BANKA SLOVENIJE

EVROSISTEM

Spletna storitev BS

(Opis izmenjave za zunanje uporabnike)

infrax
informacijske tehnologije
Infrax d.o.o., Trg tigrovcev 1, SI-5220 Tolmin

November 2015

Kazalo vsebine

1. Predstavitev procesa

1.1 Identifikacija procesa

Funkcionalnosti spletne storitve se uporabljajo kot del podsistema Banke Slovenije za komunikacijo z zunanjim svetom.

1.2 Namen in cilji

Sistem omogoča prenos poljubnega paketa (xml stavki, datoteke poljubnih oblik) med zunanjim uporabnikom in aplikacijami, ki se izvajajo na Banki Slovenije, v obe smeri. V primeru xml sporočil se lahko glede na možnosti posamezne sheme zahteva uporabo digitalnega podpisa, v vsakem primeru pa je vsebina paketa lahko šifrirana in stisnjena (zip).

1.3 Omejitve

V vlogi (podrejenega) odjemalca nastopa vedno zunanji uporabnik (izvaja klice spletne storitve). Banka Slovenije nikoli ne izvaja povratnih klicev. Komunikacija poteka preko varne (SSL) seje.

2. Opis funkcionalnosti spletne storitve BS (BSB2BWS)

2.1 WSDL shema

WSDL shema omogoča izvajanje metod za pošiljanje in prevzemanje paketov, za potrditev prevzema, za preverjanje seznama prejetih in/ali poslanih paketov, preverjanje podatkov o uporabniku in o področjih, za katera je uporabnik avtoriziran.

Vsaka metoda ima definiran en vhodni in en izhodni parameter (Request in Response), ki sta kompleksna tipa, zato v nadaljevanju pišemo dejansko o več vhodnih in več izhodnih parametrih.

Shema in posledično spletna storitev je dostopna na naslovu:

https://data-test.bsi.si/test/bsb2bws/bsb2bws.asmx za testno okolje in

https://data.bsi.si/prod/bsb2bws/bsb2bws.asmx za produkcijsko okolje.

2.2 Metode BS_B2BWS

2.2.1 SendPackage (Oddaja paketa na BS)

Vhodni parametri (SendPackageRequest):

1. SenderPackageId (Enolična identifikacija paketa pošiljatelja)
2. BSPackageType (Vsebinsko področje izmenjave podatkov z BS)
3. PackageName (Naziv paketa oziroma datoteke, npr. Navodila.doc, parameter ni obvezen)

4. PackageContent (Base64 kodirana vsebina paketa – datoteke).

Izhodni parametri (SendPackageResult):

1. StatusCode
2. ErrorMessage

Vsebina obeh parametrov, ki sta obvezna elementa tipa Response je opisana v posebnem poglavju.

2.2.2 GetNewPackage (Prevzem čakajočega paketa)

Vhodni parametri:

1. BSPackageType (Vsebinsko področje izmenjave podatkov z BS, podano je opcijsko. V primeru, da je podano, potem se uporabniku vrne prvi paket iz seznama neprevzetih paketov tega področja)

Izhodni parametri (GetNewPackageResult):

1. BSPackageId (Identifikacijska številka paketa v okviru sistema BS)
2. BSPackageType (Področje izmenjave)
3. PackageName (Ime datoteke v paketu)
4. PackageContent (Base64 kodirana vsebina paketa – datoteke)
5. PackageSize (Velikost datoteke v bytih)
6. RestPackagesQuantity (Število preostalih paketov, ki še čakajo uporabnika na BS, če vpiše v vhodni parameter vsebinsko področje, potem dobi število samo za to področje)
7. StatusCode
8. ErrorMessage

2.2.3 GetPackage (Prevzem točno določenega paketa iz BS, ponovitev prevzema)

Uporabnik lahko ponovi prevzem določenega paketa, če je le-ta sploh še na voljo.

Vhodni parametri:

1. BSPackageId (Enolična identifikacija paketa, ki jo je uporabnik prejel ob prvem prevzemu paketa)

Izhodni parametri: Enaki kot pri GetNewPackage.

2.2.4 ConfirmPackage (Potrditev prevzema paketa iz BS)

1. BSPackageId (Identifikacijska številka paketa v okviru sistema BS)

Izhodni parametri (ConfirmPackageResult):

1. StatusCode
2. ErrorMessage

2.2.5 GetPackageInfo (Vrne podatke o določenem paketu)

Vhodni parametri:

1. BSPackageId (Id paketa v sistemu BS)

Izhodni parametri (GetPackageInfoResult):

1. PackageInfo (Kompleksni tip s podatki o paketu)

    - Status (V kakšnem statusu je paket na Banki Slovenije)

      OK – V redu, datoteka je bila uspešno oddana.
      OK_CONF – V redu, uporabnik je potrdil prejem datoteke.
      WAIT_SOAP – Čaka uporabnika na potrditev prejema.
      WAIT – Čaka na obdelavo s strani Banke Slovenije.
      ERROR – Prejeta datoteka ni bila uspešno obdelana.
      RECALL – Datoteka je bila preklicana s strani Banke Slovenije.

    - SubjectAreaName (Področje izmenjave)
    - SenderFingerprint (Prstni odtis digitalnega potrdila pošiljatelja, prijavljeni na spletno storitev)
    - SigningFingerprint (Prstni odtis digitalnega potrdila podpisnika)
    - EncrFingerprint (Prstni odtis digitalnega potrdila, s katerim je bil paket kriptiran)
    - SenderUsername (Ime pošiljatelja)
    - Source (Vir)

      BSORACLE Vir datoteke je podatkovna baza v BS.
      PUBLICWS Vir datoteke je spletna storitev.

    - PackageName (Naziv datoteke v paketu)
    - PackageSize (Velikost datoteke v bytih)
    - DataDateTime
    - OrganizationIdentificationNumber (Matična številka organizacije pošiljatelja)
    - ReportType (Tip poročila, kadar je za eno področje možnih več različnih poročil)

2. StatusCode
3. ErrorMessage

2.2.6 GetPackageList (Vrne seznam poslanih in/ali prejetih paketov)

Vhodni parametri (GetPackageListRequest):

1. BSPacketType
2. SentPackages (true, false, če je true, vključi pakete poslane v BS)
3. ReceivedPackages (true, false, vključi samo iz BS prejete pakete)
4. DateTimeFrom
5. DateTimeTo

Izhodni parametri (GetPackageListResult):

1. PackageList (Izhodni parameter je kompleksnega tipa, ki ga opisuje shema get_user_file_info_p_file_list.xsd. Shema se nahaja v prilogi.)
2. StatusCode
3. ErrorMessage

2.2.7 UserAuthentication (Preveri, ali je certifikat veljaven in registriran v BS)

Vhodni parametri: Jih ni.

Izhodni parametri (UserAuthenticationResult):

3. StatusCode (OK pomeni, da je uporabnik registriran na BS, UnkUser pa pomeni, da ni)
4. ErrorMessage

2.2.8 GetUserData (Vrne podatke o lastniku digitalnega potrdila)

Vhodni parametri: Jih ni.

Izhodni parametri (GetUserDataResult):

1. UserInfo (Kompleksni tip s podatki za prstni odtis potrdila uporabnika, ki kliče metodo)

    - ContactPerson (Kontaktna oseba)
    - CertEmailAddress (e poštni naslov)
    - CertValidFrom (Začetek veljavnosti digitalnega potrdila)
    - CertValidTo (Konec veljavnosti digitalnega potrdila)

2. StatusCode (OK pomeni, da je uporabnik registriran na BS, UnkUser pa pomeni, da ni)
3. ErrorMessage

2.2.9 GetUserAuthorisation (Vrne področja, za katera je uporabnik prijavljen na BS)

Vhodni parametri: Jih ni.

Izhodni parametri (GetUserAuthorisationResult):

1. SubjectAreasList (Izhodni parameter je kompleksnega tipa, ki ga opisuje shema get_authorization_p_list_subject_areas.xsd. Shema se nahaja v prilogi.)
2. StatusCode
3. ErrorMessage

2.2.10 GetSubjectArea (Vrne podatke o posameznem področju)

Vhodni parametri:

1. BSPackageType

Izhodni parametri (GetSubjectAreaResult):

1. SubjectAreaInfo (Kompleksni tip s podatki o posameznem področju)

    - SubjectAreaName (Naziv področja)
    - Certificates (Izhodni parameter je kompleksnega tipa, ki ga opisuje shema get_subject_area_info_p_certificates.xsd. Shema se nahaja v prilogi.)
    - CodeLists (Izhodni parameter je kompleksnega tipa, ki ga opisuje shema get_subject_area_info_p_code_lists.xsd. Shema se nahaja v prilogi.)
    - NeedSign (zahtevan e podpis true/false)
    - NeedEncryption (zahtevano šifriranje true/false)
    - NeedZip (zahtevano stiskanje vsebine true/false)
    - XmlSchemaName (ime XML sheme, ki ji morajo ustrezati poslani XML dokumenti)
    - XmlSchemaLocation (spletni naslov, kjer je objavljena shema)
    - TimeStart (Dnevni začetek delovanja)
    - TimeEnd (Dnevni zaključek delovanja)
    - OperatingDays (Dnevi, ko področje deluje (npr. 12345=ponedeljek do petek, 1234567=vsak dan)
    - MaxFileSize (Največja dovoljena velikost datoteke)
    - ReplyMode (Število dni od nastanka datoteke, ko jo uporabnik še lahko prevzame preko spletnih storitev)

2. StatusCode
3. ErrorMessage

2.2.11 GetCodeList (Vrne vsebino šifranta v XML strukturi)

Vhodni parametri:

1. BSPackageType
2. CodeListType (Oznaka šifranta, ki jo dobimo iz seznama šifrantov, ki se vrača pri klicu metode GetSubjectArea v parametru CodeLists)

Izhodni parametri (GetCodeListResult):

1. CodeList (Kompleksni tip s podatki v XML strukturi, ki je odvisna od vsebine posameznega šifranta. Sheme so objavljene na spletnih straneh BS za posamezno področje izmenjave.)
2. StatusCode
3. ErrorMessage

2.3 ResponseType (splošni del pri odgovorih)

Sestoji se iz dveh elementov in sicer StatusCode in ErrorMessage. Pri klicih procedur v zaledno aplikacijo za izmenjavo sporočil z zunanjim svetom se v primeru, da pride do napake, v StatusCode in ErrorMessage prepišeta koda in opis napake, ki jo javi določena zaledna procedura.

Response		Metode	Opis
StatusCode	**ErrorMessage**		
OK		Vse	Metoda (operacija) uspešno izvedena.
BS9XXXX	V polje ErrorMessage se prepiše napaka oziroma sporočila iz sistema za izmenjavo Banke Slovenije.	Vse	
UnkUser	Digitalno potrdilo uporabnika ni bilo posredovano iz varne seje.	Vse	
SignErr	Napaka pri preverjanju podpisa.	SendMessage	V ErrorMessage se doda napaka, ki jo javi procedura za preverjanje podpisa.
DecryptErr	Pri dešifriranju paketa je prišlo do napake.	SendMessage	Javi v primeru, ko je šifriranje zahtevano, pa funkcija dešifriranja ne uspe.
InternalError		Vse	Javi se, če je npr. povezava do baze ne uspe, ali pa pride do nepredvidene napake v kodi spletne storitve.
UnzipErr	Pri razširitvi (unzip) je prišlo do napake.	SendMessage	Javi se v primeru, da pride do napake pri razširitvi paketa.
Unhndl	p_err_msg	Vse	V primeru, da klic zaledne procedura na BS ne vrne oznake napake, se vpiše Unhndl in prepiše opis napake,

Spisek možnih odgovorov sistema za izmenjavo sporočil z zunanjim svetom na Banki Slovenije:

Šifra napake	Opis napake
BS-90000	Nepričakovana tehnična napaka pri: verify_authentication
BS-90001	Avtorizacija neuspešna.
BS-90002	Seja ni veljavna.
BS-90003	Seja je potekla. Ponovno se morate prijaviti.
BS-90004	Seja ni dovoljena za izbrano vsebinsko področje.
BS-90006	Neveljavno uporabniško ali geslo.
BS-90007	Vsaj eden od parametrov uporabniško ime in prstni odtis mora biti prazen.
BS-90008	Uporabnik ni avtoriziran za vsebinsko področje.
BS-90009	Poročilo je podpisano s certifikatom, ki ni avtoriziran za vsebinsko področje.
BS-90010	Poročilo ni kriptirano s certifikatom, predpisanim za vsebinsko področje.
BS-90011	Vsebinsko področje trenutno ni odprto.
BS-90350	Nepričakovana tehnična napaka pri: get_authorization
BS-90351	V podatkovni bazi ni podatkov o certifikatu.
BS-90352	V podatkovni bazi ni podatkov o seji.
BS-90450	Nepričakovana tehnična napaka pri: get_user_info
BS-90451	Uporabnik ni avtoriziran za uporabo spletnih storitev BS.
BS-90550	Nepričakovana tehnična napaka pri: get_subject_area_info
BS-90551	Vsebinsko področje ne obstaja.
BS-90552	Aplikativni certifikat ne obstaja.
BS-90601	Velikost datoteke je večja od dovoljene.
BS-90650	Nepričakovana tehnična napaka pri: insert_file
BS-90651	Zapis datoteke v bazo ni uspel, ker datoteka s to številko že obstaja.
BS-90652	Zapis datoteke v bazo ni uspel, uporabnik ni avtoriziran za izbrano vsebinsko področje.
BS-90653	Zapis datoteke v bazo ni uspel.
BS-90654	Pošiljanje datotek v BS za to vsebinsko področje ni dovoljeno.
BS-90750	Nepričakovana tehnična napaka pri: get_user_file_info
BS-90751	Pri klicu get_user_file_info manjkajo obvezni datumski parametri.
BS-90753	Podatki o datoteki niso dostopni.
BS-90850	Nepričakovana tehnična napaka pri: get_file_info
BS-90851	Datoteka ne obstaja.
BS-90852	Datoteka pripada drugemu poslovnemu subjektu.
BS-90853	Ni nobene čakajoče datoteke.
BS-90854	Nepričakovana napaka: ni bilo možno dobiti certifikata za podpisovanje.
BS-90855	Nepričakovana napaka: ni bilo možno dobiti certifikata za kriptiranje.
BS-90856	Podatki o datoteki niso dostopni.
BS-90857	Datoteka je bila preklicana.
BS-90950	Nepričakovana tehnična napaka pri: get_file
BS-91050	Nepričakovana tehnična napaka pri: confirm_packet
BS-91051	Potrditev paketa ni uspela.
BS-91052	Potrditev paketa ni uspela.
BS-91053	Potrditev paketa ni uspela. Dovoljeno je samo potrjevanje paketov, ki so poslani iz BS.

BS-91054	Potrditev paketa ni uspela, ker je bil preklican.
BS-91100	Nepričakovana napaka pri: get_user_certs
BS-91101	Uporabnik nima registriranega certifikata za izbrano področje.
BS-91150	Nepričakovana napaka pri: get_cert
BS-91200	Nepričakovana tehnična napaka pri: get_user_list
BS-91250	Nepričakovana tehnična napaka pri: get_code_list
BS-91251	Šifrant ne obstaja oz. parametri za vračanje šifranta niso pravilni.
BS-91300	Nepričakovana tehnična napaka pri: bq_soap_zi_api.send_package.
BS-91301	Datoteka se pošilja kot odgovor na prejeto datoteko, vendar se poslovni subjekt, ki mu pošiljamo odgovor, ne ujema s tistim, ki je poslal datoteko.
BS-91302	Nepričakovana napaka pri zapisovanju datoteke.
BS-91350	Nepričakovana tehnična napaka pri: bq_soap_zi_api.get_package.
BS-91351	Parametra p_file_soap_id in p_psd_sif morata biti bodisi oba prazna bodisi oba izpolnjena.
BS-91352	Nepričakovana napaka pri prevzemu datoteke.
BS-91400	Nepričakovana tehnična napaka pri: bq_soap_zi_api.confirm_package.
BS-91401	Nepričakovana napaka pri potrjevanju datoteke.
BS-91450	Nepričakovana tehnična napaka pri: get_user_sa_chunks_info.
BS-91500	Nepričakovana tehnična napaka pri: get_file_chunk.
BS-91501	Ni nobenega čakajočega koščka ali datoteke.
BS-91502	Pobiranje koščka iz baze ni uspelo.
BS-91503	Nepričakovana napaka: ni bilo možno dobiti certifikata za podpisovanje.
BS-91504	Nepričakovana napaka: ni bilo možno dobiti certifikata za kriptiranje.
BS-91550	Nepričakovana tehnična napaka pri: insert_file_chunk.
BS-91551	Zapis koščka datoteke v bazo ni uspel.
BS-91552	Nepričakovana tehnična napaka pri: ins_file_chunk.
BS-91553	Shranjevanje koščka ni uspelo, ker je ta košček že zapisan.
BS-91600	Nepričakovana tehnična napaka pri: delete_file_chunks.
BS-91601	Brisanje koščkov datoteke ni uspelo.
BS-91650	Nepričakovana tehnična napaka pri: get_file_all_chunks.
BS-91651	Za zahtevano datoteko shranjeni koščki ne obstajajo.
BS-91652	Pobiranje vseh koščkov datoteke iz baze ni uspelo.
BS-91700	Nepričakovana tehnična napaka pri: confirm_chunk.
BS-91701	Napaka pri potrjevanju koščka.
BS-91702	Nisem našel kočka za potrditev.
BS-91703	Potrjevanje koščka ni uspelo.
BS-91750	Nepričakovana tehnična napaka pri: bq_soap_zi_api.get_user_list.
BS-91751	Nepričakovana napaka pri prevzemu liste uporabnikov

3. Protokol izmenjave paketov med zunanjim uporabnikom in BS

3.1 Uvod

Za potrebe izmenjave paketov odjemalec (zunanji uporabnik) uporablja metode SendPackage, GetNewPackage (GetPackage) in ConfirmPackage.

Ostale metode, ki jih omogoča sistem so namenjene drugim poizvedbam, ki jih je možno preko spletne storitve B2B Banke Slovenije opraviti po potrebi.

3.2 Oddaja paketa

Oddaja paketa poteka s klicem metode »SendPackage«. Posamezni parametri so opisani v razdelku 2.2.1. Opozoriti velja le, da je glede na zahteve področja izmenjave podatkov, potrebno pred oddajo datoteko elektronsko podpisati, stisniti (zip) in šifrirati (kriptirati). Kaj od tega zahteva področje izmenjave lahko preverite tudi s klicem metode »GetSubjectArea« (opis v razdelku 2.2.10), ki vam poleg tega vrne tudi kriptirno digitalno potrdilo, če je kriptiranje zahtevano in shemo, po kateri mora biti pripravljen XML stavek, če je le-ta predpisana.

V kolikor nobena izmed predvidenih kontrol ne javi nobene napake, potem spletna storitev v parametru »StatusCode« vrne odgovor »OK«, sicer pa eno izmed napak opisanih v razdelku 2.3. V primeru kakršnekoli napake je potrebno oddajo paketa ponoviti. V kolikor gre za napako, za katero je kriv zunanji uporabnik (rumeno obarvane vrstice v tabelah v razdelku 2.3), je potrebno napako predhodno odpraviti.

3.3 Sprejem paketa iz BS

Prevzem paketov iz BS se izvaja s klicem metode »GetNewMessage«. Pri klicu je možno navesti, za katero vsebinsko področje se prevzema sporočila. Če na BS pod navedenim pogojem obstaja kakšno sporočilo za prevzem, ga spletna storitev v odgovoru preda odjemalcu. Parametri kompleksnega odgovora so opisani v razdelku 2.2.2. V parametru »RestPackagesQuantity« sistem hkrati s predajo paketa sporoči še, koliko paketov še čaka na Banski Slovenije pod enakimi pogoji. Če je to število več kot 0, potem je potrebno klic metode ponoviti in prevzemati ostale pakete, dokler še kakšen obstaja. Še prej pa je potrebno prevzem vsakega paketa sproti potrditi s klicem procedure »ConfirmPackage«. V kolikor namreč sistem ne prejme potrditvenega klica, potem v naslednjem koraku ponudi odjemalcu v prevzem isti paket.

V kolikor na Banki Slovenije ob sprejemu klica klicu ne obstaja noben paket, sistem odgovori s kodo »BS-90853 Ni nobene čakajoče datoteke«, potem klica ni smiselno takoj ponoviti. enako velja za primer, ko odjemalec prevzame zadnji paket in je število preostalih paketov enako 0.

4. Elektronski podpis, stiskanje in šifriranje (kriptiranje) paketov (datotek)

4.1 Uvod

Vsako področje izmenjave lahko zahteva, da je paket, ki se ga oddaja preko spletne storitve prej ustrezno pripravljen. Na isti način se pripravijo tudi paketi namenjeni prevzemu iz Banke Slovenije. Kot je bilo omenjeno že v prejšnjem razdelku, je potrebno zahteve BS za posamezno področje preveriti s klicem metode »GetSubjectArea«, za posamezna področja izmenjave pa so navadno zahteve navedene tudi na spletni strani, ki podaja tehnične informacije o področju. V skladu z navodilom, je potrebno paket pred oddajo ali podpisati, in/ali stisniti (zip) in/ali šifrirati. Zahtevane operacije se izvede točno v navedem vrstnem redu. Pri prevzemu paketa pa se po prevzemu dešifriranje, razširjanje (unzip) in preverjanje podpisa izvede v obratnem vrstnem redu. Ali odjemalec spletne storitve slednje tri operacije izvede pred »ConfirmPackage« ali za njim, je stvar njegove odločitve.

4.2 Elektronski podpis

Trenutno je podpis možno zahtevati za xml in pdf dokumente.

V kolikor je podpis zahtevan za XML dokument, je »XMLdSig« shema vključena že v osnovno XML shemo dokumenta. Več o standardu najdete na spletni strani http://www.w3.org/TR/xmldsig-core/.

Dokumenti tipa pdf se podpisujejo v skladu s standardom, ki ga zahteva priprava tovrstnih dokumentov. Več o standardu na http://www.adobe.com/devnet/pdf/pdf_reference.html.

4.3 Stiskanje (zip)

Pripravi se običajen zip arhiv z eno vsebovano datoteko. Več o tem na strani http://en.wikipedia.org/wiki/Zip_(file_format).

4.4 Šifriranje (kriptiranje)

Pričakuje se vsebina, ki je šifrirana v ovojnici po PCKS#7/CMS formatu pri čemer se uporabi 3DES šifrirni algoritem.

http://en.wikipedia.org/wiki/Cryptographic_Message_Syntax

5. Priloga: Dopolnilne XML sheme za kompleksne parametre


get_authorization_p_list_subject_areas.


get_user_file_info_p_file_list.xsd


get_subject_area_info_p_certificates.xsd


get_subject_area_info_p_code_lists.xsd