asociația română a băncilor	**CP_SCT_A_Vers_2020** **Convenția Scheme Naționale de Plăți** **SPL Anexa 6.1 Setul de Reguli privind SPL RON**	**Data aprobării:** **30.08.2020** **Data intrării în vigoare:** **01.01.2021**

Set de Reguli privind
SPL (Standardised Proxy Lookup) RON

1. Introducere

1.1 Scopul documentului

Prezentul Set de reguli privind SPL (Standardised Proxy Lookup) RON („Setul de reguli") include regulile, practicile și standardele care fac posibilă operarea, aderarea și participarea la Schema SPL RON ("Schema") și stabilește procedurile și funcționalitățile serviciului privind schimbul de informații necesare inițierii de plăți prin intermediul unor soluții de plată bazate pe proxy.

Obiectivele Setului de reguli sunt:

- Să fie sursa principală pentru definirea regulilor serviciului SPL și obligațiilor participanților la Schemă;
- Să furnizeze informații autorizate participanților la Schemă („Participanții") și altor părți relevante cu privire la modul în care funcționează Schema.

1.2 Documente de referință

Document	**Autor**
Mobile P2P Interoperability Framework - Implementation Guidelines - version 1.0, 09/06/2017	The Berlin Group
NextGenPSD2 XS2A Framework – Implementation Guidelines - version 1.0, 08 February 2018	The Berlin Group
Standardul ISO 20022 v.1	ISO
Regulamentul nr.2 din 17 februarie 2004 privind utilizarea codurilor IBAN în România	BNR

1.3 Glosar de termeni și abrevieri

Termen, Abreviere	**Explicație, Descriere**
API	Application Programming Interface - reprezintă un set de reguli și specificații care trebuie urmărite pentru a accesa și folosi serviciile și resursele software implementate de acel API.
Date proxy	Informațiile asociate unui proxy la nivelul bazei de date (de ex. alias, număr de cont (IBAN), nume deținător cont, banca ce administrează contul, etc.)
GDPR	General Data Protection Regulation - Regulamentul general privind protecția datelor în Uniunea Europeană
HTTP	Hypertext Transfer Protocol – protocol la nivel de aplicație pentru comunicarea datelor
IBAN	International Bank Account Number - identificator utilizat de instituțiile financiare pentru a identifica unic contul unui client.

Proxy	Alias (nr. de telefon, e-mail) asociat unui cont (IBAN), înregistrat în SPL, pe baza căruia un consumator inițiază o plată.
REST	REpresentational State Transfer – tip de arhitectură software bazat pe standarde Web și HTTP.
Serviciul SPL	Serviciu care permite schimbul de date necesare inițierii de plăți bazate pe utilizarea proxy-urilor (nr. de telefon mobil, adresa de email, alte tipuri de coduri), între entitățile participante.
STP	Straight Through Processing – Procesare directă între aplicaţii, fără intervenţie manuală.

1.4 Context

Prezentul Set de Reguli SPL a fost elaborat de Grupul de lucru SPL înființat în cadrul Asociației Române a Băncilor din reprezentanți ai Participanților la Schema de Transfer Credit SEPA RON și/sau la Schema de transfer credit instant SEPA RON.

Obiectivul inițial al Schemei SPL îl constituie facilitarea plăților efectuate de pe terminale mobile, utilizând soluțiile de plată dezvoltate de participanți și un serviciu în care numărul de telefon este utilizat ca proxy către un număr de cont IBAN.

Se estimează că se vor înregistra evoluții ulterioare, prin care vor fi adăugate noi tipuri de proxy-uri și identificatori de cont.

Părțile semnatare ale Convenției privind Schemele Naționale de Plăti, care au aderat la Schema de Transfer Credit SEPA RON și/sau la Schema de transfer credit instant SEPA RON, convin următoarele:

- Transmiterea informațiilor de identificare ale deținătorului unui cont IBAN, pe baza unui proxy, este făcută de Participantul care administrează contul respectiv;
- Datele privind proxy-urile, numerele de cont IBAN și deținătorul acestora sunt stocate centralizat, la nivelul bazei de date SPL;
- Aplicația SPL face toate validările necesare pentru a înscrie datele proxy valide în baza de date SPL.

1.5 Rolul ARB

În baza împuternicirii date de Părțile semnatare ale Convenției privind Schemele Naționale de Plăti și a mandatului Băncii Naționale a României privind funcția de guvernanță a Schemelor Naționale de Plăți, Asociația Română a Băncilor administrează Schema SPL ca serviciu adițional opțional la Schemele de transfer credit SEPA RON.
Atributele ARB în calitate de administrator al Schemei SPL includ:

a. Asigură respectarea regulilor Schemei, prevenirea neconformităţilor și neregularităților la nivelul Participanţilor la Schema (inclusiv prin aplicarea regimului sancționatoriu) în conformitate cu atribuțiile stabilite de Banca Națională a României.
b. Asigură administrarea procesului de aderare la Schemele SEPA RON a semnatarilor Convenției;

c. Asigură administrarea procesului de dezvoltare și actualizare a Schemei în baza acordului Participanților la Convenție;
d. Asigură procesul de raportare privind administrarea schemelor SEPA RON, în conformitate cu cerințele BNR.

1.6 Natura obligatorie a Setului de reguli

Calitatea de Participant la Schemă implică semnarea Contractului de aderare la Schema SPL RON. Prin semnarea Contractului de aderare la Schema SPL RON, Participanții se obligă să respecte regulile descrise în Setul de reguli, în care sunt incluse drepturile și obligațiile Participanților.

Setul de reguli acoperă în detaliu principalele aspecte ale relațiilor dintre Participanții la Schemă.

În plus, există un acord între Asociația Română a Băncilor în calitate de Administrator al Schemei SPL RON și Furnizorul serviciului SPL, care descrie rolurile și responsabilitățile respective în raport cu Schema SPL RON.

2 Participarea la Schema SPL RON

2.1 Eligibilitate

Înscrierea sau interogarea de informații din baza de date SPL poate fi efectuată de orice persoană juridică care respectă cumulativ următoarele criterii de eligibilitate:

- Este persoană juridică care a fost legal constituită și are personalitatea juridică în conformitate cu legile și practicile țării sale de origine
- A primit o autorizație - care nu a fost suspendată sau retrasă - de la o autoritate competentă din cadrul Spațiului Economic European și este reglementată ca „prestator de servicii de plată" (PSP), astfel cum este definit în Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată pe piața internă, de modificare a directivelor 2002/65 / CE, 2009/110 / CE și 2013/36 / UE și ale Regulamentului (UE) nr. 1093/2010 și de abrogare a Directivei 2007 / 64 / CE, în continuare „PSD2" sau a primit o autorizație echivalentă - care nu a fost suspendată sau retrasă - de la o autoritate competentă echivalentă stabilită într-o altă țară sau teritoriu inclusă în domeniul geografic al schemelor SEPA;
- A aderat la Convenția privind Schemele Naționale de Plăți, este participant la Schema de Transfer Credit SEPA RON și/sau la Schema de Transfer Credit Instant SEPA RON și aderă la Schema SPL (Standardised Proxy Lookup) RON.

2.2 Participanți

În funcționarea serviciului SPL sunt implicate trei tipuri de entități:

- Participantul inițiator – este entitatea care transmite solicitări de interogare a informațiilor corespunzătoare unui proxy, în conformitate cu prezentul Set de Reguli;
- Participantul destinatar – este entitatea care transmite solicitări de înregistrare în baza de date SPL a datelor proxy ale unui utilizator, în conformitate cu prezentul Set de Reguli;

- Furnizorul serviciului SPL – este entitatea care operează serviciul SPL și administrează aplicația și serviciile necesare funcționării acestui serviciu, în conformitate cu prezentul Set de Reguli.

Un participant poate acționa în oricare din rolurile de Participant inițiator sau Participant destinatar sau ambele.

În vederea participării la serviciul SPL, Participantul va asigura o conexiune securizată cu Furnizorul serviciului SPL.

2.3 Obligaţiile Participanţilor

Ca principiu general, participanții la Schemă trebuie să asigure:

- Elaborarea termenilor și condițiilor care reglementează furnizarea și utilizarea serviciilor bazate pe Schemă;
- Termenii și condițiile sunt în concordanță cu Setul de reguli;
- Implementarea măsurilor de gestionare a riscurilor operaționale și de securitate;
- Conformitatea regulilor și procedurilor interne, precum și acordurilor contractuale cu legile, regulamentele și cerințele generale de supraveghere aplicabile acestora.

2.4 Obligaţiile Participantului iniţiator

Pentru îndeplinirea unei solicitări a unui client al său, un Participant inițiator:

- Se asigură că a furnizat clientului toate informațiile necesare in legătură cu funcționarea Schemei și a obținut toate acordurile necesare pentru dezvăluirea oricărei informații obținute prin utilizarea serviciului SPL. Metoda utilizată în acest scop trebuie să fie conformă cu standardele privind protecția informațiilor.
- Informează persoana vizata in legătura cu activitățile de prelucrare date aferente Schemei
- Transmite solicitări de interogare a informațiilor corespunzătoare unui proxy, exclusiv în baza intenției clientului de a inița o plată; serviciul SPL nu va fi utilizat în alte scopuri, cum ar fi interogarea numelui posesorului unui număr de telefon.
- Se asigura ca Serviciul SPL nu este utilizat în mod abuziv în scopul preluării de informații care nu sunt destinate inițierii unei plăți prin monitorizarea si restricționarea pe o perioada de 15 minute a celor care au mai mult de 3 încercări consecutive fără a se inița plata Perioada de restricționare la sistem va fi mărita exponențial cu fiecare interogare ce nu a fost finalizata cu o inițiere de plata. ok
- Include codul IBAN al destinatarului în mesajul de plată generat prin utilizarea serviciului SPL.

Participantul inițiator care recepționează informații, urmare transmiterii către serviciul SPL a unei solicitări de interogare, se asigură că furnizează clientului plătitor informații care să confirme/infirme funcția de proxy a numărului de telefon.
Participantul inițiator nu are obligația să finalizeze plata, urmare transmiterii către serviciul SPL a unei solicitări de interogare (în situații cum ar fi: renunțarea de către clientul său la inițierea plății sau încălcarea politicilor interne la efectuarea plății către destinatarul identificat prin utilizarea serviciului SPL).

2.5 Obligaţiile Participantului destinatar

Pentru îndeplinirea unei solicitări a unui client al său, un Participant destinatar:

- Se asigură că a obținut toate acordurile necesare pentru orice informație dezvăluită prin utilizarea serviciului SPL. Metoda utilizată în acest scop trebuie să fie conformă cu standardele privind protecția informațiilor.
- Informează persoana vizata in legătură cu activitățile de prelucrare date aferente Schemei si colectează consimțământul;
- Verifică dacă proxy-ul aparține deținătorului contului IBAN asociat proxy-ului sau dacă acesta din urmă a fost autorizat de deținătorul proxy-ului să stabilească asocierea între proxy și contul IBAN. Verificarea va fi efectuată înaintea înregistrării datelor proxy în cadrul serviciului SPL.
- Actualizează în cel mai scurt timp informațiile înregistrate în baza de date SPL, în cazul modificării datelor aparținând deținătorului contului IBAN asociat proxy-ului sau in cazul retragerii consimtamantului de catre persoana vizata.
- Informează in cel mai scurt timp deținătorului contului IBAN asociat proxy-ului, despre suprascrierea informației printr-un SMS utilizând numărul declarat in cadrul Serviciului SPL.

2.6 Obligaţiile Furnizorului serviciului SPL

- Furnizorul de servicii SPL va fi autorizat de administratorul Schemei să opereze serviciul SPL în conformitate cu prevederile prezentului Set de reguli.
- Furnizorul de servicii SPL colectează și păstrează într-o bază de date centralizată (baza de date SPL) următoarele informații transmise de Participanți:
    - Proxy-ul clientului Participantului;
    - Codul IBAN al contului clientului Participantului, pe care acest client alege să îl asocieze proxy-ului;
    - Codul BIC al Participantului care administrează codul IBAN;
    - Numele și prenumele sau denumirea clientului Participantului;
    - Data (timestamp, în format UTC) la care Participantul a obținut consimțământul clientului său de a dezvălui datele sale personale către ceilalți participanți la Serviciul SPL.
- Furnizorul de servicii SPL asigură colectarea și procesarea solicitărilor Participanților la Serviciul SPL de administrare și regăsire a informațiilor păstrate în baza de date SPL, precum și a schimburilor de mesaje cu Participanții, din cadrul Serviciului SPL.
- Furnizorul de servicii SPL va informa administratorul Schemei în ceea ce privește modificarea documentației serviciului de tip SPL furnizat.
- Furnizorul de servicii SPL va asigura un timp maxim de răspuns de 2 secunde, de la recepționarea mesajului de interogare alias recepționat de la Participantul inițiator, până la momentul transmiterii mesajului de răspuns către acesta.
- Furnizorul de servicii SPL va transmite administratorul Schemei statistici trimestriale privind:
    - Numărul de interogări reușite/nereușite (pentru care a fost/nu a fost găsit un proxy).
    - Timp de răspuns mediu și maxim pentru solicitările de interogare a informațiilor corespunzătoare unui proxy, pe fiecare Participant inițiator.
    - Timpul de răspuns mediu și maxim pentru solicitările de interogare a informațiilor corespunzătoare unui proxy, aferente serviciului SPL furnizat.
    - Disponibilitatea și performanța serviciului SPL.

- Obligațiile comerciale ale Furnizorului de servicii SPL vor fi definite prin acordurile legale semnate cu fiecare Participant.

3 Serviciul SPL

3.1 Accesul la SPL

Accesarea de către participanți a serviciului SPL este realizată prin intermediul unui API, care asigură funcționalitățile de recepționare, transmitere, validare și procesare mesaje.

Serviciul SPL va putea fi accesat exclusiv de către participanții la Convenția privind Schemele Naționale de Plăti, care au aderat la Schema de Transfer Credit SEPA RON și/sau la Schema de Transfer Credit Instant SEPA RON și care îndeplinesc cerințele stabilite de Furnizorul serviciului SPL .

Interogarea de către participantul inițiator a informațiilor aferente unui proxy, prin utilizarea serviciului SPL, poate fi efectuată exclusiv în scopul inițierii unei plăți

3.2 Funcţionarea serviciului SPL

Serviciul SPL furnizat conform prezentului Set de reguli se bazează pe asocierea, pentru un client al unei bănci, a datelor de cont ale acestuia (BIC, IBAN, nume deținător cont), de un alias sau proxy (nr. de telefon mobil) stabilite de deținătorul contului. Informațiile aferente unui proxy se transmit prin schimburi STP de mesaje între participanții autorizați și aplicația SPL, utilizând un serviciu de tip web service/API.

Ulterior, un client al altei bănci, în procesul de iniţiere a unei plăţi, poate utiliza acel proxy (nr. de telefon mobil) pentru identificarea beneficiarului plății, celelalte date ale beneficiarului (nume, cod BIC şi cod IBAN) fiind obținute și completate (în mesajul/instrucțiunea de plată) de către banca sa, prin interogarea serviciului SPL.

3.3 Arhitectura de securitate a serviciului SPL

Compromiterea informației furnizate de serviciul SPL mărește riscul de fraudă, ce poate conduce la înregistrarea de pierderi financiare pentru participanți sau utilizatorii finali ai acestui serviciu.

Modelul de securitate are in vedere următoarele:

- Baza de date care stochează informațiile referitoare la beneficiarul plății (datele proxy) este sigură;
- Inițiatorul cunoaște identitatea beneficiarului plății și proxy-ul stabilit de acesta, înregistrat de către banca beneficiarului.

Participanții la Schema SPL și Furnizorul serviciului SPL implementează o arhitectură de securitate care asigură integritatea și/sau confidențialitatea informațiilor transmise/recepționate, astfel încât să se conformeze obiectivelor de securitate precizate la pct. 3.3.1.

3.3.1 Obiective de securitate

a) Bazele de date utilizate în cadrul serviciului SPL protejează integritatea și confidențialitatea informațiilor personale ale beneficiarilor înrolați;
b) Accesul la informațiile schimbate pe parcursul proceselor de adăugare /modificare /ștergere date proxy este permis numai participanților la Schema SPL;
c) plată poate fi inițiată numai de către un client al participantului inițiator;
d) Beneficiarul unei plăți bazate pe proxy poate fi doar un client al unui participant destinatar;
e) Identificatorul contului de plată al beneficiarului din ordinul de plată generat de prestatorul de servicii de plată al beneficiarului va fi numai IBAN-ul furnizat de serviciul SPL;
f) Serviciul SPL nu poate fi utilizat în mod eronat în scopul preluării de informații care nu sunt destinate inițierii unei plăți.

3.3.2 Cerințe de securitate

a) Integritatea proxy-ului (numărul de telefon mobil) trebuie păstrată pe durata procesării: de la momentul în care este introdus soluția de plată bazată pe proxy până la momentul în care este interogat de către participantul inițiator și primit de către serviciul SPL.
b) Informațiile despre clienți furnizate în timpul procesului de înscriere în baza de date proxy de către participantul destinatar trebuie să fie corecte. Aceste informații asociază identitatea clientului, numărul de telefon mobil, un IBAN, și data înscrierii
c) Furnizorul serviciului SPL trebuie să asigure integritatea înregistrărilor din baza de date proxy.
d) Orice schimb de informații din cadrul serviciului SPL trebuie să fie realizat prin autentificarea mutuală a celor două părți.
e) Aplicația de plată mobilă a plătitorului trebuie:
   - Să verifice integritatea și originea datelor primite ca răspuns de la serviciul SPL;
   - Să nu stocheze IBAN-ul primit de la serviciul SPL;
   - Să asigure un mecanism de jurnalizare;
   - Să asigure ca IBAN-ul folosit pentru a genera plata este ultimul recepționat într-un răspuns validat de la serviciul SPL;
   - Să furnizeze plătitorului un mecanism de confirmare a identității beneficiarului plății, înainte de generarea ordinului de plată;
   - Să furnizeze plătitorului un mecanism de confirmare a execuției plății.

3.3.3 Comunicația prin HTTPS și TLS

Comunicația între participanții la serviciul SPL trebuie realizată prin canale securizate, care asigură integritatea și confidențialitatea datelor transmise. Această cerință poate fi realizată prin utilizarea criptării la nivelul de transport a informației HTTPS și TLS[1].

Astfel :

- Participanții folosesc 2 certificate : unul pentru autentificarea la aplicație și un altul pentru semnarea oricărui mesaj;
- Autentificarea mutuală securizată este asigurată prin utilizarea certificatelor calificate de server și de client.
- Comunicarea se face prin canale securizate folosind protocolul HTTPS respectiv criptarea la nivel de transport folosind TLS 1.2 sau mai nou. Nu se accepta SSL sau TLS mai vechi de 1.2;

[1] Conform definiției din cap. 3.1.1 “Niveluri de Securitate” din *Mobile P2P Interoperability Framework Implementation Guidelines* publicat de Berlin Group.

Pentru auditare toate operațiunile facute de Participant sunt logate de către aplicatie.

3.4 Înrolare / modificare proxy (*enroll*) în SPL

Adăugarea unui proxy în baza de date proxy se face de către Participantul destinatar (care are asociat rolul corespunzător), în baza consimțământului acordat de clientul său (beneficiarul), prin furnizarea următoarelor date:

- Alias (proxy);
- Tip alias (tip proxy);
- Număr de cont IBAN al beneficiarului;
- Numele/denumirea beneficiarului;
- Data consimțământului (data la care beneficiarul a agreat utilizarea serviciului SPL).

La recepționarea unui mesaj de adăugare proxy, se verifică dacă proxy-ul din mesaj (tip proxy, valoare proxy) există în lista proxy-urilor active:

1) Dacă proxy-ul există în lista proxy-urilor active, se verifică dacă informațiile recepționate sunt mai recente decât cele înregistrate. Se compară data consimţământ din mesaj cu cea înregistrată:
   a) Dacă data consimţământului din mesaj este mai recentă decât data consimţământului din proxy-ul existent în baza de date proxy, se compară BIC-urile participanților destinatari:
      i) Dacă BIC-urile sunt diferite, informațiile existente sunt marcate ca înlocuite (REP) și se adaugă (ADD) informațiile din mesaj;
      ii) Dacă BIC-urile sunt identice, se modifică (MOD) informațiile proxy-ului existent cu valorile din mesaj.
   b) Dacă data consimțământului din mesaj este mai veche decât data consimţământului din proxy-ul existent în baza de date proxy, informațiile rămân nemodificate.
2) Dacă proxy-ul din mesaj nu există în lista proxy-urilor active, se adaugă (ADD) proxy-ul din mesaj în lista proxy-urilor active.

3.5 Ștergere proxy (*delete*) din SPL

Ștergerea unui proxy din baza de date proxy se face de către Participantul destinatar care a efectuat ultima înrolare a proxy-ului, prin furnizarea următoarelor date:

- Alias (proxy);
- Tip alias (tip proxy).

La recepționarea unui mesaj de ștegere proxy, se verifică dacă proxy-ul din mesaj (tip proxy, valoare proxy) există în lista proxy-urilor active pentru participantul destinatar. Dacă sproxy-ul există, proxy-ul existent este marcat ca șters.

3.6 Ștergere GDPR proxy (*erasure*) din SPL

Ștergerea GDPR a unui proxy din baza de date proxy se face de către Participantul destinatar care a efectuat ultima înrolare a proxy-ului, prin furnizarea următoarelor date:

- Alias (proxy);
- Tip alias (tip proxy).

La recepționarea unui mesaj de ștegere GDPR proxy, se verifică dacă proxy-ul din mesaj (tip proxy, valoare proxy) există în istoricul proxy-urilor pentru participantul destinatar. Dacă există înregistrări, sunt șterse din lista proxy-urilor active și din istoric proxy informațiile aferente proxy-ului respectiv, create de participantul destinatar.

3.7 Interogare informații proxy (*lookup*) din SPL

Interogarea informațiilor aferente unui proxy poate fi efectuată de un Participant inițiator (care are asociat rolul corespunzător).

La recepționarea unui mesaj de interogare informații proxy, se verifică dacă proxy-ul din mesaj (tip proxy, valoare proxy) există în lista proxy-urilor active. Dacă proxy-ul există, sunt transmise Participantului inițiator informațiile aferente proxy-ului.

3.8 Descărcarea bazei de date SPL de către participanţi

Serviciul asigură o funcționalitate de descărcare regulată, sub forma de fisier a listei numerelor de telefon ale persoanelor active înrolate în serviciu, functie care poate fi apelată într-un interval orar prestabilit.

4 Formatul datelor şi mesajelor utilizate

În definirea denumirilor și a tipurilor de câmpuri folosite în mesaje au fost utilizate standardul ISO 20022 și cadrul de interoperabilitate elaborat de The Berlin Group.

Cod BG	Descriere	Denumire	Tip data	Explicații
AT-05	Transaction Identification	TxId	Text(35)	Id-ul mesajului, formatul este doar ca recomandare
AT-06	Creation Date Timestamp	CreDtTm	Timestamp	Momentul crearii mesajului
AT-01	Alias Beneficiary	AlsBfy	Object (Tp,Id)	Aliasul
	+Type	Tp	Text(10)	Tipul aliasului=NrMobil/Email
	+Identification	Id	Text(256)	Valoarea aliasului
AT-03	Beneficiary BIC Bank	BIC	Text(11)	Codul Swift (BIC) al bancii
AT-10	IBAN	IBAN	Text(34)	Codul IBAN

Cod BG	Descriere	Denumire	Tip data	Explicații
AT-12	Beneficiary Name	BfyNm	Text(140)	Numele si prenumele / Denumirea titularului
AT-16	Registration Date Timestamp	RegDtTm	Timestamp	Data consimțământului
AT-08	Response Type	Resp	Object (Resp, Rslt, RslDtls)	Indică tipul de răspuns
	+Result	Rslt	Boolean	Indică tipul de rezultat
AT-09	++ResultDetails	RsltDtls	Array [Text(256)]	Prezent doar în răspunsurile negative. Conține detalii despre eroare.

5 Validări

Validarea mesajelor constă în:

1. Validarea sintactică:
   - Se validează fiecare câmp/parametru individual din punct de vedere al prezenţei (obligatoriu sau opţional), lungimii şi formatului acceptat;
   - Mesajul nu conţine alte câmpuri sau caractere nepermise.
2. Validarea semantică:
   - Se efectuează validări referitoare la corelările între diverse câmpuri
   - Se efectuează validări conform regulilor de business.

În cazul eșuării procesului de validare, expeditorul mesajului este notificat printr-un mesaj de răspuns care conține rezultatul validării.

Lista mesajelor de răspuns generate urmare validării mesajelor recepționate de la participanți, în funcție de tipul de mesaj, este prezentată în tabelul nr.1.

Tabelul nr. 1 – Lista mesajelor de răspuns generate la validarea mesajelor SPL

Rslt:	RsltDtls:
enroll	
true	
false	Iban code is not valid
	Structure AlsBfy is required
	Field BfyNm is required
	Max size for field BfyNm is 140 characters
	Field IBAN is required
	Max size for field IBAN is 34 characters
	Field RegDtTm is required
	Timestamp in field RegDtTm must be previous to the current API processing time

	Timestamp in field RegDtTm must be after the RegDtTm timestamp in the database
	Field Tp is required
	Field Id is required
delete	
true	
false	No match in the database
	Structure AlsBfy is required
	Field Tp is required
	Field Id is required
	Max size for field Id is 256 characters
erase	
true	
false	No match in the database
	Structure AlsBfy is required
	Field Tp is required
	Field Id is required
	Max size for field Id is 256 characters
lookup	
true	
false	No match in the database
	Structure AlsBfy is required
	Field Tp is required
	Field Id is required
	Max size for field Id is 256 characters