;/Permission></saml:AttributeValue>
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><![CDATA[<Permission permissionName="ENQUIRY_ORGUNIT_VIEW"
permissionId="10"><Organization>1021</Organization><Organization>1000</Organization></Permission>]]></saml:AttributeVa
lue>
                        <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">&lt;Permission permissionName="VIEW_ENQUIRY_TYPE_ORGUNIT_AM"
permissionId="50">&lt;Organization>1021&lt;/Organization>&lt;/Permission></saml:AttributeValue>
                     </saml:Attribute>
                  </saml:AttributeStatement>
               </saml:Assertion>
            </wst:RequestedSecurityToken>
            <wst:RequestedAttachedReference>
               <wsse:SecurityTokenReference wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLV2.0" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
                  <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLID">#ID_b0fd0f6b-9402-4c03-916e-e5c2dfb31ccd</wsse:KeyIdentifier>
               </wsse:SecurityTokenReference>
            </wst:RequestedAttachedReference>
         </wst:RequestSecurityTokenResponse>
      </wst:RequestSecurityTokenResponseCollection>
   </env:Body>
</env:Envelope>
```

Primer SAML zahtevka s parametrom OnBehalfOf tipa TAX_NUMBER:

- klic:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
```

```
    <Action xmlns="http://www.w3.org/2005/08/addressing">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</Action>
    <MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:b028dda7-018f-49e6-a560-d88574fad68f</MessageID>
    <To
xmlns="http://www.w3.org/2005/08/addressing">https://ezdravje.hsl.eu:8543/VS.webservices/services/PicketLinkSTS</To>
    <ReplyTo xmlns="http://www.w3.org/2005/08/addressing">
      <Address>http://www.w3.org/2005/08/addressing/anonymous</Address>
    </ReplyTo>
  </soap:Header>
  <soap:Body>
    <wst:RequestSecurityToken xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
      <wst:SecondaryParameters>
                              <t:TokenType xmlns:t="http://docs.oasis-open.org/ws-sx/ws-
trust/200512">http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</t:TokenType>
                              <t:KeyType xmlns:t="http://docs.oasis-open.org/ws-sx/ws-
trust/200512">http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey</t:KeyType>
                              <t:KeySize xmlns:t="http://docs.oasis-open.org/ws-sx/ws-trust/200512">256</t:KeySize>
      </wst:SecondaryParameters>
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
      <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
          <wsa:Address>https://am-test.gov.si:443/AM.web/j_spring_cas_security_check</wsa:Address>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
      <wst:Renewing />
      <wst:OnBehalfOf>
        <wsse:UsernameToken xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="TAX_NUMBER">
          <wsse:Username>56458956</wsse:Username>
        </wsse:UsernameToken>
      </wst:OnBehalfOf>
    </wst:RequestSecurityToken>
  </soap:Body>
</soap:Envelope>
```

- odgovor:

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
   <env:Header>
      <Action xmlns="http://www.w3.org/2005/08/addressing">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RSTRC/IssueFinal</Action>
      <MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:3d04d8a9-f1f7-49e1-b075-
a642cd413e64</MessageID>
      <To xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/anonymous</To>
      <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:b028dda7-018f-49e6-a560-
d88574fad68f</RelatesTo>
   </env:Header>
   <env:Body>
      <wst:RequestSecurityTokenResponseCollection xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
         <wst:RequestSecurityTokenResponse>
            <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
            <wst:Lifetime>
               <wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">2015-12-02T16:22:42.017Z</wsu:Created>
               <wsu:Expires xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">2015-12-03T16:22:42.017Z</wsu:Expires>
            </wst:Lifetime>
            <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
               <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
                  <wsa:Address>https://am-test.gov.si:443/AM.web/j_spring_cas_security_check</wsa:Address>
               </wsa:EndpointReference>
            </wsp:AppliesTo>
            <wst:KeySize>256</wst:KeySize>
            <wst:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey</wst:KeyType>
            <wst:RequestedSecurityToken>
               <saml:Assertion ID="ID_68d3ebba-4779-45ba-88df-7131f25fbf91" IssueInstant="2015-12-02T16:22:42.017Z"
Version="2.0" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml:Issuer>VS-STS</saml:Issuer>
                  <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
                     <dsig:SignedInfo>
                        <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments"/>
                        <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <dsig:Reference URI="#ID_68d3ebba-4779-45ba-88df-7131f25fbf91">
                           <dsig:Transforms>
                              <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                              <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                           </dsig:Transforms>
                           <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                           <dsig:DigestValue>VpojZt1+dLO/66hOAU/rXq1lO1o=</dsig:DigestValue>
                        </dsig:Reference>
                     </dsig:SignedInfo>

<dsig:SignatureValue>ClIfkBIJdyvcP9Wcg98Na5fcJ0Bsw0YzgVJxjImf3ln50+dOoOAma7I3bHmDawgxGM5wyX8ZWdPFwvn6T/YQgOXWjafUpDG6I
cHUTUz9//4DlYVGPu3S4NOffrKlEdo8h7QfWRCCZxGJDE6p0qIM3ZkwUeZhhJoaSnoGqJkRExI=</dsig:SignatureValue>
                     <dsig:KeyInfo>
                        <dsig:KeyValue>
                           <dsig:RSAKeyValue>
```

<dsig:Modulus>reZRBVj/a/GYfMhxNh8JPEowCpc8Zflstekf1fUH96MW4z39avCMKS50qDJC3dqEnXXA9CfS8dFcHP03xWXbh1Ax0yYSAWn/7iSoMkzy
hd5goK3NoJGOjvUaUd6gSc3pZcJYSlhAYseiUQdc7fzVR4rB1VlCXxevwi4wRXSbbZ0=</dsig:Modulus>
<dsig:Exponent>AQAB</dsig:Exponent>
</dsig:RSAKeyValue>
</dsig:KeyValue>
</dsig:KeyInfo>
</dsig:Signature>
<saml:Subject>
<saml:NameID NameQualifier="urn:picketlink:identity-federation">56458956</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
</saml:Subject>
<saml:Conditions NotBefore="2015-12-02T16:22:42.017Z" NotOnOrAfter="2015-12-03T16:22:42.017Z">
<saml:AudienceRestriction>
<saml:Audience>https://am-test.gov.si:443/AM.web/j_spring_cas_security_check</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2015-12-02T16:22:42.017Z">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:cm:sender-
vouches</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="taxNumber">
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">56458956</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="email">
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">sandi@hermes.si</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="name">
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">VNamMatej MJU</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="permission">
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">ENQUIRY_ORGUNIT_EDIT</saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">ENQUIRY_ORGUNIT_VIEW</saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">VIEW_ENQUIRY_TYPE_ORGUNIT_AM</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="role">
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">AM_Referent</saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">AM_Testna_vloga</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="roleOnOrgs">
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><![CDATA[<Role roleName="AM_Referent"
roleId="10"><Organization>1021</Organization><Organization>1021</Organization><Organization>1021</Organization></Role>
]]></saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Role roleName="AM_Testna_vloga"
roleId="2520"><Organization>1000</Organization></Role></saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="permissionOnOrgs">
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Permission permissionName="ENQUIRY_ORGUNIT_EDIT"
permissionId="11"><Organization>1021</Organization></Permission></saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><![CDATA[<Permission permissionName="ENQUIRY_ORGUNIT_VIEW"
permissionId="10"><Organization>1021</Organization><Organization>1000</Organization></Permission>]]></saml:AttributeVa
lue>
<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Permission permissionName="VIEW_ENQUIRY_TYPE_ORGUNIT_AM"
permissionId="50"><Organization>1021</Organization></Permission></saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</wst:RequestedSecurityToken>
<wst:RequestedAttachedReference>
<wsse:SecurityTokenReference wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLV2.0" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd">
<wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLID">#ID_68d3ebba-4779-45ba-88df-7131f25fbf91</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
</wst:RequestedAttachedReference>
</wst:RequestSecurityTokenResponse>
</wst:RequestSecurityTokenResponseCollection>
</env:Body>
</env:Envelope>

8 VARNOST

Vse strani vpletene v komunikacijo z aplikacijo Varnostna shema morajo podpirati protokol HTTPS za vzpostavitev varne povezave med sodelujočimi informacijskimi sistemi. Uporabnik spletnega servisa se mora identificirati z veljavnim digitalnim potrdilom (certifikatom), ki je registriran v Varnostni shemi kot sistemski uporabnik. Za prenos podatkov po tako vzpostavljeni povezavi je uporabljena metoda POST.

Pri vzpostavitvi integracije s posamezno aplikacijo je potrebno izmenjati informacije o javnih ključih digitalnih potrdil, ki bodo uporabljena tako za vzpostavitev varne SSL/TLS seje (strežniška digitalna potrdila) kot za avtentikacijo klicateljev (odjemalska digitalna potrdila).

9 PREPOZNAVA IN PRIREJANJE NEZNANIH CERTIFIKATOV

V primeru, da se uporabnik poskuša prijaviti preko VS z uporabo certifikata, ki v VS še ni registriran, bo VS poskusil prirediti certifikat obstoječemu uporabniškemu računu na osnovi davčne številke, po postopku:

1. Iz certifikata se ugotovi davčna številka lastnika (različni postopki za različne overitelje)

   V primeru neuspeha se postopek prijave konča, uporabniku VS izpiše besedilo napake:

   »Vaš certifikat nima davčne številke.«

2. VS poišče v bazi uporabnikov uporabnika z enako davčno številko.

   V primeru uspeha se certifikat registrira kot certifikat najdenega uporabnika.

   Sicer se uporabnik šteje za novega/neregistriranega in se preusmeri na prošnjo za dodelitev pravic.

9.1 IZJEME (SISTEMSKI CERTIFIKATI)

V primeru da gre za certifikat informacijskih sistemov (in ne fizičnih oseb), kar se pri certifikatih overiteljev SIGEN-CA in SIGOV-CA prepozna po vzorcu serijske številke certifikata, pri SITEST-CA pa se vsi certifikata upoštevajo kot taki, se združitev z obstoječim uporabnikom na osnovi ujemanja davčne številke ne izvede. Če obstaja uporabniški račun z enako davčno številko, se pri poskusu prijave izpiše napaka:

»Združitev neregistriranega sistemskega certifikata z obstoječim uporabnikom zavrnjena.«