

 <p>asociația română a băncilor</p>	<p>CP_SCT_A_V6.1_vers 2024 Convenția Scheme Naționale de Plăți SPL Anexa 6.1 Setul de Reguli privind SPL RON</p>	<p><u>Data aprobării:</u> <u>09.01.2024</u></p> <p><u>Data intrării în vigoare:</u> <u>01.01.2025</u></p>
--	---	---

Set de Reguli privind SPL (Standardised Proxy Lookup) RON

1.	Introducere.....	3
1.1	Scopul documentului.....	3
1.2	Documente de referință	3
1.3	Glosar de termeni și abrevieri	3
1.4	Context	4
1.5	Rolul ARB	5
1.6	Natura obligatorie a Setului de reguli SPL.....	5
2	Participarea la Schema SPL RON.....	6
2.1	Eligibilitate	6
2.2	Participanți.....	6
2.3	Obligațiile Participanților.....	6
2.4	Obligațiile Participantului care consultă un alias.....	7
2.5	Obligațiile Participantului care înrolează un alias	7
2.6	Obligațiile Furnizorului serviciului SPL	8
3	Serviciul SPL	9
3.1	Accesul la serviciul SPL.....	9
3.2	Funcționarea serviciului SPL.....	9
3.3	Arhitectura de securitate a serviciului SPL	10
3.3.1	Obiective de securitate	10
3.3.2	Cerințe de securitate.....	10
3.3.3	Comunicația prin HTTPS și TLS	11
3.4	Înrolare / modificare proxy (<i>enroll</i>) în SPL	11
3.5	Ștergere proxy (<i>delete</i>) din SPL.....	12
3.6	Ștergere GDPR proxy (<i>erasure</i>) din SPL	12
3.7	Interogare informații proxy (<i>lookup</i>) din SPL	12
4	Formatul datelor și mesajelor utilizate	12
5	Validări.....	13

I.Istoric document

Data	Autor	Versiune	Descrierea modificarii
11.06.2020	ARB - DAS	V 2020	Versiunea inițială
03.01.2024	ARB - DAS	V 2024	Actualizarea documentului pentru corelarea cu prevederile Schemei RoPay pentru fluxul P2P la distanță fără proximitate, flux care folosește aceeași bază de date

1. Introducere

1.1 Scopul documentului

Prezentul Set de reguli privind SPL (Standardised Proxy Lookup) RON („Setul de reguli SPL”) 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 SPL 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
Documentului tehnic pentru participanții la sistemul SENT secțiunea a V-a AliasPay	TRANSFOND

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.
Aplicație SPL	Standardised Proxy Lookup - serviciul care facilitează solicitarea/efectuarea de plăți pe baza unui alias (numărul de telefon mobil) pe care cel care solicită/efectuează plata îl cunoaște la momentul inițierii acesteia.
Date proxy	Informațiile asociate unui proxy la nivelul bazei de date SPL (de ex. alias, identificare cont (IBAN), nume deținător cont, banca ce administrează contul, scopul înregistrării informațiilor, etc.)
GDPR	General Data Protection Regulation - Regulamentul general privind protecția datelor în Uniunea Europeană (UE) 2016/679
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.
Participant	PSP-ul semnatat al contractului de aderare la Schema SPL RON, care înscrie și/sau consultă date proxy utilizând serviciul SPL.
Proxy	Alias (nr. de telefon) asociat unui cont (IBAN), înregistrat în baza de date SPL, pe baza căruia un consumator inițiază o plată sau o solicitare de plată RoPay P2P la distanță.
REST	REpresentational State Transfer – tip de arhitectură software bazat pe standarde Web și HTTP.
Schema RoPay	Set de practici și standarde emise de ARB și TRANSFOND la care Participanții au aderat în scopul furnizării Serviciului RoPay;
Serviciul RoPay	Serviciu de inițiere a unei solicitări de plată de către Utilizatorul beneficiar, furnizat de participanții la Schema RoPay, în conformitate cu Setul de reguli privind Schema RoPay.
Serviciul SPL	Serviciu care permite schimbul de date necesare inițierii plăților/solicitărilor de plată 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 aplicații, fără intervenție 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 RÓN și/sau la Schema de transfer credit instant SEPA RON.

Obiectivul Schemei SPL RON îl constituie facilitarea inițierii plăților și a solicitărilor de plăți, 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 identificator cont (cod IBAN).

Părțile semnatare ale Convenției privind Schemele Naționale de Plăți, 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 identificat prin IBAN, pe baza unui proxy, este făcută de Participantul care administrează contul respectiv;
- Datele privind proxy-urile, codurile IBAN și deținătorul acestora sunt stocate centralizat, la nivelul bazei de date SPL;
- Prin aplicația SPL se fac toate validările necesare pentru a asigura înscrierea datelor proxy valide în baza de date SPL.

1.5 Rolul ARB

În baza împuternicirii date de Părțile semnatare ale Convenției privind Schemele Naționale de Plăți, Asociația Română a Băncilor administrează Schema SPL RON ca serviciu adițional opțional la Schemele de transfer credit SEPA RON.

Atributele ARB în calitate de administrator al Schemei SPL RON includ:

- a. Asigură respectarea regulilor Schemei, prevenirea neconformităților și neregularităților la nivelul Participanților la Schema (inclusiv prin aplicarea regimului sancționatoriu);
- b. Asigură administrarea procesului de aderare la Schema SPL RON;
- c. Asigură administrarea procesului de dezvoltare și actualizare a Schemei SPL RON;
- d. Asigură procesul de raportare privind administrarea schemei SPL RON,

1.6 Natura obligatorie a Setului de reguli SPL

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 SPL, în care sunt incluse drepturile și obligațiile Participanților.

Setul de reguli SPL 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 TRANSFOND Furnizorul serviciului SPL, care descrie rolurile și responsabilitățile respective în raport cu Schema SPL RON.

2 Participarea la Schema SPL RON

2.1 Eligibilitate

La Schema SPL RON poate participa 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/sau la Schema RoPay.

2.2 Participanți

În funcționarea serviciului SPL sunt implicate două tipuri de entități:

- **Participantul SPL**, care acceptă Setul de Reguli privind SPL (Standardised Proxy Lookup) RON. Acesta poate avea unul dintre rolurile următoare:
 - Participant care consultă un alias – este entitatea care transmite solicitări de identificare a informațiilor corespunzătoare unui proxy în baza de date SPL, în conformitate cu prezentul Set de Reguli SPL;
 - Participant care înrolează un alias – 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 SPL;
- **Furnizorul serviciului SPL** – este entitatea care operează serviciul SPL și administrează aplicația SPL și serviciile necesare funcționării acestui serviciu, în conformitate cu prezentul Set de Reguli SPL.

Un participant poate acționa în rolul de Participant care înrolează un alias sau Participant care înrolează un alias și consultă un alias.

2.3 Obligațiile Participanților

Ca principiu general, participanții la Schema SPL RON trebuie să asigure:

- Elaborarea termenilor și condițiilor care reglementează furnizarea și utilizarea serviciilor bazate pe Schema SPL RON. Acestea trebuie să fie în concordanță cu Setul de Reguli SPL;
- Implementarea măsurilor de gestionare a riscurilor operaționale și de securitate;

- Conformitatea regulilor și procedurilor interne, precum și a acordurilor contractuale cu legile, regulamentele și cerințele generale de supraveghere aplicabile acestora.

2.4 Obligațiile Participantului care consultă un alias

Pentru îndeplinirea unei solicitări a unui client al său de identificare a datelor proxy, un Participant SPL:

- Se asigură că a furnizat clientului toate informațiile necesare în legătură cu funcționarea Schemei SPL RON 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 și reglementările privind protecția informațiilor;
- Informează persoana vizată în legătură cu activitățile de prelucrare date aferente Schemei SPL RON;
- Transmite solicitări de consultare a datelor proxy, cu intenția de a iniția o plată sau o solicitare de plată RoPay; serviciul SPL nu va fi utilizat în alte scopuri, cum ar fi aflarea numelui posesorului unui număr de telefon;
- Include în solicitarea de consultare a datelor proxy scopul în care este efectuată consultarea, conform punctului 3.2 de mai jos;
- Se asigură că Serviciul SPL nu este utilizat în mod eronat în scopul preluării de informații care nu sunt destinate inițierii unei plăți prin monitorizarea și restricționarea accesului la sistem, pe o perioadă de 15 minute, a celor care au mai mult de 3 încercări consecutive fără a se finaliza o tranzacție. Perioada de restricționare a accesului la sistem va fi majorată exponențial cu fiecare interogare ce nu a fost finalizată cu o inițiere de plată;
- În cazul interogărilor pentru RoPay scenariul P2P la distanță, Participantul acceptă până la maxim 70 de interogări efectuate de un client al său în 24 de ore, după această valoare fiind restricționat accesul pentru o perioadă de 24 de ore. În acest caz, Participantul care consultă un alias nu va afișa utilizatorului său IBAN-ul aferent plătitorului;
- Include în mesajul de plată /solicitarea de plată RoPay generat/generată codul IBAN obținut prin utilizarea serviciului SPL;
- Informează persoana vizată în legătură cu activitățile de prelucrare date aferente Schemei SPL și colectează consimțământul.

Participantul care recepționează informații, ca urmare a transmiterii către serviciul SPL a unei solicitări de consultare alias, se asigură că furnizează clientului său informații care să confirme/infirme funcția de proxy a numărului de telefon.

Participantul care consultă un alias nu are obligația să finalizeze plata/ solicitarea de plată RoPay, ca urmare a transmiterii către serviciul SPL a unei solicitări de consultare alias (în situații cum ar fi: renunțarea de către clientul său la inițierea plății/transmiterea unei solicitări de plată, sau încălcarea politicilor interne referitoare la efectuarea de plăți/ inițierea solicitărilor de plată către destinatarul identificat prin utilizarea serviciului SPL).

2.5 Obligațiile Participantului care înrolează un alias

Pentru îndeplinirea unei solicitări a unui client al său de înrolare a datelor proxy, Participantul:

- 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 vizată în legătură cu activitățile de prelucrare date aferente Schemei SPL RON și colectează consimțământul utilizatorului;

- Verifică dacă proxy-ul aparține deținătorului contului asociat proxy-ului sau dacă acesta din urmă a fost autorizat de deținătorul proxy-ului să stabilească asocierea între proxy și codul IBAN. Verificarea va fi efectuată înaintea înregistrării datelor proxy în cadrul serviciului SPL.
- Transmite o solicitare de înrolare în baza de date a serviciului SPL a informațiilor corespunzătoare unui proxy, cu specificarea scopului în care poate fi consultat alias-ul;
- Actualizează în cel mai scurt timp informațiile înregistrate în baza de date SPL, în cazul modificării datelor aparținând deținătorului contului al cărui cod IBAN este asociat proxy-ului sau în cazul retragerii consimțământului de către persoana vizată;
- Informează, în cel mai scurt timp, deținătorul contului al cărui cod IBAN este asociat proxy-ului, despre suprascrierea informației, printr-un SMS utilizând numărul declarat în cadrul Serviciului SPL.

2.6 Obligațiile Furnizorului serviciului SPL

- Furnizorul de servicii SPL va opera serviciul SPL în conformitate cu prevederile prezentului Set de reguli SPL;
- Furnizorul de servicii 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
- Furnizorul de servicii SPL colectează și păstrează într-o bază de date centralizată (bază 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;
 - Scopul pentru care pot fi dezvăluite informațiile aferente proxy-ului;
 - 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 înrolare și consultare a informațiilor păstrate în baza de date SPL, precum și a schimburilor de mesaje cu Participanții, din cadrul Serviciului SPL;
- Furnizorul de servicii SPL are obligația de a păstra log-urile pentru eventuale investigații ulterioare conform specificațiilor aferente serviciului SPL menționate la bullet 3 de la secțiunea 3.3.2.
- Furnizorul de servicii SPL va furniza în răspunsul la o solicitare de consultare alias exclusiv informațiile care au fost înrolate pentru scopul specificat în solicitare;
- Furnizorul de servicii SPL va informa administratorul Schemei SPL RON 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 care consultă un alias, până la momentul transmiterii mesajului de răspuns către acesta;
- Furnizorul de servicii SPL va transmite administratorului Schemei SPL RON 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 care consultă un alias;
- 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 serviciul SPL

În vederea participării la serviciul SPL, Participantul îndeplinește cerințele tehnice stabilite de Furnizorul serviciului 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 Plăți, care au aderat la Schema de Transfer Credit SEPA RON și/sau la Schema de Transfer Credit Instant SEPA RON și/sau la Schema RoPay și care îndeplinesc cerințele stabilite de Furnizorul serviciului SPL, conform Documentului tehnic pentru participanții la sistemul SENT secțiunea a V-a AliasPay elaborat de TRANSFOND.

Interogarea de către un Participant a informațiilor aferente unui proxy, prin utilizarea serviciului SPL, poate fi efectuată exclusiv în scopul inițierii unei plăți/solicitări de plată.

3.2 Funcționarea serviciului SPL

Serviciul SPL furnizat conform prezentului Set de Reguli SPL se bazează pe asocierea datelor de cont ale unui client al unui Participant (BIC, IBAN, nume deținător cont), scop, cu un proxy (nr. de telefon mobil) stabilite de deținătorul contului.

Informațiile aferente unui proxy se transmit prin schimburi STP de mesaje între participanți și aplicația SPL, utilizând un serviciu de tip web service/API.

Scopurile pentru care pot fi înrolate datele de cont asociate unui proxy sunt următoarele:

- a) **recepționarea unei plăți** de către beneficiarul plății, client al unui Participant;
- b) **recepționarea unei solicitări de plată** de către plătitor, client al unui Participant, în vederea efectuării unei plăți.

Scopurile pentru care pot fi consultate datele de cont asociate unui proxy sunt următoarele:

- a) **efectuarea unei plăți** de către plătitor, client al unui Participant, prin utilizarea în mesajul/instrucțiunea de plată a informațiilor despre beneficiarul plății (nume, cod BIC și cod IBAN), regăsite prin interogarea serviciului SPL;

- b) **inițierea unei solicitări de plată** de către beneficiarul plății, client al unui Participant, prin utilizarea în solicitarea de plată RoPay a informațiilor despre plătitor (nume, cod BIC și cod IBAN), regăsite prin interogarea serviciului SPL.

3.3 Arhitectura de securitate a serviciului SPL

Compromiterea informației furnizate de serviciul SPL mărește riscul de fraudă, ceea ce determină pierderi financiare pentru utilizatorii finali ai acestui serviciu.

Modelul de securitate are în vedere următoarele:

- Baza de date care stochează informațiile asociate unui alias (datele proxy) este sigură;
- Participantul care înrolează un alias cunoaște identitatea clientului său care a solicitat înrolareași proxy-ul stabilit de acesta.

Participanții la Schema SPL RON 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 clienților înrolați;
- b) Accesul la informațiile schimbate pe parcursul proceselor de adăugare/modificare /ștergere date proxy este permis numai participanților la Schema SPL RON;
- c) Plata sau solicitarea de plată RoPay poate fi inițiată numai de către un client al unui Participant cu rol de consultare alias;
- d) Beneficiarul unei plăți sau destinatarul unei solicitări de plată bazate pe proxy poate fi doar un client legitim al unui participant cu rol de înrolare alias;
- e) Identificatorul contului de plată al beneficiarului din ordinul de plată generat de prestatorul de servicii de plată al plătitorului va fi numai IBAN-ul furnizat de serviciul SPL, dacă datele de cont asociate proxy-ului au fost consultate în scopul efectuării unei plăți;
- f) Identificatorul contului de plată al plătitorului din solicitarea de plată RoPay generată de prestatorul de servicii de plată al beneficiarului, va fi numai IBAN-ul furnizat de serviciul SPL;
- g) Serviciul SPL nu poate fi utilizat în mod eronat în scopul preluării de informații care nu sunt destinate scopului pentru care au fost înrolate informațiile respective.

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 în soluția de plată bazată pe proxy, până la momentul în care este transmis de către participantul care interoghează un alias și primit de către serviciul SPL;
- b) Datele proxy furnizate în timpul procesului de înscriere în baza de date proxy de către participantul care înrolează un alias trebuie să fie corecte. Aceste informații asociază identitatea clientului, numărul de telefon mobil, un cod IBAN, scopul înrolării și data acordării consimțământului de procesare a datelor cu caracter personal;
- 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 furnizată de Participant clientului său 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 că IBAN-ul folosit pentru a genera plata sau solicitarea de plată RoPay este ultimul recepționat într-un răspuns validat de la serviciul SPL;
- Să furnizeze clientului său un mecanism de confirmare a identității beneficiarului unei plăți sau destinatarului unei solicitări de plată RoPay, înainte de generarea ordinului/solicitării de plată.

3.3.3 Comunicația prin HTTPS și TLS

Comunicația între participanții la serviciul SPL și Furnizorul serviciului SPL trebuie realizată prin canale securizate, care asigură integritatea și confidențialitatea datelor transmise. Această cerință este realizată prin utilizarea criptării la nivelul de transport a informației HTTPS și TLS¹.

Astfel :

- Participanții folosesc 2 certificate: unul pentru autentificarea la aplicația SPL 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;

Pentru auditare, toate acțiunile efectuate de Participant sunt logate de către aplicația SPL.

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

Adăugarea unui proxy în baza de date proxy se efectuează de către Participantul cu rol de înrolare alias, în baza consimțământului acordat de clientul său prin furnizarea următoarelor date:

- Alias (proxy);
- Tip alias (tip proxy);
- Număr de cod IBAN al clientului;
- Numele/denumirea clientului;
- Scopul înrolării alias-ului;
- Data acordării consimțământului.

La recepționarea unui mesaj de adăugare proxy, se verifică dacă proxy-ul din mesaj (tip proxy, valoare proxy, scop înrolare) 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 acordării consimțământului din mesaj cu cea înregistrată:
 - a) Dacă data consimțământului din mesaj este mai recentă decât data consimțământului din proxy-ul existent în baza de date proxy, se compară BIC-urile participanților care efectuează înrolarea:
 - i) Dacă BIC-urile sunt diferite, informațiile existente sunt marcate ca înlocuite (REP) și se adaugă (ADD) informațiile din mesaj;

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

- 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 consimțământului 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 efectuează de către Participantul care a efectuat ultima înrolare a proxy-ului, prin furnizarea următoarelor date:

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

La recepționarea unui mesaj de ștergere proxy, se verifică dacă proxy-ul din mesaj (tip proxy, valoare proxy, scop înrolare) există în lista proxy-urilor active pentru participantul care solicită ștergerea. Dacă proxy-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 efectuează de către Participantul care a efectuat ultima înrolare a proxy-ului, prin furnizarea următoarelor date:

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

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

3.7 Interogare informații proxy (*lookup*) din SPL

Interogarea informațiilor aferente unui proxy poate fi efectuată de un Participant cu rol de consultare alias.

La recepționarea unui mesaj de interogare informații proxy, se verifică dacă proxy-ul din mesaj (tip proxy, valoare proxy, scop consultare) există în lista proxy-urilor active. Dacă proxy-ul există pentru scopul precizat în solicitare, sunt transmise Participantului care a transmis solicitarea de consultare a informațiilor aferente proxy-ului.

4 Formatul datelor și 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 creării 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 băncii
AT-10	IBAN	IBAN	Text(34)	Codul IBAN
AT-12	Beneficiary Name	BfyNm	Text(140)	Numele și prenumele / Denumirea titularului
AT-16	Registration Date Timestamp	RegDtTm	Timestamp	Data consimțământului
	Consent Purpose	Scope	Numeric(1,2)	Scopul consimțământului
AT-08	Response Type	Resp	Object (Resp, Rslt, RsltDtls)	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:

- Validarea sintactică:
 - Se validează fiecare câmp/parametru individual din punct de vedere al prezenței (obligatoriu sau opțional), lungimii și formatului acceptat;
 - Mesajul nu conține alte câmpuri sau caractere nepermise.
- 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 ca urmare a 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