

EPC250-18
Version 1.0
Date issued: 20 December 2018
Date effective: 1 January 2019



Public – Internal Use – Confidential – Strictest Confidence
Distribution: General Public

SEPA PROXY LOOKUP (SPL) SCHEME RULEBOOK



TABLE OF CONTENTS

0 Information	5
0.1 Change history	5
0.2 Purpose of document.....	5
0.3 About the EPC	5
1 SPL Scheme	5
1.1 Scope.....	5
1.2 Actors	5
1.3 Application to SEPA.....	5
1.4 Binding nature of the Rulebook.....	6
1.5 Separation between the SPL Scheme and SEPA payment Schemes	6
1.6 The business benefits of the Scheme.....	6
1.7 Fees.....	6
2.Rights & Obligations of Participants	6
2.1 Eligibility for participation	6
2.2 Reachability	7
2.3 Becoming a Participant	7
2.3.1 Appeals.....	8
2.4 Scheme list of Participants	8
2.5 Obligations of Participants.....	9
2.5.1 Obligations of an Initiating Registry Provider (IRP)	9
2.5.2 Obligations of a Responding Registry Provider (RRP).....	9
2.6 Limitation of liability.....	10
2.6.1 Compensation for breach of the Rulebook	10
2.6.2 Limits on Liability	10
2.6.3 Force Majeure.....	10
2.7 Liability of the EPC.....	10
2.8 Compliance	11
2.8.1 General.....	11
2.8.2 Compliance and Adherence Committee/Appeals Committee	11
2.8.3 Complaints handling	11
2.8.3.1 Role of CAC in Complaints	11
2.8.3.2 Investigation of Complaints	12
2.8.3.3 Evaluation of Complaint	12
2.8.3.4 Sanctions	13
2.8.3.5 Emergency Injunction Procedure	16
2.8.3.6 Appeals Arising from Complaints	16
2.8.3.7 Timing of Sanctions	16
2.8.3.8 Eligibility, Merger and Acquisition of a Participant	17



2.8.3.9	Costs	17
2.8.4	Appeals.....	17
2.8.4.1	Introduction to the Appeals Process	17
2.8.4.2	Submission of Appeals Notice	17
2.8.4.3	Meeting.....	18
2.8.4.4	Costs	18
2.8.4.5	Further Steps.....	19
2.9	Termination	19
2.10	Intellectual property.....	20
2.11	Contractual provisions	20
2.12	Applicable legislation	20
2.13	Governing law	20
3.	Scheme Management	21
3.1	SPL Scheme Participant Group.....	21
3.1.1	Composition of the SPL Scheme Participant Group.....	21
3.1.2	Organisation	21
3.1.3	Mandate.....	21
3.1.4	Scope	21
3.2	Maintenance and Evolution (change management process)	22
3.2.1	Guiding principles.....	22
3.2.2	Role of the SPL SPG.....	22
3.2.3	Submission of Change Requests to the Secretariat	23
3.2.4	Acknowledgement of Receipt of a Change Request	23
3.2.5	Consideration of a Change Request	23
3.2.6	Publication of Change Requests.....	24
3.2.7	Process for Major Rulebook changes	24
3.2.7.1	Preparation of SPL SPG Recommendation.....	24
3.2.7.2	Dialogue with the Initiator	25
3.2.7.3	Public Consultation on Change Request.....	25
3.2.7.4	Process following Public Consultation	25
3.2.7.5	Board Deliberations on the SPL SPG Change Proposal Submission Document	25
3.2.7.6	Publication	26
3.2.7.7	Exceptional Change	26
3.2.7.8	Change for regulatory reasons	26
3.2.8	Process for Minor Rulebook changes	26
3.2.9	Frequency of the change management process	27
4.	SPL Service Provider(s)	27
4.1	SPL service provider(s).....	27
4.2	Roles.....	27



4.3 Obligations.....	27
4.4 Liabilities	28
5. Terms defined.....	28
6. Annexes	29



0 Document information

0.1 Change history

Issue N°	Date	Reason for revision
V1.0	20/12/2018	Approval by the Board.

0.2 Purpose of document

The present SPL Scheme Rulebook (the “Rulebook”) consists of a set of rules, practices and standards that makes it possible to operate, join and participate in the SPL Scheme.

The objectives of the Rulebook are:

- To be the primary source for the definition of the rules and obligations of the Scheme.
- To provide authoritative information to Scheme Participants (the “Participants”) and other relevant parties as to how the Scheme functions.

0.3 About the EPC

The European Payments Council (EPC) is one voice for payment service providers (PSPs) on all European payment issues. The EPC’s goal is to contribute to harmonised payments in the Single Euro Payments Area (SEPA)– a goal which ultimately supports European competitiveness and innovation.

1. SPL Scheme

1.1 Scope

The SPL Scheme (the “Scheme”) covers the exchange of the data necessary to initiate payments between proxy-based payment solutions on a pan-European level. It aims to facilitate interoperability between participating payment solutions.

Initially the focus will be on (mobile) payments whereby the mobile telephone number is used as a proxy to an IBAN. It is envisaged that the Scheme will evolve over time to support additional proxy types, account identifiers and use cases.

1.2 Actors

The three types of actors involved in the Scheme include:

- Initiating Registry Providers (IRP): entity which makes a lookup request into the SPL, in accordance with the Rulebook.
- Responding Registry Providers (RRP): entity which responds to a lookup request from the SPL, in accordance with the Rulebook.
- SPL Service Provider(s): entity which operates the SPL service, the software and the services related to it in accordance with the Rulebook.

1.3 Application to SEPA

The Scheme is applicable in the countries listed in the EPC List of SEPA Scheme Countries, as amended from time to time (the “SEPA geographic area”)¹.

¹ EPC409-09 EPC List of SEPA Scheme Countries



1.4 Binding nature of the Rulebook

Becoming a Participant in the Scheme involves signing the adherence agreement. By signing the Scheme adherence agreement (See Annex 1), Participants agree to respect the rules described in the Rulebook. The Rulebook describes the liabilities and responsibilities of each Participant in the Scheme.

The Rulebook covers in depth the main aspects of the relationships between the Scheme actors.

In addition, there is an agreement between the EPC and each SPL Service Provider describing their respective roles and responsibilities in relation to the SPL service.

1.5 Separation between the SPL Scheme and SEPA Payment Schemes

The Scheme is limited to a look-up function with the sole purpose of initiating a payment. The actual payment is however not part of the Scheme and is covered by an 'overseen' payment scheme within the SEPA geographic area.

1.6 The business benefits of the Scheme

The Scheme aims to ensure a convenient way to allow any payment service user to initiate a pan-European (mobile) payment safely and securely, using a simple method with information other than a payment account identifier which the counterparty is prepared to share in order to enable a payment.

IRPs will benefit from the fact that they can offer their customers proxy-based payment solutions on a pan-European level. Also, there are benefits enjoyed by the RRP as it will enable its customers to receive payments.

The value of the Scheme is directly proportional with the number of Participants.

1.7 Fees

The EPC reserves the right to recover costs to manage the Scheme from the Participants. The policy of the EPC with regard to fees related to the management of the Scheme will be decided from time to time by the Board, upon recommendation of the SPL SPG, as set out in more detail in Annex. These fees will be published on the EPC website.

2. Rights & Obligations of Participants

2.1 Eligibility for participation

A lookup or response request can be made by anyone who fulfils the Scheme eligibility requirements and is a registered Participant in the Scheme.

Eligible for Scheme participation is any legal entity which has been legally constituted and has the legal personality in accordance with the laws and practices of its country of origin and:

- has received an authorisation - which has not been suspended or withdrawn - from a competent authority of the European Economic Area and is regulated as a 'payment service provider' (PSP) as defined in Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, hereafter "PSD2", or has received an equivalent authorisation - which has not been suspended or withdrawn - from an equivalent competent authority established in another country or territory included with the geographical scope of the SEPA Schemes; or



- is a legal entity representing and, directly or indirectly, having as members PSPs, and being established in a country or territory included within the SEPA geographic area; or
- is a legal entity providing technical or operational services to PSPs in the context of an 'overseen' payment scheme in the SEPA geographic area including access to the SPL service, being established in a country or territory included within the geographical scope of such schemes and being designated by one or more of those PSPs to represent it (them) at the level of the Scheme.

2.2 Reachability

A Participant in the SPL Scheme may act as either an IRP or RRP or both.

In order to be reachable, a Participant will need to ensure a secure connection with (one of) the available SPL service provider(s).

2.3 Becoming a Participant

The EPC Secretariat (the "Secretariat"), is responsible for approving applications to join the Scheme.

The Secretariat will only approve an applicant for participation in the Scheme if it can demonstrate that it satisfies the eligibility criteria set out in section 2.1 of the Rulebook. The information provided by an applicant in accordance with the instructions included in the present section and using the template adherence agreement (see Annex 1) should enable the Secretariat to determine whether or not the applicant is able to satisfy these criteria and make a positive or negative decision regarding the application. The Secretariat will only reject applications on the basis of failure to meet these criteria.

Each legal entity that seeks to adhere to the Scheme must agree to accept the rights and obligations of a Participant in relation to the Scheme. Upon admission to the Scheme, the adhering legal entity shall assume all of the rights and responsibilities arising from admission to the Scheme.

A subsidiary entity or affiliate of an adhering entity, i.e. each entity that has a separate and distinct legal personality within the adhering entity's group or organisational structure, must adhere separately from a parent or group entity. A subsidiary or affiliate shall be a Participant in its own right and shall assume all the rights and responsibilities arising from admission to the Scheme.

The Secretariat uses reasonable efforts to send a written acknowledgement of receipt of the application to the applicant within 10 Business Days of receiving the application.

The Secretariat shall use reasonable efforts to determine the application within 60 Calendar Days of receiving the application. In the event that the Secretariat requires more time to arrive at a determination, it shall notify the applicant as soon as it is reasonably practicable to do so.

The Secretariat may request the applicant to provide such additional information as may be required in the course of determining the application.

In the course of determining the application, the Secretariat may take into consideration views expressed by national regulators (this term extends to include such bodies as insolvency officers, law enforcement authorities and local courts).

In the case of a successful application, the applicant will receive a written notification of admission to the Scheme. The applicant becomes a Participant and becomes subject to the Rulebook on the Admission Date published on the EPC website within 5 Business Days following the confirmation of successful application (or later in line with the



readiness date of the applicant). The Secretariat may send the written notification to the applicant in paper or electronic format.

It is important that applicants provide accurate, up-to-date and complete information in relation to the criteria set out in the Rulebook. If an applicant fails to provide the necessary information, consideration of its application could be subject to delay or further investigation.

Only applications made in accordance with the template adherence agreement (see Annex 1) and completed in the English language will be taken into consideration.

The completed adherence agreement should be couriered to:

European Payments Council AISBL

Cours Saint-Michel 30

B-1040, Brussels

Belgium

The Secretariat may reject an application for participation in the Scheme if an applicant fails to satisfy the eligibility criteria set out in the Rulebook.

Where an application is rejected, the Secretariat shall provide the applicant with a written notification setting out the reasons for rejecting the application.

An applicant may not re-apply to become a Participant until 3 months after the determination of its application by the Secretariat or after a determination in an appeal begun in accordance with the Rulebook or after a final determination of a tribunal or court responsible for determining the case.

2.3.1 Appeals

An applicant whose application for participation in the Scheme has been rejected may appeal to the Appeals Committee for a re-consideration of its application. A notice of appeal in such case must be filed within 21 Calendar Days of the applicant receiving a notification of rejection of its adherence application. The appeals notice must include a copy of the adherence application together with a copy of the written notification setting out the reasons for rejecting the application supplied to the applicant under section 2.3 and any other information relevant for the appeal. The appeal shall be determined in accordance with the Appeals Process set out in [Document]².

2.4 Scheme register of Participants

The Secretariat shall maintain a Scheme register of Participants. The register shall contain the name, contact address and other details determined by the EPC in respect of the Participant.

The Scheme register of Participants shall be maintained in good and up-to-date order by the Secretariat and arrangements will be made for such register to be made available to Participants when issued or updated, through the register of Participants published on the EPC website.

If the Participant changes its details, so that the register does not carry accurate data in respect of the Participant, the Participant shall notify the Secretariat as soon as it is reasonably practicable to do so. It is the responsibility of the Participant to ensure that the Secretariat is provided with information in relation to the Participant that is accurate and up-to-date at all times.

² Reference to the document to be added.



In the event of Participants no longer being able to pay their debts as they fall due, becoming insolvent or having ceased to exist (each an Event of Default), the Secretariat may decide to rectify the register of Participants after verification of such event with the relevant national regulator or national authority. The failure of a Participant to pay the fees mentioned in section 1.7 of the Rulebook shall constitute an Event of Default for the purposes of this section, on the basis of which the EPC may, at its sole discretion and upon notice by registered mail, temporarily or permanently suspend the entry of the Participant in the register of Participants, as of the first following update publication, but not earlier than 30 calendar days after the issuance of such notice of suspension.

The register of Participants, containing the Participants' EPC registration number, name, address, operational readiness date and Scheme leaving date (if applicable), may be accessed and searched through the EPC website. The register is not an operational database in respect of Scheme usage. Any operational data needed by Participants in relation to other Participants shall be supplied outside of the Scheme.

By submitting an application to become a Participant, an undertaking consents to publication of the details referred to in this section.

2.5 Obligations of Participants

As a general principle, the Participants shall:

- Ensure that terms and conditions exist governing the provision and use of services relating to the Scheme;
- Ensure that such terms and conditions are consistent with the Rulebook;
- Ensure that such terms and conditions make adequate provision for the Participant's succession (e.g. through merger or acquisition), in accordance with the Rulebook;
- Ensure adequate risk management and security;
- Ensure the ongoing compliance of its own rules, procedures and agreements with the laws, regulations and generic supervisory requirements applicable to them.

2.5.1 Obligations of an Initiating Registry Provider (IRP)

In respect of each of its customers, an IRP shall:

- Only perform lookups for the intention of initiating a payment (e.g. SPL lookup service shall not be used for a phone number-name lookup service).
- Ensure that all required consents have been collected for any information disclosed via the SPL service. The method to do this should be compliant with local standards where the information is collected.
- Include the recipient's IBAN in constructing the payment message (following the look-up).

It should be noted that the IRP that is receiving information from an SPL enquiry is under no obligation to disclose all of that information to its customers. Moreover, just because the SPL service has returned an IBAN there is no obligation on the IRP to complete the payment (for example if the customer does not confirm the initiation of the payment or if it would breach internal policy).

2.5.2 Obligations of a Responding Registry Provider (RRP)

In respect of each of its customers, an RRP shall:

- Ensure that all required consents have been collected for any information disclosed via the SPL service. The method to do this should be compliant with local standards where the information is collected.



- Verify, before a proxy can be shared through the SPL service, that the proxy is in control of the account holder (i.e. payee), or otherwise authorised by the possessor of the proxy to link it to the destination account.
- Guarantee the accuracy of the revealed identity of the beneficiary (if applicable) in a lookup.
- Guarantee the speed of updating of changes to the proxy database.

It should be noted that the RRP will be liable in case the response is inaccurate (e.g. incorrect IBAN).

2.6 Limitation of liability

2.6.1 Compensation for breach of the Rulebook

A Participant who is party to a lookup request shall be liable to the other Participant who is also party to that lookup request for all foreseeable losses, costs, damages and expenses (including reasonable legal fees), taxes and liabilities for any claims, demands or actions (each referred to as a "Loss"), where the Loss arises out of or in connection with:

1. any breach of the Rulebook relating to the lookup request by the relevant Participant, its employees or agents;
2. any negligent act or omission of the relevant Participant, its employees or agents relating to the lookup request insofar as relevant to the operation of the Scheme;
3. any operational failure of the relevant Participant, its employees or agents relating to the lookup request insofar as relevant to the operation of the Scheme.

2.6.2 Limits on liability

A Participant's liability under the Rulebook is limited as follows:

- The maximum amount which may be claimed in respect of a Loss is [Tbd].
- The cap on liability applies even if there has been gross negligence by the liable Participant, its employees or agents.
- The cap on liability does not apply in the event of wilful intent by the liable Participant, or by the Participant's employees or agents.
- The maximum amount which may be claimed in respect of a Loss is subject to proportionate reduction in the case of contributory negligence of the Participant making the claim, its employees or its agents.
- A Loss which results from action taken to limit or manage risk shall not be claimed.
- A Loss can be regarded as foreseeable only if it is regularly experienced by Participants active in making lookup requests related to cross border payments to SEPA countries.

2.6.3 Force Majeure

Further, a Participant shall not be liable for any failure, hindrance or delay in performance in whole or in part of its obligations under the Rulebook if such failure, hindrance or delay arises out of circumstances beyond its control. Such circumstances may include, but are not limited to, acts of God, criminal action, fire, flood and unavailability of energy supplies.

2.7 Liability of the EPC

The EPC, its agents, employees or the employees of its agents shall not be liable for anything done or omitted in the exercise of any discretion under the Rulebook unless it is shown that the act or omission was effected in bad faith.



The EPC, its agents, its employees and the employees of its agents shall not be liable for any losses which are not foreseeable.

2.8 Compliance

2.8.1 General

A Participant shall comply with the Rulebook, including amendments as and when they are made, properly communicated to Participants and effective.

The parties to the Rulebook are the EPC and each Participant.

The Rulebook is a multilateral agreement comprising contracts between:

- the EPC and each Participant; and
- each Participant and every other Participant.

A person who is not a party to the Rulebook shall have no rights or obligations under the Rulebook.

A Participant shall procure that its employees, its agents and the employees of its agents comply with all applicable obligations under the Rulebook.

2.8.2 Compliance and Adherence Committee/Appeals Committee

The Compliance and Adherence Committee (CAC) is responsible for performing the compliance function related to the Scheme. The role of the CAC is limited to the following:

- Adherence – the CAC shall be responsible for overseeing the adherence process for becoming a Participant in the Scheme; and
- Complaints – the CAC shall be responsible for investigating complaints made against Participants for alleged breaches of the Rulebook, evaluating such complaints and determining appropriate sanctions against Participants who are found to be in breach.

The rules covering the composition and organisation of the CAC are set out in [Document]³.

The Appeals Committee shall be responsible for hearing appeals brought in respect of decisions taken by the CAC in accordance with a fair process that is separate from the process of decision-making at first instance.

The rules covering the composition and organisation of the CAC are set out in [Document]⁴.

2.8.3 Complaints handling

2.8.3.1 Role of CAC in Complaints

The CAC shall oversee the implementation of the Rulebook by Participants. The CAC may investigate breaches or potential breaches of the Rulebook following a complaint made by a Participant to the CAC.

Unless otherwise stated, a complaint may be submitted by any Participant and must be filed in writing with the Secretariat. A complaint that is filed with the Secretariat must state the name of the Participant that is the subject of the complaint (the "Affected Participant") together with details of the complaint.

In addition, the CAC may investigate breaches or potential breaches of the Rulebook of its own accord.

³ Reference to the document to be added.

⁴ Reference to the document to be added.



For the purposes of this section, investigations made by the CAC into breaches or potential breaches of the Rulebook, whether or not initiated by the CAC itself, shall be referred to as complaints.

References to the CAC include any person nominated by the CAC to carry out a function in relation to a complaint, and where a complaint is made by or on behalf of the CAC itself, references to the "parties" are to the Affected Participant only.

2.8.3.2 Investigation of Complaints

The CAC may nominate a group of members of the CAC to investigate and evaluate a complaint or the CAC may delegate its power to investigate a complaint to the EPC Secretariat or any other person.

The CAC shall as soon as reasonably possible notify the Affected Participant that it is subject to investigation by the CAC. The Affected Participant shall have 28 Calendar Days from receipt of such notification to file written representations in respect of the Complaint. The Affected Participant may be required to cease any activity that could constitute conduct suspected of being in breach of the Rulebook.

CAC members investigating the complaint may in the course of the investigation call for such information and documentation from the Affected Participant as may be relevant for determining whether a breach of the Rulebook has taken place. The Affected Participant shall use reasonable efforts to provide such information to the relevant CAC members as is within the Affected Participant's possession, custody or control. The Affected Participant shall have 28 Calendar Days to respond to such requests for information and documentation.

The CAC may additionally require the Affected Participant to give all reasonable assistance in the course of the CAC investigation. A failure to provide such assistance shall be deemed to be a breach of Scheme rules and may therefore be actionable in accordance with this section.

In addition, in the course of the investigation, relevant CAC members may consult Participants as well as end-users and suppliers and may call for information and documentation, liaising through Participants.

CAC members investigating the complaint may engage any person in order to carry out tasks related to the investigation. The CAC may also engage a legal professional to give legal advice on any aspects of the investigation. Where this is done following EPC approval, the cost incurred by the CAC and paid by the EPC may be added by the CAC to the costs payable under section 2.8.3.9 below.

2.8.3.3 Evaluation of Complaint

The CAC shall evaluate any information that it may obtain in the course of the investigation. It may engage a skilled person in order to carry out tasks related to the evaluation of the complaint as well as a legal professional to give legal advice on any aspects of the evaluation and adjudication of the complaint at the cost of the EPC and within the budget of the EPC. The CAC may request advice from the EPC Legal Support Group ("LSG") to determine whether a Participant is in breach of the Rulebook. The CAC shall ensure that any person engaged in this manner shall be subject to a duty of confidentiality in respect of information acquired in the course of its engagement with the CAC.

In the course of this evaluation, the Affected Participant shall be invited to discuss the complaint with the CAC. The Affected Participant may seek legal advice at any stage of this process at its own cost.

When evaluating any complaint, the CAC shall take into account the date of the alleged breach and, except in exceptional circumstances at the discretion of the CAC or where



a breach is continuing, shall determine a complaint to be invalid which relates to a breach which occurred three years or more before the complaint is filed.

In the event of a complaint as to a Participant's compliance of their own rules, procedures and agreements with applicable legislation, regulations or generic supervisory requirements a complainant Participant should refer such matter to the relevant competent authority. The CAC – at its discretion - could also refer such matter to the relevant competent authority. Only if a complaint as to a Participants' compliance of their own rules, procedures and agreements with applicable legislation, regulations or generic supervisory requirements constitutes an issue of a scheme-wide importance such complaint shall be a matter for the CAC in respect of its investigations and possible sanctions.

For the sake of clarity, an issue of scheme-wide importance shall be understood to be a matter that could be seen as creating reputational damage to the Scheme or that could negatively affect the integrity or the proper functioning of the Scheme. The CAC may refuse complaints if it reaches the conclusion that a particular complaint at hand does not qualify to be of scheme-wide importance. The CAC may decide to consult with the Board in such matters before refusing a complaint.

2.8.3.4 Sanctions

On completion of the evaluation, the CAC shall prepare a report on the conduct of the case, setting out the facts of the case and a preliminary evaluation of the complaint. The CAC shall review the contents of this report, following which the CAC may consider that:

- no further action should be taken in relation to the alleged breach of the Rulebook if the CAC considers that either there is no evidence of a breach, or that the breach is of a trivial nature;
- discussions should take place with the Affected Participant to decide how to proceed in respect of a breach that has already occurred or one that is continuing - no sanctions are contemplated at this stage;
- discussions should take place with the Affected Participant and the Affected Participant should be sanctioned.

If the CAC considers that the Affected Participant should be sanctioned, the CAC shall send a written notice to the Affected Participant setting out details of the complaint and the sanction proposed, the report and any material that is believed to be relevant to the matter.

Subject to section 2.8.3.6, the Affected Participant shall have 30 Calendar Days following receipt of the notification to accept the sanction, or to present written or oral representations to the CAC (the "Representation Right"). The Affected Participant may consult legal counsel at any stage of the sanctioning process.

In considering any representations made to it, the CAC is not bound to follow rules of evidence, as followed in a court or tribunal. It will not normally consider oral evidence. Any party may however adduce written evidence in the course of the deliberations of the CAC and make such representations as it considers appropriate in accordance with this section.

Within 30 Calendar Days of hearing representations from the Affected Participant, the CAC shall determine the sanction to be made against the Affected Participant. The CAC shall notify the Affected Participant of its determination.

The sanctions available to the CAC are the following:

- private warning



- written notification of complaint
- public warning
- report to a national regulator or equivalent national authority, including a NASO
- termination

Private Warning

The CAC may give a private warning to the Affected Participant. The private warning shall constitute a formal notice to the Affected Participant and aims to deter the Affected Participant from committing a further breach of the Rulebook or to cease conduct that is in breach of the Rulebook. A record of the private warning shall be made by the CAC. This record shall be confidential.

Written Notification of Complaint

The CAC may give a written notification of a complaint to the Affected Participant. A written notification constitutes a formal reprimand to the Affected Participant. The written notification shall set out details of the breach and is aimed to deter the Affected Participant from committing a further breach of the Rulebook or to cease conduct that is on breach of the Rulebook. The CAC may publish details of this sanction on the EPC website.

Public Warning

The CAC may give a public warning to the Affected Participant. The public warning shall constitute a formal notice to the Affected Participant and aims to deter the Affected Participant from committing a further breach of the Rulebook or to cease conduct that is in breach of the Rulebook. The public warning shall publish the name of the Affected Participant, together with details of the breach, on the EPC website.

Circumstances which may indicate which Warning Sanctions may be applied

The decision as to which sanction or sanctions may be appropriate in respect of any Affected Participant shall be entirely at the discretion of the CAC. However, the following circumstances would tend to indicate that one of the above three sanctions would be more appropriate than the sanction of termination (described below):

- the conduct of the Affected Participant did not display bad faith nor was it due to gross negligence towards other Participants or to the Scheme;
- the conduct of the Affected Participant did not display dishonesty and the Affected Participant did not act in a grossly unprofessional manner;
- the breach was not of such a serious nature as to potentially undermine the operation and integrity of the Scheme;
- the Affected Participant had not committed a breach, or a breach of this type, in the past;
- the breach was of a nature that the CAC believes would be best addressed by deterrent action envisaged by these three sanctions and that it remains appropriate for the Affected Participant to continue as a Participant in the Scheme rather than facing expulsion under the sanction of termination; and
- the breach can be rectified without loss or cost to any other Participant or user or the EPC.

As regards which of the three Warning Sanctions might be applicable to any case:



- a private warning may generally be considered more appropriate for a first breach where the breach was not of a serious nature, had not adversely affected other Participants or the Scheme, and there would be no merit in other Participants being informed of the breach;
- a written notification of complaint, being a formal reprimand, would be applied where the CAC considered the breach to be of a sufficiently serious nature to record a reprimand against the firm. The CAC may consider publishing the notification on its website if it believed this would be in the interests of other Participants and/or the Scheme;
- a public warning, being a formal notice, would be applied in the case of a more serious breach and where the CAC believes it would be in the interests of other Participants and/or the Scheme to publicise the notice. This sanction is the most likely of the three to be used in conjunction with the sanction of termination.

Report to National Regulator

In addition to giving a private warning, public warning or written notification of breach, the CAC may report the Affected Participant to its national regulator or to an equivalent national authority. The regulator shall be provided with the name of the Affected Participant together with details of the conduct of the Participant.

Considerations which may indicate the appropriateness of this sanction would be if the CAC believed that the breach by the Affected Participant may also constitute a breach of the rules or guidelines of a relevant regulator or if the Affected Participant's conduct cast doubt on its fitness and propriety to continue as a regulated entity. However, the decision whether or not to report a breach by an Affected Participant to a regulator will be entirely at the CAC 's discretion.

Termination

In addition to making a report to a relevant national regulator or giving a private warning, written notification of breach or public warning to the Affected Participant, the CAC may terminate the Scheme participation of an Affected Participant in the following circumstances:

- where the breach committed by the Affected Participant is sufficiently serious to undermine the operation and integrity of the Scheme;
- where the Affected Participant has committed a repeated breach of the Rulebook, notwithstanding any earlier sanctions given to the Affected Participant by the CAC;
- where the conduct of the Affected Participant displays bad faith or gross negligence towards other Participants or towards the Scheme; or
- where the conduct of the Affected Participant displays dishonesty or is grossly unprofessional.

Before making a termination order, the CAC may consult with relevant groups to determine the impact of the sanction. Such groups may include other Participants, the Board, the SPL provider(s) or PSP communities. The CAC shall consult with relevant regulators before applying the termination sanction.

If the CAC decides to terminate the participation of an Affected Participant, it shall make a termination order setting out the terms and conditions on which the termination is to be effected. Such an order shall set out the steps to be taken by the Affected Participant to ensure the continued orderly and efficient operation of the Scheme.

In the event of termination, the Affected Participant shall be barred from exercising rights under the Rulebook in accordance with the terms and conditions set out in the



termination order. The Affected Participant shall fulfil all obligations arising under the Rulebook in accordance with the termination order.

If the participation of an Affected Participant is terminated, the Affected Participant may re-apply to join the Scheme after 6 months, starting from the date of the termination of its participation. However, an Affected Participant may re-apply earlier if it can demonstrate to the CAC that it has remedied the breach and/or that there is no reasonable likelihood of the Participant committing the breach in future.

The CAC may publish details of a termination of participation on the EPC website together with the relevant order and details of the conduct giving rise to the complaint.

2.8.3.5 Emergency Injunction Procedure

Where a termination order is issued to an Affected Participant, such Affected Participant may within 21 Calendar Days of receiving notification of the order, apply for an injunction against such order to a competent court in Brussels, during which time the sanction shall be suspended pending the court's determination of the matter. Where the court decides not to grant the injunction requested by the Affected Participant, the CAC may enforce the conditions of the termination order. The courts of Belgium shall have exclusive jurisdiction in respect of proceedings brought in accordance with this section.

2.8.3.6 Appeals Arising from Complaints

Within 30 Calendar Days of receiving the notification of a sanction, the Affected Participant may appeal to the Appeals Committee in accordance with section 2.8.4.

2.8.3.7 Timing of Sanctions

Except in exceptional circumstances described in more detail below, a determination by the CAC of a sanction to be made against an Affected Participant shall not take effect until the conclusion of appeals proceedings before the Appeals Committee that may be commenced in accordance with the Rulebook, or until such time as the time period for referring a matter to an appeal to the Appeals Committee has expired in accordance with the Rulebook.

Of all sanctions available to the CAC, the imposition of the following sanctions only shall be suspended awaiting the determination of the appeal: (i) public warning, (ii) report to national regulator or equivalent national authority and/or (iii) termination.

The following applies only if the CAC considers that the conduct or circumstances of the Affected Participant will undermine the operation of the Scheme or would cause a serious risk of undermining the operation of the Scheme. The CAC may impose a sanction of which it has notified the Affected Participant with immediate effect, or at any other time specified by the CAC. In particular, the CAC may impose a sanction in such circumstances even though the Representation Right has not expired; or any appeal under section 2.8.4 has not yet been determined.

However, both the Representation Right and the right to appeal against any sanction will remain available to any Affected Participant notwithstanding the expedited imposition of any sanction.

The decision whether or not to expedite the imposition of sanctions under this section shall be entirely at the discretion of the CAC, however, issues which would tend to indicate the need for such action would be insolvency, loss of regulatory licence(s), or criminal conviction of the Affected Participant.

In cases where a sanction takes effect with immediate effect or at any other time specified by the CAC, the sanction shall remain in force for as long as determined by the CAC or until it is revoked by a determination of the case at appeal. No Affected Participant will have any right of recourse against the CAC for any loss suffered due to



the imposition of a sanction if a sanction is subsequently revoked on appeal or under any other circumstances.

2.8.3.8 Eligibility, Merger and Acquisition of a Participant

In addition to the circumstances set out in section 2.8.3.7, the CAC may investigate, initiate or respond to a complaint in the following circumstances:

- a Participant has failed to satisfy one or more of the Scheme eligibility criteria; and
- a Participant has failed to notify the EPC of its intention to terminate its participation.

The CAC may treat evidence of the existence of these circumstances coming to its attention as if it were a formal complaint, and deal with the matter in accordance with section 2.8.3.7 of the Rulebook. Any references to a 'breach' of the Rulebook in section 2.8.3.7 shall include a breach of the Adherence Agreement (including the representations and warranties set out in the Adherence Agreement) entered into by the Participant and may be treated by the CAC as being references to the circumstances set out in this section.

2.8.3.9 Costs

An upfront, non-refundable administrative fee published on the EPC website will be payable by the complainant to the EPC, upon lodging the complaint, to cover basic administrative costs. This fee will be recoverable from the losing party, as appropriate.

The EPC will ensure that any fee set under this section is quantified so as to be consistent with the costs incurred by the EPC and the EPC's status as a non-profit association under Belgian law. In addition, any relevant non-administrative costs incurred during the course of the proceedings will be recovered from the losing party.

Where the complaint is withdrawn by the complainant before a formal CAC decision on the complaint has been made, the CAC's costs incurred to handle the complaint proceedings up to that point in time will be recovered from the complainant.

Where the CAC initiates a complaint, it may require the Affected Participant to contribute to any costs incurred by the CAC in relation to the complaint, if the Affected Participant were found to be in breach of the Rulebook.

2.8.4 Appeals

2.8.4.1 Introduction to the Appeals Process

In this section and unless the context otherwise indicates, a reference to the Appeals Committee shall be read as a reference to those persons comprising the Appeals Committee who have been nominated to carry out the Appeals Function of Scheme Management in accordance with [Document].

Where the decision under appeal is a decision in which the CAC had initiated a complaint under section 2.8.3 of the Rulebook, the CAC is not to be regarded as a "party" to the appeal.

The role of the Appeals Committee shall be to determine whether, on the basis of the material put before it by the appellant, a decision reached in complaints and adherence matters was correct and justified.

2.8.4.2 Submission of Appeals Notice

A person with the right to an appeal under the Rulebook must file an appeals notice with the Secretariat. An appeals notice shall set out details of the case under appeal, reasons supporting the appeal, together with a copy of the determination that is the subject of the appeal.



Within 21 Calendar Days of receiving the appeals notice, the Secretariat shall provide a copy of the appeals notice to the CAC. The CAC members shall have 21 Calendar Days to file written representations in respect of the appeal. They may appoint one or more representatives from their number to take the appeal forward on their behalf.

The Appeals Committee shall then consider the appeals notice and any representations filed and, within 21 Calendar Days of receiving representations from each party, shall notify all parties of the date of the appeal meeting.

At any time before the date of the meeting, the Appeals Committee may, but is not obliged to make such directions to the parties as may be useful for the swift and fair determination of the appeal. Such directions may include the following:

- directions to exchange documents relevant for the appeal; and
- directions to exchange names and written statements of any witnesses, including expert witnesses (if any).

The Appeals Committee shall ensure that all documents and evidence received from the CAC by the Appeals Committee or by one or other of the parties is provided to all the parties to the appeal in a timely manner in advance of the appeal meeting.

2.8.4.3 Meeting

The Appeals Committee shall aim to determine the appeal between the parties in a manner that is fair, open and amicable at a meeting involving all relevant parties.

Unless otherwise agreed, this meeting shall be private. Parties may bring legal representatives to a meeting.

In the event that a party does not attend the meeting, or if both parties do not attend, the Appeals Committee may arrive at such determination as it considers appropriate or may postpone the date of the meeting.

The Appeals Committee shall consider all the material put before it and allow the parties to make oral representations during the meeting.

The Appeals Committee shall then deliver a decision on the appeal.

The Appeals Committee may make either of the following determinations:

- confirm, vary, or reverse the decision of the CAC at first instance;
- impose any sanction that may have been imposed but was not imposed by the CAC at first instance.

The Appeals Committee may publish the details of the appeals decision on the website of the EPC. Any decisions of the CAC at first instance that are published on the website of the EPC, if varied or reversed at appeal, shall be amended accordingly on the EPC Website.

A party to an appeal may withdraw from the appeal at any time by giving notice to the Appeals Committee. The appeal shall be closed with immediate effect and the Appeals Committee may make such determination in respect of the subject matter of the appeal and in respect of the allocation of costs for the appeal as may be appropriate.

2.8.4.4 Costs

An upfront, non-refundable administrative fee published on the EPC website will be payable to the EPC upon lodging the appeal, by the party filing the appeal in question, to cover basic administrative costs. This fee will be recoverable from the losing party, as appropriate.

The EPC will ensure that any fee set under this section is quantified so as to be consistent with the costs incurred by the EPC and the EPC's status as a non-profit



association under Belgian law. In addition, any relevant non-administrative costs incurred by the EPC during the course of the proceedings will be recovered from the losing party.

Where the appeal is withdrawn by the appeal filing party before a formal Appeals Committee decision on the appeal has been formulated, the EPC's costs incurred to handle the appeal proceedings up to that point in time will be recovered from the appeal filing party.

Where there is a sole party to the appeal, the Appeals Committee shall have the power to require that party to bear the EPC's costs in respect of the appeal, if that party were found to be in breach of the Rulebook.

2.8.4.5 Further Steps

Following the determination of the Appeals Committee, if a party to the appeal does not consider the issue to have been correctly resolved, it shall be open to that party to attempt to resolve the matter through such means as it considers appropriate, including litigation in a competent court in Brussels. As the EPC shall always be a defendant in such proceedings, the courts of Brussels shall have exclusive jurisdiction in respect of proceedings brought in accordance with this section. Such a party may challenge the decision before the courts of Brussels, but only on the grounds of a serious breach by the EPC of the Rulebook or of a breach of mandatory rules of law, or on the grounds that the decision, when subject to a prima facie review (examen marginal / marginale toetsing) by the court, appears manifestly incorrect.

2.9 Termination

A Participant may terminate its status as a Participant by giving no less than one (1) months' prior written notice to the Secretariat, such notice to take effect on a designated day. As soon as reasonably practicable after receipt of such notice, it shall be published to all other Participants in an appropriate manner.

Notwithstanding the previous paragraph, upon receipt of the Participant's notice of termination by the Secretariat, the Participant and the Secretariat may mutually agree for the termination to take effect on any day prior to the relevant designated day.

A former Participant shall continue to be subject to the Rulebook in respect of all activities which were conducted prior to termination of its status as a Participant and which were subject to the Rulebook, until the date on which all obligations to which it was subject under the Rulebook prior to termination have been satisfied.

Upon termination of its status as a Participant, an undertaking shall not incur any new obligations under the Rulebook. Further, upon such termination, the remaining Participants shall not incur any new obligations under the Rulebook in respect of such undertaking's prior status as a Participant. In particular, no new lookup request obligations may be incurred by the former Participant or in favour of the former Participant.

The effective date of termination of a Participant's status as a Participant is (where the Participant has given notice in accordance with the first paragraph of the present section) the effective date of such notice, or (in any other case) the date on which the Participant's name is deleted from the Register of Participants, and as of that date the Participant's rights and obligations under the Rulebook shall cease to have effect except as stated in this section 2.9

This section, as well as sections 2.6, 2.7, 2.10 and 2.11 of the Rulebook shall continue to be enforceable against a Participant, notwithstanding termination of such Participant's status as a Participant.



2.10 Intellectual property

The Participants acknowledge that any copyright in the Rulebook belongs to the EPC. The Participants shall not assert contrary claims, or deal with the Rulebook in a manner that infringes or is likely to infringe the copyright held by the EPC in the Rulebook.

2.11 Contractual provisions

The Rulebook contains legal obligations which are binding on the Participants and which are enforceable against a Participant by the EPC or another Participant. The whole Rulebook is intended to have legal effect. In the event of any inconsistency between the provisions of the Rulebook, the provisions of this Chapter 2 shall prevail. Subject to the prevalence of provisions in this Chapter 2, the provisions of Chapter 3 shall prevail over any other provision in the Rulebook.

In the event of an inconsistency between the provisions of the Rulebook and any other agreement or convention between the Participants and the EPC in relation to the subject matter of this Rulebook, the provisions of this Rulebook shall prevail.

Every document that is required to be provided under the Rulebook shall be provided in the English language.

Any reference in the Rulebook to a person or an undertaking (howsoever described) shall include its successors.

Headings in the Rulebook are used for ease of reference only.

The Rulebook is drawn up in the English language. If the Rulebook is translated into any other language, the English language text prevails.

2.12 Applicable legislation

Each Participant that is not subject to the General Data Protection Regulation (GDPR)⁵ under its national law shall vis-à-vis other Participants and vis-à-vis its Customers and to the extent permitted by the national law applicable to such Participant, comply with and perform obligations that are substantially equivalent to those provisions in the GDPR which are relevant for lookup requests.

Further, each Participant (whether or not subject to the GDPR) shall refrain, to the extent reasonably possible, from exercising any rights accorded to it under its national law vis-à-vis other Participants and vis-à-vis its Customers that either conflict or that could potentially conflict with the provisions of the GDPR.

2.13 Governing law

The governing laws of the agreements in relation to the Scheme are as follows:

- The Rulebook is governed by Belgian law.
- The Adherence Agreement is governed by Belgian law.

Each Participant shall refrain, to the extent reasonably possible, from exercising any rights accorded to it under its national law vis-à-vis other Participants and vis-à-vis its Customers that either conflict or that could potentially conflict with the provisions set forth in the Rulebook and the Adherence Agreement.

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.



3. Scheme Management

3.1 SPL Scheme Participant Group

3.1.1 Composition of the SPL Scheme Participant Group

The SPL Scheme Participant Group (SPL SPG) will consist of a maximum of 30 members drawn from representatives of registered, committed or “interested” eligible Participants (see section 2.1 for eligibility criteria).

The composition of the SPL SPG will be initiated by the Nominating and Governance Committee (NGC), with a call for candidates published through the EPC Secretariat. The Board will approve the final composition. The same procedure will apply to subsequent vacancies and additions. The composition of the SPL SPG will be well balanced in terms of geographic representation and types of institution represented.

Each member is entitled to appoint one alternate, subject to NGC approval. An alternate may only attend a meeting when the principal member is unable to attend.

The Chair will be elected by the Board following a recommendation by the NGC that the candidate(s) meet(s) the profile for the role. The Chair will be responsible for proactively guiding the Group in meeting its deliverables and ensuring coherence with EPC objectives.

The Secretary of the Group will be provided by the EPC Secretariat. The Secretary supports the Chair and is accountable for ensuring compliance with EPC processes.

3.1.2 Organisation

The SPL SPG will meet physically or by telephone/web conference, according to the demands of its work programme.

Calls for SPL SPG meetings and draft agendas will be issued at least two weeks in advance and meeting papers will be provided at least one week in advance. Minutes of meetings will be made available by the EPC Secretariat to all SPL SPG members within three weeks of the corresponding meeting.

The SPL SPG will develop its conclusions and recommendations on the basis of broad consensus. In circumstances where such consensus is not achievable, and the matter is appropriate for the conduct of a vote, a vote may be taken and, for this to be binding on the group, a 2/3 majority on the basis of a quorum of 2/3 of the Group membership must be obtained.

3.1.3 Mandate

The SPL SPG holds its mandate from and is accountable to the Board. It will hold its mandate until otherwise directed by the Board.

The SPL SPG is expected to be replaced by a dedicated governance body (SPL Scheme Management Board) as per decision of the Board.

The members of the SPL SPG will at all times execute their mandate in accordance with the stipulations of the EPC Code of Conduct on competition law (EPC212-14), as amended from time to time.

3.1.4 Scope

The SPL Scheme Participant Group shall be responsible for performing the following functions of SPL Scheme management:

- Maintenance and evolution of the Scheme rules;
- Proposal of any extension of the scope of the Scheme, for final approval by the Board;



- Monitoring of the general quality level of the service (not day-to-day) rendered by the available SPL service provider(s) and its compliance with the Scheme rules, based on SPL service users' feedback;
- Organisation of the procurement of the SPL service on behalf of SPL service users (when renewal of the contract is due and as long as a single preferred provider solution is appropriate);
- Proposal of the annual work plan, budget and Participant fees, for final approval by the General Assembly.

The SPL Scheme Participant Group can decide to set up subgroups for the elaboration of the agreed deliverables. The SPL Scheme Participant Group will designate the Chair and outline the mandate, scope and deliverables of the subgroups. The subgroups will report to the SPL Scheme Participant Group.

3.2 Maintenance and Evolution (change management process)

3.2.1 Guiding principles

It is a key objective of the EPC that the Scheme is able to evolve with an evolving payments market. To meet the demands of the Participants and Stakeholders including end-users and PSP communities, the Scheme shall be subject to a change management process that is structured, transparent and open, governed by the rules of the management and evolution function of SEPA Scheme Management.

The key principles underpinning change management are the following:

- Innovation - the Scheme shall be open to innovative proposals to improve delivery of the Scheme in order that the Scheme is competitive, efficient and able to benefit from the latest developments in payments technology.
- Compliance with applicable legislation and regulation - the Scheme shall be and remain at all times in compliance with the relevant Belgian and EU legislation and with any relevant regulatory requirements.
- Transparency - the change management process shall be transparent and open so that changes implemented into the Scheme are carefully considered and scrutinised. Establishing open channels for Participants, end-users and suppliers to propose changes is a key aim of change management.
- Impact analysis - proposals for change are supported, where appropriate, by a careful analysis evaluating its impact on the Scheme to ensure that implemented changes are viable.
- Development of an integrated European landscape (SEPA) – The Scheme is an important platform for Participants to develop SEPA-enabled products and services that allow both end-users and Participants to take advantage of the development of and investment in SEPA.

3.2.2 Role of the SPL SPG

The change management process of the Scheme shall be performed by the SPL SPG who will formulate recommendations on the Change Requests received and interact with Stakeholders and end-users on the evolution of the Scheme and implement changes, taking into account the overall strategy and policy goals of SEPA and the EPC, identifying key needs and finding appropriate solutions.



3.2.3 Submission of Change Requests to the Secretariat

A Change Request denotes any concrete and comprehensible proposal for making a change to the Scheme which is to be presented along with a substantiated reasoning on why and how it concerns the Initiator (or the Stakeholders it is representing). A Change Request may be devised by any individual or organisation that is able to claim a legitimate interest in this change management process and is submitted to the Secretariat.

A Change Request shall be submitted to the Secretariat in accordance with the rules set out in this section. Change Requests shall be submitted in all cases in accordance with a format which will be published for this purpose on the EPC website.

The Initiator needs to substantiate the interests it represents (e.g., a specific institution, an association of institutions at national or at SEPA-level) in order that the SPL SPG and any contributor during the public consultation can understand the potential impact of the Change Request on the concerned Participant or stakeholder.

It is recommended that different individuals or organisations representing as a whole a specific stakeholder community at national and/or at SEPA level through e.g., an association or a representative body, agree first on a joint Change Request on that stakeholder community level and then submit it to the Secretariat. Such a joint Change Request will ease the Change Request review process for the SPL SPG prior to the public consultation and for the contributors when analysing the Change Requests during the public consultation.

It is recommended that the Initiator supports the Change Request, where appropriate, with an impact analysis. Such an impact analysis emphasises the merits of the Change Request and can influence the formulation of the SPL SPG recommendation on the Change Request prior to the start of the public consultation and the opinion of the contributors when analysing the Change Requests during the public consultation.

3.2.4 Acknowledgement of Receipt of a Change Request

The Secretariat shall acknowledge receipt of the Change Request to the Initiator within 5 business days of receiving the Change Request. An acknowledgement of receipt does not imply that a Change Request has been accepted but only that the Change Request has been received.

3.2.5 Consideration of a Change Request

The SPL SPG shall analyse (a) whether the change as suggested in a Change Request falls within the scope of the Scheme and (b) whether the change proposed by the Change Request is a Minor Change or a Major Change.

In respect of (a), as part of this analysis, the SPL SPG shall consider the change proposed by a Change Request in accordance with the following broad criteria:

- the change presents a case for wide SEPA market-acceptance;
- the change is sufficiently concrete
- the change is feasible to implement; and
- the change must not compromise SEPA-wide interoperability of the Scheme or the integrity of the Scheme.

In respect of (b), the SPL SPG shall assess whether a Change Request proposing a change can be defined as a Minor Change or a Major Change.



A Minor Change is a change of an uncontroversial and usually technical nature that facilitates the comprehension and use of the Rulebook. Clarifications of existing rules shall not be deemed to affect the substance of the Rulebook or the Scheme and will therefore be a Minor Change. More information about the process for Minor Changes is set out in section 3.2.8 of this Rulebook.

A Major Change by contrast is a change that affects or proposes to alter the substance of the Rulebook and the Scheme. Examples of such changes include the proposals for new services to be offered in the Scheme, or changes affecting policy. Changes that are classified as Major Changes are approved through detailed consultation.

Change Requests that impact the SPL API specification (see Annex 4) might need to be submitted to the Berlin Group (in line with their change management process). This in view of the fact that the SPL API specification uses data elements that are described in the repository level of the Berlin Group's Mobile P2P Interoperability Framework.

3.2.6 Publication of Change Requests

All Change Requests that comply with the published EPC template for Change Requests and with the section 3.2.5 of this Rulebook shall be submitted for Public Consultation. The SPL SPG shall provide the Initiator with a written response before the start of the Public Consultation indicating the reasons in the event that a Change Request cannot be considered for the Public Consultation.

3.2.7 Process for Major Rulebook changes

3.2.7.1 Preparation of SPL SPG Recommendation

Once a Change Request from the Initiator has been classified as a Major Change by the SPL SPG, the SPL SPG is responsible for analysing in detail the submitted Change Request (and if provided the related impact analysis) and for preparing its Recommendation for the Public Consultation.

The analysis of the SPL SPG will also indicate if the Change Request meets the criteria set out in section 3.2.5 of this Rulebook. The SPL SPG may ask the Initiator to provide an impact analysis to demonstrate the potential of the Change Request.

The SPL SPG will determine whether any Change Request which includes a request for expedited implementation in accordance with section 3.2.9 of this Rulebook on grounds that the proposed change constitutes a non-operational change, does indeed qualify as such. If the SPL SPG is satisfied that a Change Request would have no operational impact on Participants and that it is suitable for an expedited implementation, the SPL SPG will make a recommendation to the Board that the Change Request is implemented as a non-operational change in accordance with section 3.2.9.

Where the change as presented in the Change Request proposes to modify the Rulebook, the SPL SPG recommendation on the basis of the Change Request shall also show the likely amendments to be made to the Rulebook in case of implementing the proposed change.

The SPL SPG shall make all reasonable efforts to complete the analysis and its recommendation for each Change Request in a timely manner. Each Change Request will be given one of the SPL SPG Recommendation options below:

- a. The change is already provided for in the Scheme: no action is necessary for the EPC.
- b. The change should be incorporated into the Scheme: The Change Request becomes part of the Scheme and the Rulebook is amended accordingly.
- c. The change should be included in the Scheme as an optional feature:
 - The new feature is optional, and the Rulebook will be amended accordingly.



- Each Participant may decide to offer the feature to its customers, or not.
- d. The change is not considered fit for the SEPA geographic area.
- e. The change cannot be part of the Scheme:
- It is technically impossible or otherwise not feasible (to be explained on a case by case basis).
 - It is out of scope of the Scheme.

The SPL SPG will share the Public Consultation Document containing the Change Requests and the related SPL SPG recommendations with the Board prior to the start of the Public Consultation on the Change Requests.

3.2.7.2 Dialogue with the Initiator

In the course of developing its recommendation on the Change Request, the SPL SPG may consult with the Initiator for clarification purposes. To that end the SPL SPG can invite the Initiator to present its Change Request(s).

The Initiator can also ask the Secretariat to present its Change Request in further detail to the SPL SPG.

3.2.7.3 Public Consultation on Change Request

Once the SPL SPG has concluded on its recommendations related to each Change Request, the SPL SPG shall begin the process of consulting Participants and Stakeholders on the submitted Change Requests, via a Public Consultation. The Public Consultation shall start with the publication of the Public Consultation Document on the EPC website.

The SPL SPG shall aim to conclude the Public Consultations after 90 Calendar Days of publication of the Public Consultation Document on the EPC website.

Participants are requested to inform whether they support or not the Change Request or the related SPL SPG Recommendation. Participants may provide comments on the Change Requests to the SPL SPG.

3.2.7.4 Process following Public Consultation

The SPL SPG shall collect and analyse the support for each Change Request and the comments received from all Participants and Stakeholders and shall develop its Change Proposals based on the comments received from the Public Consultation.

A Change Proposal as developed by the SPL SPG may bring together more than one change, developed from one or more Change Requests.

The SPL SPG will consolidate the Change Proposals, along with each Change Request and the related non-confidential comments received from the contributors during the Public Consultation, in the Change Proposal Submission Document.

The Change Proposal Submission Document shall indicate that each stage of the change management process, from initiation to consultation, has been properly completed in respect of the Change Request submitted.

The Change Proposal Submission Document is then submitted to the Board for decision-making purposes in accordance with section 3.2.7.3 of this Rulebook.

3.2.7.5 Board Deliberations on the SPL SPG Change Proposal Submission Document

The Board deliberates on the Change Proposal Submission Document from the SPL SPG.



3.2.7.6 Publication

The Change Proposal Submission Document submitted to the Board shall be published on the EPC website along with the decision of the Board on each Change Proposal. The SPL SPG shall publish all Change Requests and Change Proposals, irrespective of whether the change has been accepted or rejected by the Board.

3.2.7.7 Exceptional Change

In exceptional circumstances, the Board can approve the urgent implementation of a Change Proposal only in cases whereby the failure to implement a change may result in a disruption to the Scheme or to users of the Scheme (e.g., material mistakes or significant flaws in the Scheme are reported).

The SPL SPG shall prepare an Exceptional Change Proposal Submission Document for submission to the Board alongside the Exceptional Change Proposal.

The Board shall determine whether or not to accept the Exceptional Change Proposal.

An Exceptional Change Proposal that has been considered by the Board shall be published on the EPC website together with the Exceptional Change Proposal Submission Document and the decision of the Board.

The EPC may implement an Exceptional Change Proposal, as approved by the Board, at the earliest from the business day following the date on which the Exceptional Change Proposal is published on the EPC website. Such date will be determined by the Board on a case by case basis.

3.2.7.8 Change for regulatory reasons

The creation of or amendments to relevant rules and regulations might necessitate the urgent alignment of the Scheme with such rules and regulations.

In such case the SPL SPG will prepare a Regulatory Change Proposal. This will be done as soon as reasonably possible, in light of the date on which the new or amended rules and regulations will enter into force.

The SPL SPG shall complete a Regulatory Change Proposal Submission Document for submission to the Board alongside the Regulatory Change Proposal. The Regulatory Change Proposal Submission Document shall specify that the change proposed relates to a mandatory rule of law, and the reasons why the regular change management process could not be followed.

The Board shall determine whether or not to accept the Regulatory Change Proposal.

A Regulatory Change Proposal that has been considered by the Board shall be published on the EPC website together with the Regulatory Change Proposal Submission Document and the decision of the Board.

The EPC may implement a Regulatory Change Proposal, as approved by the Board, at the earliest from the business day following the date on which the Regulatory Change Proposal is published on the EPC website. Such date will be determined by the Board on a case by case basis following consideration of a recommendation from the SPL SPG and the LSG.

3.2.8 Process for Minor Rulebook changes

The SPL SPG shall notify the list of Minor Changes within the Public Consultation Document used for Major Rulebook Changes (see section 3.2.7.3 of this Rulebook).



As Minor Changes do not affect the substance of the Rulebook or the Scheme, the contributors taking part in the Public Consultation are not requested to provide comments to these Minor Changes. These Changes will also be included in the SPL SPG Change Proposal Submission Document (see section 3.2.7.4 and 3.2.7.5 of this Rulebook).

In the event that the SPL SPG receives extensive comments on the list of Minor Changes, where some items on the list are identified by contributors as potentially Major Changes, the SPL SPG may remove the item from the list and consider re-classifying this item.

The SPL SPG shall consult with the relevant Initiator(s) on the status of the item with a view to determining whether a change is a Minor or a Major Change. Following such a consideration, the change may be re-classified and approved as a Major Change.

3.2.9 Frequency of the change management process

The frequency of the change management process will be assessed and based on market needs and communicated well in advance.

4. SPL Service Provider(s)

4.1 SPL service provider(s)

The EPC will license at least one provider to operate the SPL service. Interoperability needs to be ensured in case more than one provider is operational.

4.2 Roles

An SPL service provider needs to operate the SPL service in accordance with the Rulebook and SPL API specification, as amended from time to time.

The following operational principles apply:

- The SPL service only ever returns one IBAN and one corresponding name (unless it cannot be provided) or alias in response to a lookup.
- In a scenario whereby, multiple solutions have a claim on the same proxy, the polling hierarchy logic as described in Annex 3 will come into effect.

The following general principles apply:

- The service is an online service for the purpose of real-time one-off lookups that are provided within established maximum response times.
- The service shall take (among other things) a proxy as an input and will yield (among other things) an IBAN and certain information on the associated account holder defined in the Scheme rules.
- The service maintains an updated directory of Participants and functions according to Scheme-compliant processes that enables qualifying Participants to join and leave the lookup service.
- All things being equal, a given lookup shall result in the same (identical) response with regard to the IBAN produced every time.
- The service will keep track of queries processed for the purpose of providing an audit trail to relevant parties involved.
- Participants will ensure that (contractual and implicit) privacy expectations of end users (both on the sending and receiving end of transactions) are met.

4.3 Obligations

The SPL service provider(s) shall:



- Inform the EPC regarding changed specifications in the execution of the SPL service.
- Inform the EPC in case of changes in related SPL service provider documentation.
- Be responsible for the client specific Service Level Agreement (“SLA”) including the agreement regarding the duration of the SLA.
- Provide EPC with quarterly statistics on:
 - Number of (un)successful responses.
 - Response time per RRP.
 - Transit time of SPL service provided.
 - SPL service availability and performance.

4.4 Liabilities

The commercial liabilities of the SPL service provider(s) will be defined by the legal agreements signed by the SPL Service provider(s) and IRP/RRPs.

5. Terms defined

Term	Definition
Alias	An alternative name. In case of a person this would be any name different than the birth name. For a company there could be a difference between the legal and commercial name.
IBAN	International Bank Account Number.
IRP	Initiating Registry Provider: entity which makes a lookup request into the SPL, in accordance with the Rulebook.
Proxy	Data required by the SPL service in order to retrieve a payment account identifier. Initially the proxy is the mobile phone number of the beneficiary of the payment.
RRP	Responding Registry Provider: entity which responds to a lookup request from the SPL, in accordance with the Rulebook.
SEPA geographic area	SEPA countries listed in the EPC List of SEPA Scheme Countries (document EPC409-09, as amended from time to time).
SPL	SEPA Proxy Lookup. A directory service which will initially forward to the IRP an IBAN associated to a mobile phone number provided by an RRP.
SPL Service provider	Entity which operates the SPL service, the software and the services related to it in accordance with the Rulebook.



ANNEXES

TABLE OF CONTENTS

1	Adherence agreement.....	30
2	Schedule information to the Adherence Agreement.....	32
3	Polling hierarchy logic	34
4	Scheme Management Cost Allocation	34
5	SPL API Specification	35
5.1	Scope.....	35
5.2	Introduction	35
5.3	Terminology & List of Acronyms.....	36
5.4	Applicable Documentation.....	36
5.5	Requirements for the Entities Participating in the SPL Service.....	37
5.5.1	Components and Interfaces for Interoperability.....	37
5.5.2	List of functionalities to be supported by the SPL Service Provider(s)	38
5.5.3	Responsibilities of the IRP	39
5.5.4	Responsibilities of the RRP.....	40
5.6	API Specifications	41
5.6.1	Introduction	41
5.6.2	Berlin Group “Mobile P2P Interoperability Framework”	41
5.6.3	API for the communication between the IRP and the SPL.....	42
5.6.4	API for the communication between the SPL and the RRP	42
5.7	Data Elements.....	42
5.7.1	Introduction	42
5.7.2	List of Data Elements for the SPL Request	43
5.7.3	List of Data Elements for the SPL Response	45
5.7.4	Possible Return and Response Codes	47
5.8	SPL Service Logic.....	48
5.8.1	Overview.....	48
5.8.2	Polling Hierarchy	49
5.8.3	Routing Algorithm	50
5.9	SPL Security Architecture.....	50
5.9.1	Problem Statement.....	50
5.9.2	Security Objectives.....	51
5.9.3	Security Requirements.....	51
5.9.4	Security architecture implementation aspects	52
5.10	Data Protection Requirements	52



1 Adherence agreement

SPL Scheme	SEPA PROXY LOOKUP SCHEME ADHERENCE AGREEMENT				
	Date received by EPC: _____				
	Check	Y/N	Date	Initials	Narrative
	Adherence Agreement check OK				
	Plausible readiness date				
	Contact e-mail address				
	Entered into Register as "received"				
	The above is exclusively for use by EPC – please leave blank				
	SEPA Proxy Lookup (SPL) Scheme Adherence Agreement				
	To:	The European Payments Council AISBL (the "EPC")			
	From:	Name of Applicant[s]*:			
		[As set out in the list annexed to this Adherence Agreement]*			

		([each]* an " Applicant ")			
SPL Scheme	*Please include the text in square brackets if this Adherence Agreement covers more than one entity.				
	PREAMBLE				
	(A) The Single Euro Payments Area (SEPA) Proxy Lookup (SPL) Scheme (the " Scheme ") is a pan-European lookup Scheme that operates in all SEPA countries, as listed in the EPC List of SEPA Scheme Countries (document EPC409-09, as amended from time to time). The SPL Scheme covers the exchange of the data necessary to initiate payments between proxy-based payment solutions on a pan-European level. It aims to facilitate interoperability between participating payment solutions.				
	(B) The EPC oversees the operation of the Scheme in accordance with the terms and conditions set out in the SEPA Proxy Lookup Scheme Rulebook (the " Rulebook ").				
SPL Scheme	(C) The Rulebook sets out the rights and obligations of all institutions bound by its terms (the " Participants "), and the EPC and binds each Participant to comply with their obligations to the EPC and to all other Participants pursuant to the rules set out therein.				
	(D) The EPC, acting on its behalf and on behalf of all Participants, will notify the Applicant of the date following the Readiness Date on which this Adherence				



SPL Scheme	<p>Agreement becomes effective (the “Effective Date”) as between the Applicant, the EPC and other Participants.</p>
	<p>(E) As of the Effective Date the Applicant shall become a Participant and be bound to all the obligations, and entitled to all the benefits, set out in the Rulebook.</p>
SPL Scheme	<p>IT IS HEREBY AGREED AS FOLLOWS:</p>
	<p>1. The Applicant hereby undertakes to all Participants and to the EPC to perform the obligations imposed by and to comply with the provisions of the Rulebook, as modified from time to time, with effect from the Effective Date.</p>
	<p>2. The Applicant makes the following representations and warranties:</p>
	<p>2.1. The Applicant has the power and authority to enter into and has taken all corporate action to authorise its entry into the Scheme and to perform the obligations and comply with the provisions of the Rulebook.</p>
	<p>2.2. The signatories of the Applicant [and the agent signing on behalf of the Applicant] have all necessary corporate authorisations and the power and authority to bind the Applicant to the Rulebook.</p>
	<p>2.3. The Applicant shall ensure that it satisfies and will at all times during its participation in the Scheme satisfy the eligibility criteria for participation in the Scheme as set out in the Rulebook. If at any time, the Applicant has reason to believe that it no longer satisfies such criteria, or may be unable to satisfy such criteria, it shall notify the EPC immediately of the circumstances.</p>
SPL Scheme	<p>2.4. The Applicant is in a position to comply with all of the obligations set out in the Rulebook by the “Readiness Date” as stated in the accompanying Schedule.</p>
	<p>3. By submitting this completed form of Adherence Agreement the Applicant agrees to be bound by the provisions of the Rulebook governing applications for participation in the Scheme, whether or not it becomes a Participant.</p>
<p>4. Any communication, including service of process, to be made with the Applicant under or in connection with the Rulebook shall be made in writing and addressed to the Applicant at the address set out above.</p>	
<p>5. The Applicant consents to the publication of its name and basic details of its adherence application on the public website of the EPC.</p>	
<p>6. This Agreement is governed by Belgian law.</p>	
<p>FOR AND ON BEHALF OF THE APPLICANT</p>	
<p>Signed by (1)</p>	<p>By (2) (if necessary)</p>
<p>-----</p>	<p>-----</p>
<p>Name/Position -----</p>	<p>Name/Position -----</p>
<p>Date of signature -----</p>	<p>Date of signature -----</p>
<p>Where this Adherence Agreement was signed by two signatories on different dates, it shall be considered as being dated the later date.</p>	



2 Schedule information to the Adherence Agreement

SPL Scheme	SCHEDULEⁱ INFORMATION TO THE ADHERENCE AGREEMENT FOR ADHERENCE TO THE SEPA PROXY LOOKUP (SPL) SCHEME									
	<p>(A) The Applicant must supply the information requested in the Schedule in support of its application to adhere to the Scheme. A failure to supply this information may result in a rejection of the application or a delay in processing it. The information set out below must be included in the Schedule.</p> <p>(B) Templates to be used for providing the Schedule information (Excel or Word) can be downloaded from the EPC website at www.epc-cep.eu. It is strongly recommended that Applicants provide the Schedule information as an Excel File.</p> <p>(C) The information supplied below shall be recorded on the EPC's Register of Participants for the SEPA Proxy Lookup (SPL) Scheme. The Applicant acknowledges and agrees that any information supplied in this section (C) of the Schedule shall be published in the relevant EPC Register of Participants on the public website of the EPC and may be made generally available for download by the EPC.</p>									
	SPL Scheme	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;">Full Name of Applicant</td> <td></td> </tr> <tr> <td>Official Address for Notices</td> <td></td> </tr> </table>	Full Name of Applicant		Official Address for Notices					
Full Name of Applicant										
Official Address for Notices										
SPL Scheme	(D)									
	SPL Scheme	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;">Details of Contact Point (for communication with the EPC, a generic email must be supplied here, e.g. sepa@psp.com)</td> <td></td> </tr> <tr> <td>Readiness Date</td> <td></td> </tr> <tr> <td>Reachable as of Readiness Date as</td> <td> <input type="checkbox"/> Initiating Registry Provider (IRP) only <input type="checkbox"/> Responding Registry Provider (RRP) only <input type="checkbox"/> IRP and RRP </td> </tr> <tr> <td>E-mail and phone number of contact person handling Applicant's Adherence Application in-house</td> <td></td> </tr> </table>	Details of Contact Point (for communication with the EPC, a generic email must be supplied here, e.g. sepa@psp.com)		Readiness Date		Reachable as of Readiness Date as	<input type="checkbox"/> Initiating Registry Provider (IRP) only <input type="checkbox"/> Responding Registry Provider (RRP) only <input type="checkbox"/> IRP and RRP	E-mail and phone number of contact person handling Applicant's Adherence Application in-house	
	Details of Contact Point (for communication with the EPC, a generic email must be supplied here, e.g. sepa@psp.com)									
	Readiness Date									
Reachable as of Readiness Date as	<input type="checkbox"/> Initiating Registry Provider (IRP) only <input type="checkbox"/> Responding Registry Provider (RRP) only <input type="checkbox"/> IRP and RRP									
E-mail and phone number of contact person handling Applicant's Adherence Application in-house										
(E)										



SPL Scheme	VAT Number	
	Generic E-mail address for invoicing	
	E-mail and phone number of contact person/ department for invoicing	
	Invoicing Address (if different from the Official Address for Notices)	
	Legal Entity Identifier 'LEI' ⁱⁱ (if available)	
	Preferred payment instrument for Scheme Participation fee invoicing	<input type="checkbox"/> SEPA Direct Debit Core ⁱⁱⁱ <input type="checkbox"/> SEPA Credit Transfer
SPL Scheme	(F) All EPC communication may be sent to the generic e-mail address specified in the Schedule.	

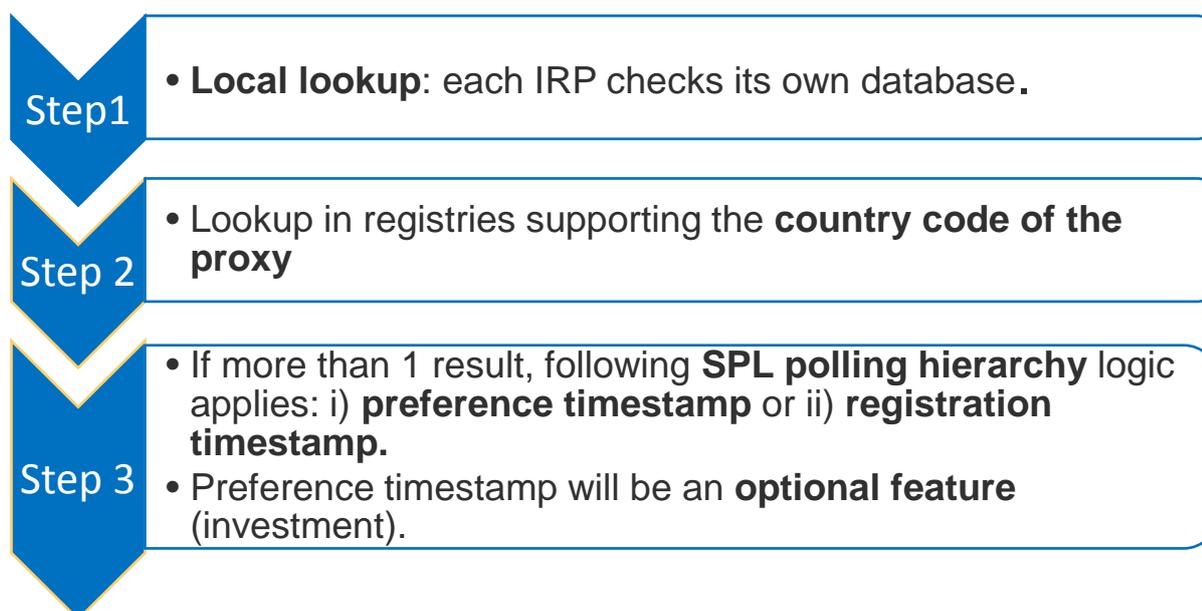
ⁱ Where more than one Applicant is covered by this Adherence Agreement, please ensure that information requested by this Schedule is supplied in respect of each Applicant. Organisations adhering to one or more SEPA payment Schemes are requested to always include the same Schedule information including the same reference BIC with each application. If a participant in one or more SEPA payment Schemes submits an application pack for adherence to the SPL Scheme featuring different Schedule information, the related information in the SEPA payment Schemes Participant Registers will be overwritten.

ⁱⁱ The LEI is based on the international standard ISO17442:2012 "[Financial Services - scheme to identify the legal entities \(LEI\)](#)"

ⁱⁱⁱ The Secretariat will send a numbered SDD Core mandate to be signed and sent back (via email or regular mail) to each successful Applicant wishing to make use of SDD Core to settle its Scheme participation fees.



3 Polling hierarchy logic



Supplementary rules related to step 3:

- There are two types of timestamps:
 - Preference timestamp (optional) is the time at which a preference was explicitly indicated by the customer (payee).
 - Registration timestamp (mandatory) is the time at which the customer registered with the service.
- RRP's response should be provided within a reasonable timeframe. (e.g. within 1 second).
- 'Preference' relates to the fact that the customer opts in to receive payments into a specific account (explicit consent is required). This is only possible if the RRP has developed this additional feature.
- If only one RRP responds that has not build the preference feature then there is no conflict and the payment can be directed to this RRP.
- If there is a conflict then the payment will be directed to the RRP that has been selected as preferred or if there is no "preferred" status with the "registration timestamp" indicating the most recently registered account.
- If more than one Participant (RRP) responds and they have both been selected as preferred, then the preference timestamp will be checked. The payment will be directed to the RRP with the most recently preferred service.

(Note: the efficiency of the logic could for example be revisited after 1 year)

4 Scheme Management Cost Allocation

The EPC may set an annual Scheme participation fee to recover the costs related to the Scheme Management function performed by the EPC and the Scheme Management governance bodies.



5 SPL API Specification

5.1 Scope

This is an implementation specification of a SEPA Proxy Lookup (SPL) service as a central component of an interoperable mobile person-to-person technical architecture.

The emphasis is placed on:

- the definition of a technical architecture to support the principles governing the management of the SPL service;
- the underlying security architecture enabling the establishment of secure communication channels for the compliance with the applicable EU Legal Framework.

This document includes the following items:

- The description of the SPL service and roles;
- The SPL functional model list as a system made up of logical components and interfaces;
- The API for the communication between the Initiating Registry Provider (IRP) and the SPL;
- The API for the communication between the SPL and the Responding Registry Provider(s) (RRP);
- The list of Data Elements required to support the communication through both APIs;
- A standard algorithm to be executed by the SPL for the selection of a unique IBAN;
- A security architecture.

The following is out of the scope of this document:

- The effective execution and initiation of the mobile person-to-person payment;
- Customer protection mechanisms (e.g. including fair contract terms, rules on transparency of charges, clarification of liability, complaints mechanisms and dispute resolution).

Future versions of this specification are expected to introduce additional functionalities, using different proxies and account identifiers supporting other payment instruments and other types of payment.

5.2 Introduction

Three types of entities, i.e. IRP, RRP and an intermediary SPL are needed to provide the service. The IRP and the RRP do not establish any direct communication. Instead both, the IRP and the RRP establish a connexion with the SPL using the entry points of two APIs offered by the SPL. One API is available for the communication between the IRP and the SPL. The second one supports the communications between the SPL and the RRP(s). Both are specified in this document, which is structured as follows:

- Section 5 sets out the functionalities and requirements for the entities participating in the service;
- Section 6 specifies the two APIs offered by the SPL to the enrolled IRP(s) and RRP(s);
- Section 7 identifies the list of Data Elements to be used during the SPL transaction;



- Section 8 specifies the SEPA Proxy Lookup Service Algorithm;
- Section 9 sets out a security architecture for the SPL service; and
- Section 10 discusses and proposes some Data Protection requirements.

Initially the focus of the SPL service is to enable mobile person-to-person (P2P) payments between mobile payment-based schemes within the SEPA geographic area whereby the mobile telephone number is used as a proxy to an IBAN.

5.3 Terminology & List of Acronyms

Term	Definition
IBAN	International Bank Account Number
Initiating Registry Provider (IRP)	Entity that queries the SPL for the IBAN associated to the mobile phone number of the beneficiary of the payment.
Proxy	Data required by the SPL service in order to retrieve a payment account identifier. In this specification, the proxy is initially the mobile phone number of the beneficiary of the payment.
Responding Registry Provider (RRP)	Entity that upon request by the SPL provides the IBAN associated to the mobile phone number of a customer.
SPL	Directory service which will initially forward to the IRP an IBAN associated to a mobile phone number provided by an RRP.
SPL Service Algorithm (PLA)	Algorithm to be implemented by the SPL service to select just the IBAN to be transmitted to the IRP when there is more than one responding RRP (in case two or more IBANs received by the SPL).
SPL Service Operator(s)	Entity designated to operate the SPL service by offering API's for the connection of the IRP(s) and RRP(s) participating in the SPL Scheme.
SPL Transaction Data	Set of message(s) exchanged between the IRP, the SPL and the RRP(s), starting with the IRP Request addressed to the SPL and concluding with the SPL response to the IRP request.
Time Stamp	Data encoding the enrolment and preference date of a payment service user (PSU) by an RRP. There are two types of time stamps: <ul style="list-style-type: none">• Registration time stamp (mandatory) is the time at which the customer registered with the service.• Preference time stamp (optional) is the time at which a preference was explicitly indicated by the customer (beneficiary);

5.4 Applicable Documentation

D1	SPL Scheme Rulebook
D2	Berlin Group Mobile P2P Interoperability Framework Operational Rules v1.0 https://www.berlin-group.org/mobile-p2p-interoperability (Creative Commons Attribution-No Derivatives 4.0 International Public License applies)



D3	ISO TS 12812-4 Mobile Payments-to-Persons
D4	European Banking Authority: Regulatory Technical Standard specifying the requirements on Strong Customer Authentication and common and secure communication under PSD2
D5	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR)

5.5 Requirements for the Entities Participating in the SPL Service

5.5.1 Components and Interfaces for Interoperability

The SPL Scheme is made up of at least three categories of roles:

- The IRP, for instance a financial institution, which offers the service to customers acting as originator.
- The RRP, which enrolls customers acting as beneficiaries (initial scope) of the payments. The RRP maintains a customer database. In this database an individual record associates the mobile phone number of the customer with an International Bank Account Number (IBAN).
- SPL service provider(s), which intermediate(s) between IRPs and RRPs, offering API's for the information exchange.

Jointly, they assure two data flows:

- One between the IRP and the SPL using API-1 as shown in Figure 1;
- One between the SPL and the RRP using API-2 as shown in Figure 1.

Note: The IRP and RRP roles may be played by the same entity.

The IRP, acting as an agent of the originator, interacts with the SPL service using as data input the mobile phone number of a beneficiary of a mobile P2P payment. Upon the verification of the IPR request, the SPL forwards the request message to the RRP having enrolled for the SPL service. Those RRP(s) having identified the mobile phone number as the one of an enrolled customer will provide as a response to the SPL query the IBAN associated to that particular mobile phone number. It is assumed that the same customer may enrol the same mobile phone number with different RRP(s) with the same or different IBAN's.

Finally, the SPL concludes its operation by providing the IRP with an IBAN sent by a responding RRP. If more than one RRP is responding using different IBANs, then the SPL shall execute the PLA algorithm according to section 5.8 provisions, in order to select a single IBAN that will be sent to the IRP.

This specification assumes that the originator has a contractual agreement with an entity, named the IRP, and the beneficiary has a contractual agreement with a second entity, the RRP. Both the IRP and the RRP have a contractual agreement with the SPL service, which is operated by (a) third entity(ies).

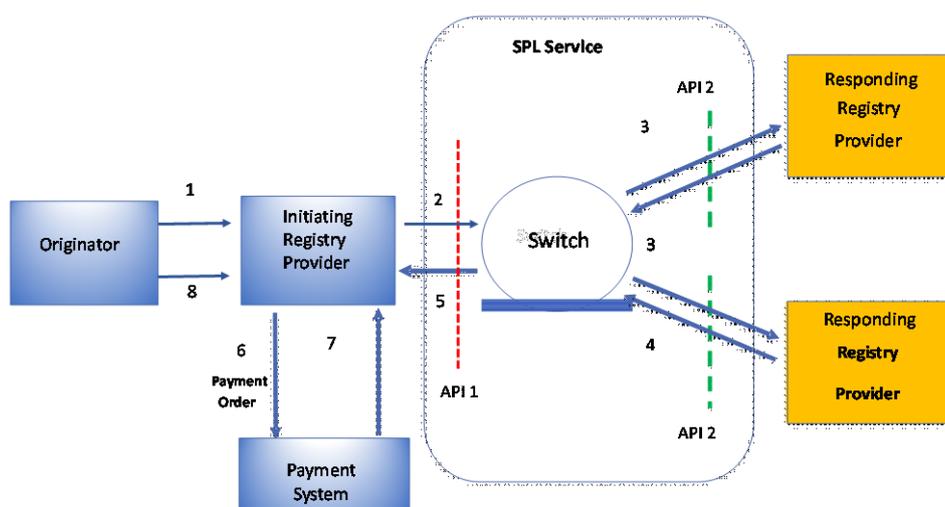


Figure 1 : High Level Functional Model for the SEPA Proxy Lookup

5.5.2 List of functionalities to be supported by the SPL Service Provider(s)

5.5.2.1 Management responsibilities of the SPL Service Provider(s)

- Provide an interface to contract with both IRP(s) and RRP(s) for access to the SPL service providing a sufficient level of information;
- Assign a unique identifier for the enrolled IRP(s) and RRP(s) to be used in the corresponding Data Element(s) of section 5.7;
- Authenticate both the IRP and the RRP identities during a transaction;
- Validate any IRP request;
- Forward exclusively to the RRP(s) validated IRP requests using the identifier of the IRP;
- Validate RRP(s) responses;
- Provide the IRP with only one IBAN associated with a validated RRP response;
- Establish a secure communication channel with either the IRP or the RRP when required;
- Maintain a transaction log without storing personal data (originator and/or beneficiary of the payment) for at least a three-month period;
- Facilitate any audit upon request by the SPL Scheme Manager (EPC);
- Certify operational practices as well as sensitive components required for the SPL operation: APIs, cryptographic devices, storage, processing and communication hardware and software components;
- Maintain its own technical infrastructure according to future evolutions of this specification.

Other components are out of the scope of the present specification.



5.5.2.2 Infrastructure components under the responsibility of the SPL Service Provider(s)

The SPL Service Provider(s) shall be responsible to develop and make available an implementation of this technical specification. Therefore, the SPL Service Provider(s) shall implement and maintain the following computing, storage and processing components:

- An API supporting a Request/Response exchange with the SPL initiated by an IRP according to the requirements set out in section 5.6 using the list of Data Elements in section 7 (Request by the IRP, Response by the SPL);
- A polling process according to the requirements set out in section 5.6 for API-2;
- An implementation of the SPL Service Algorithm (PLA) as specified in section 5.8;
- Authentication servers for the authentication of the IRP(s) and the RRP(s) according to the requirements set out in section 5.9;
- Cryptographic devices and associated components (see Key Management Systems, Hardware Security Module (HSM), Random Number Generators) enabling the establishment of a secure communication interface with both the IRP and RRP according to the requirements set out in section 5.9;
- Databases for the SPL transaction data log, protected according to the requirements set out in section 5.10;
- A fall-back infrastructure to ensure the availability of the Service.

Notes:

Interface components required to establish a communication with a third party other than IRPs and RRP are out of the scope of the specification;

The SPL Scheme Manager (EPC) establishes a contractual “Service Level Agreement” with the SPL Service Provider(s).

5.5.2.3 List of optional functionalities

SPL optional functionalities refer to:

- Internal arrangements of the SPL Service Provider(s) in order to improve the quality of the service.
- Support of Data Elements for Value Added Services – section 5.7 includes optional Data Elements that may be used for additional services not required for the implementation of this specification;
- Provide identification services to help the originator payment service provider (PSP) to comply with their legal duties in terms of customer due diligence, prior to the execution of the payment;
- Future support to other proxies (e.g. email) or payment account identifiers (e.g. PAN) to initiate a payment using other instruments (card, e-money);
- Tokenization service, to avoid the proliferation of payment account identifiers;
- Quality-of-Service (QOS) offers.

5.5.3 Responsibilities of the IRP

The IRP shall:

- Enrol with the SPL Scheme Manager (EPC) and contract with an SPL Service Provider for the service;



- Provide a mobile phone mechanism for access of the originator to the SPL service. As a minimum this mechanism shall:
 - Implement a user interface enabling the originator to enter the mobile phone number of the beneficiary of the payment;
 - Not disclose any personal information of the originator to the SPL;
 - Not reveal to the originator payment account information of the beneficiary of the payment;
- Assign a unique identifier to each SPL request. This unique identifier shall be recorded along with transaction data, other than the IBAN;
- Ensure that the mobile number that is sent to the SPL respects the MSISDN format;
- Exclusively use the API provided by the SPL to initiate a request to the SPL;
- Establish a secure channel with the SPL for the protection of sensitive data;
- Validate the SPL response prior to use of the IBAN to initiate the payment order;
- Not store the IBAN of the beneficiary of the payment;
- Provide SPL transaction data required to resolve a dispute;

5.5.4 Responsibilities of the RRP

The RRP shall:

- Enrol with the SPL Scheme Manager (EPC) and contract with an SPL Service Provider for the service;
- Assign a unique identity to each customer (beneficiary of the payment);
- Implement an API (API-2 in Figure 1) enabling the access by the SPL to RRP information. This API will support:
 - the mutual authentication of both the SPL and the RRP;
 - a polling method to be exclusively evoked by an authenticated SPL.
- Maintain a system, with an individual entry for each customer recording:
 - The mobile phone number (s) of the customer;
 - The customer identity;
 - The IBAN provided by the customer during the enrolment;
 - Time-stamps required for the PLA execution as per section 5.8 requirements;
 - Metadata;
 - A log with the SPL transaction data.
- Maintain a risk management program describing the access control mechanisms for the customer database as well as the process and security mechanisms to ensure the integrity of the database;
- Provide a mobile phone mechanism for the explicit authorisation by the end-customer of the disclosure of information to the SPL other than the IBAN and the associated time-stamps;
- Establish a secure channel with the SPL for the protection of in transit sensitive data;
- Validate the SPL request prior to providing the IBAN associated to the received mobile phone number;
- Upon request provide SPL transaction data evidence for the resolution of a dispute.



5.6 API Specifications

5.6.1 Introduction

When defining this specification, the goal was to reuse existing specifications and standards as much as possible in order to create a system based on open standards, for maximum interoperability and to support a quick time to market.

The “Mobile P2P Interoperability Framework” specified by the Berlin Group has been identified as a perfect fit for the requirements defined by the SPL Scheme.

The specification provided by the Berlin Group covers a much broader scope because it also specifies the application and the payment layer of a mobile P2P transaction. However, it also specifies the proxy lookup mechanism, and the corresponding API, which are relevant for the SPL service.

The Berlin Group specification supports both a centralised and a decentralised approach for the communication between different mobile P2P schemes because the API is agnostic of the role of the counterpart. It can be either another mobile P2P scheme or a central hub, which forwards the request between the different P2P schemes.

In order to allow maximum interoperability with different schemes the existing “Mobile P2P Interoperability Framework” specified by the Berlin Group is used to implement the technical interfaces of the SPL service.

5.6.2 Berlin Group “Mobile P2P Interoperability Framework”

The SPL service communicates with the IRP via API 1 and the RRP via API 2. Both APIs are technically identical and are based on the specification of a “Repository Lookup” defined by the Berlin Group “Mobile P2P Interoperability Framework”.

The following chapters provide the specification of the APIs, which shall be used by the SPL:

- Mobile P2P Interoperability Framework Operational Rules Version 1.01: 5.1.1 Repository Lookup;
- Mobile P2P Interoperability Framework Implementation Guidelines 1.01: 3.3.1 Repository Lookup;
- Mobile P2P Interoperability Framework Implementation Guidelines 1.01: 3.1.1 Security levels.

The Berlin Group Mobile P2P Interoperability Framework supports both XML based SOAP Web services and JSON-based REST services as alternative technical implementations. For the SPL service it is required to implement the API as a JSON-based REST service.

The Berlin Group Mobile P2P Interoperability Framework states that data exchange via internet shall be performed using virtual private networks (VPN) by using client certificates on transport level but doesn't define further details and suggests that this has to be defined bilaterally between Mobile P2P schemes. However, for the SPL service, the secure channels between the involved parties are clearly defined within this specification. Further information on the secure communication between all the involved parties (IRP, RRP and SPL) is provided in section 5.9 of this specification.

Note:

The Reachability Check and the Payment Notification defined in the Berlin Group Mobile P2P Interoperability Framework are currently out of scope of the SPL specification but may be included in a future version of this specification.



5.6.3 API for the communication between the IRP and the SPL

If the IRP makes a request to the SPL in order to lookup a proxy, it shall use the repository lookup API specified by the Berlin Group specification. Therefore, it makes a call to the SPL as if it would make a lookup directly to the beneficiary's scheme in order to identify the IBAN related to a given mobile phone number. After the SPL receives the request via the JSON-based REST service API, containing the information described in section 5.7.2, it executes the SPL algorithm which is specified in section 5.8 of this specification. After the execution the result shall be returned via the JSON-based REST service API as it would have been returned directly by the beneficiary's scheme. The IRP neither can see the different contacted RRs following the SPL algorithm execution nor gets any information about the details of the execution of the routing algorithm and the polling hierarchy. The SPL shall only return the IBAN, if one could be identified, and the supporting information as described in section 5.7.3.

5.6.4 API for the communication between the SPL and the RRP

During the execution of the polling hierarchy the SPL contacts one or several RRs as described in section 5.8.2. For the lookup requests the SPL shall use the repository lookup API specified by the Berlin Group specification. After the SPL sends a request to each of the identified RRs via the JSON-based REST service API, containing the information described in section 5.7.2, it waits for the response during a predefined timeout. For this call the SPL acts like the originator's scheme in a bilateral interoperability. The RRP not only acts like the beneficiary's scheme but in this case is the beneficiary's scheme of the mobile P2P payment. Each RRP then initiates an internal lookup in its own database in order to find the IBAN corresponding to the mobile phone number provided by the SPL. If an IBAN is found by the RRP the result shall be returned to the SPL via the JSON-based REST service API. The RRP only shall return the IBAN, if one could be identified, and the supporting information as described in section 5.7.3.

5.7 Data Elements

5.7.1 Introduction

The Data Elements referred in this section shall be used in the messages exchanged between the:

- IRP and the SPL; and
- SPL and the RRP.

These Data Elements are listed in the two tables below. Please find below the figure which is used as a reference for the interfaces IF2-IF3-IF4-IF5 in the Table listing the Data Elements required for the Interoperability of the Proxy Lookup service.



Figure 2 Interfaces (IF2-IF3-IF4-IF5) for the Data Elements to be exchanged in the APIs

The first Table summarises the Data Elements needed to execute a Lookup Request. These Data Elements are conveyed in the interface IF2 (between the IRP and the SPL service) and in the interface IF3 (between the SPL service and the RRP”);

The second Table summarises the Data Elements needed to execute a Lookup Response. These Data Elements are conveyed in the interface IF4 (between the RRP and the SPL service) and in the interface IF5 (between the SPL service and the IRP).

Both Tables contain six columns organized as follows:

C1	Data Elements, respecting the name and identifier assigned by the Berlin Group.
C2	REST message attribute identifier per data element.
C3	Data type description per data element.
C4	“Purpose” is a rewording of the Berlin Group definition of the Data Element.
C5	Is divided into two sub-columns identifying the interfaces where the Data Element is exchanged. Note that the content of the same Data Element may change according to each interface.
C6	Indicates if the Data Element is Mandatory/Optional/Conditional in the Berlin Group Specifications.

5.7.2 List of Data Elements for the SPL Request

C1 Element	Data	C2 Tag	C3 Type	C4 Purpose	C5 Interface		C6 Berlin Group (M/O/C)
					IRP -> SPL (IF2)	SPL-> RRP (IF3)	
Mobile Number Beneficiary (AT 01)		AlsBfy	AliasType	Encodes the alias (phone number) of the beneficiary	X	X	M
Mobile Number Originator (AT - 13)		AlsOrig	AliasType	Encodes the phone number of the originator	X	X	O



			The Receiver Scheme can mandate to provide personal IBAN data only to Originators which are on a customer's white list			
Originator Scheme ID (AT – 02)	OrigSch	SchemeType	Identifies the Originator Scheme by a unique identifier	X	X	M
Receiver Scheme ID (AT – 03)	RecSch	SchemeType	Identifies the Receiver Scheme by a unique identifier	X Conveys the scheme ID of the SPL	X Conveys the scheme ID of the RRP contacted by the SPL	M
Transaction Amount (AT – 04)	TxAmt	AmountType	The transaction amount in Euros	X	X	O
Lookup Request Reference Data (AT – 05)	TxID	Max35Text	Unique identifier for the Request	X Generated by the IRP only for the SPL or Generated by the IRP for both the SPL and the RRP	X Generated by the SPL only for the RRP or to reuse the unique identifier generated by the IRP	M
Time stamp Request (AT – 06)	CreDtTm	ISODatetime	Non repudiable evidence of the time a Lookup request was initiated	X Generated by the IRP only for the SPL or Generated by the IRP for both the SPL and the RRP	X Generated by the SPL only for the RRP or to reuse the time stamp generated by the IRP	M



5.7.3 List of Data Elements for the SPL Response

C1 Element	Data	C2 Tag	C3 Type	C4 Purpose	C5 Interface		C6 Berlin Group (M/O/C)
					SPL -> IRP (IF5)	RRP -> SPL (IF4)	
Lookup Request Reference Data (AT – 05)		TxID	Max35Text	Unique identifier for the Request	X The same received by the SPL during the Request	X The same received by the RRP during the Request	M
Response Result Yes/No (AT – 08)		Resp	Response Type	Indicates whether the alias could be matched to account data or not.	X	X	M
Reason Code (AT-09)		RsltDtIs	CodeSet	This Data Element is an optional addition in case of a negative response. It is not used in case of a positive response.	X	X	C Conditional: Mandatory only if AT-08 = "No match"
Originator Scheme ID (AT – 02)		OrigSch	Scheme Type	Identifies the Originator Scheme by a unique identifier	X	Only if the Originator ID has been transmitted to the RRP during the Request, otherwise the Data Element contains the SPL scheme ID	M
Receiver Scheme ID (AT – 03)		RecSch	Scheme Type	Identifies the Receiver Scheme by a unique identifier	X Conveys the SPL scheme ID or the scheme ID of the <u>single RRP selected by the polling hierarchy is to be included</u>	X Conveys the scheme ID(s) of the RRP(s) contacted by the SPL that is responding to the request	M
Creditor Account Data (IBAN, "IBAN") (AT – 10)	Type	CdtrAcct	Creditor Account Type	The IBAN of the beneficiary's payment account data to be used for the payment	X This IBAN is the one selected by the SPL based on the routing algorithm	X NOTE: Several IBANs can be retrieved from responding RRP	C Conditional: Mandatory only if AT-08 = "match"



Creditor Account Type Indicator (AT – 11)	SchAcct	TrueFalse Indicator	This indicator is included in the case where the IBAN transmitted (Scheme IBAN) is not equal to the IBAN of the final beneficiary	X	X	C Conditional: Mandatory only if credit account does not equal the beneficiary account.
Name Beneficiary (AT – 12)	BfyNm	Max140Text	According to the Berlin Group “The legal name of the Beneficiary as registered in the Receiver Mobile P2P Scheme following the KYC levels”. This Data Element is only included in the case of a positive response, as an optional entry, due to possible data protection issues. This entry might be used for embargo and AML checks.	X	X	O (BG) Note: SPL SPG = O/C Conditional means: If AT-8 = “no match”, AT-12 cannot be sent If AT-8 = “match”, AT-12 is optional
Notification Message Link (AT – 14)	PmtNtfc Path	String	This Data Element is included if the Receiver Mobile P2P Scheme requires the use of Transaction Notification Messages on Application Level, cp. Section 5.3. This Data Element consists of a path. The Originator P2P Scheme is required to post the corresponding notification on the URL consisting of the Receiver Mobile P2P Scheme website added by this path.	X In phase 1, the SPL is not expected to support Notification Services. In that case, AT-14 is sent in a way transparent to the IRP.	x	O



Preference Indicator (AT – 15)	PrfInd	ISODate Time	The Beneficiary might be registered in more than one Mobile P2P Scheme with the same MSISDN. Some schemes allow their members to flag the scheme as preferred for receiving funds under a MSISDN. Therefore, a preference indicator may optionally be provided in the Lookup response message. The indicator Data Element contains the time stamp when the Beneficiary declared the Receiver Scheme as preferred.	X	X	O
Registration Time stamp (AT – 16)	RegDtTm	ISODate Time	This Data Element contains information about date and time when the Beneficiary has registered its account number with the Receiver Scheme. This time stamp may be used in the selection of the Receiver Scheme in case of multiple responses to a Proxy Lookup Request.	X	X	M

5.7.4 Possible Return and Response Codes

An overview of the possible return codes as defined in the Mobile P2P Interoperability Framework Implementation Guidelines are listed below:

Status Code	Message Code	Description
200		Transaction was correct, no Payment Advice required,



		IBAN might be contained or not
201 (Created)		Transaction was correct, IBAN is contained and Payment Notification Advice is required, a hyperlink for the corresponding resource is contained.
400 (Bad Request)		Validation error occurred.
401 (Unauthorized)	CERTIFICATE_NOT_VALID	
403 (Forbidden)	MP2P_NOT_ADMITTED	Initiating Party is not admitted to the system

The Mobile P2P Interoperability Framework Implementation Guidelines list the following allowed reason codes (AT-09) to decline a request:

Code	Description
NMMD	No match of MSISDN in database
TALE	Transaction amount limit exceeded
NOTX	Number of transaction limit exceeded
CTLE	Cumulative transaction amount limit exceeded
SYUA	System unavailable
FERR	Format error

5.8 SPL Service Logic

5.8.1 Overview

This section describes the SPL service logic which covers the requests to the different participants (RRPs) in the service and the evaluation of the answers to these requests and the decision, under certain predefined rules, which IBAN should be returned to the IRP.

The logic of the SPL service can be divided into two main building blocks:

- **The Polling Hierarchy:** Defines which RRP's are requested by the SPL and in which order;
- **The Routing Algorithm:** Defines which IBAN is returned to the IRP based on the number of responses and the time stamps.

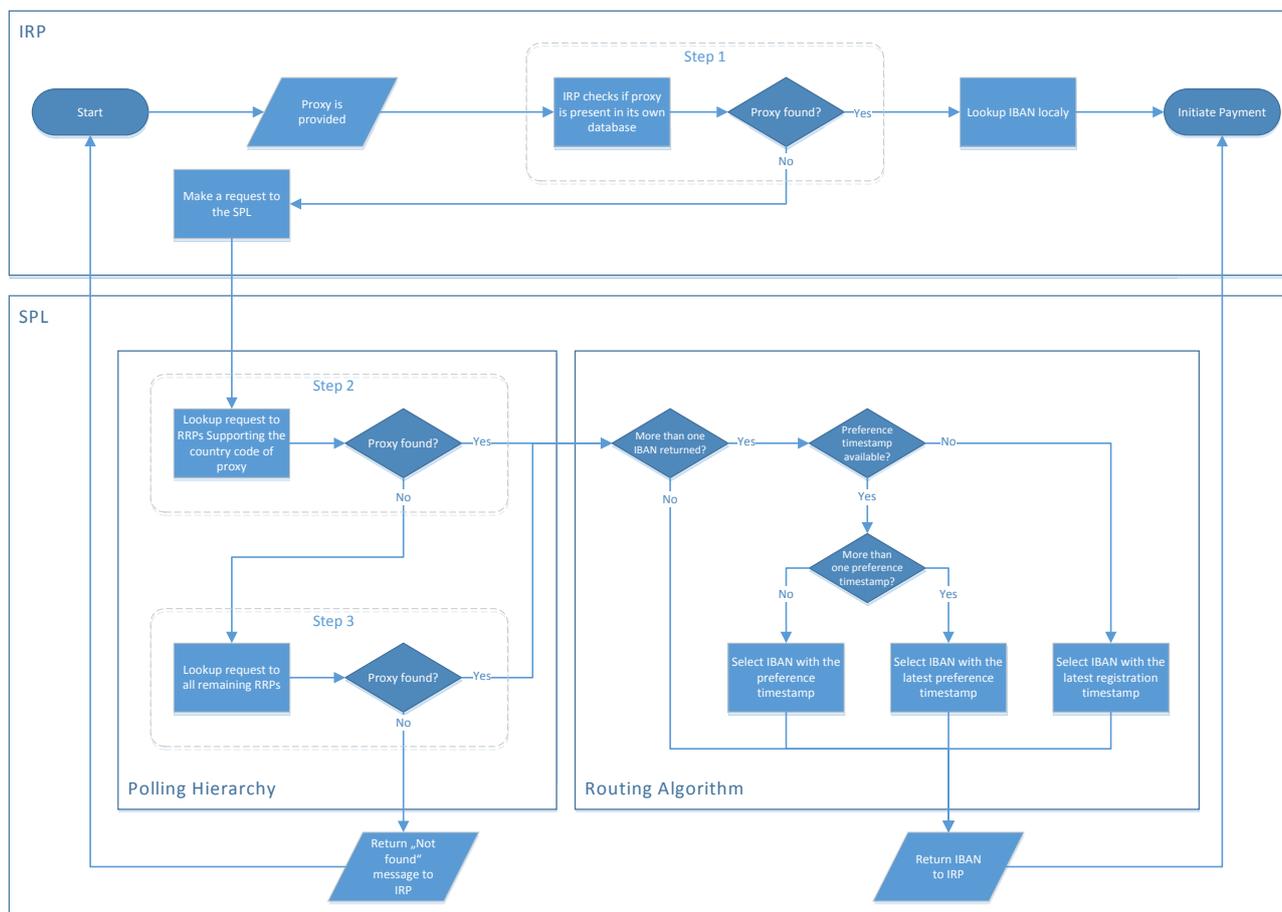


Figure 3 Flow of an SPL lookup request

The following chapters describe the two separate building blocks more in detail.

5.8.2 Polling Hierarchy

Upon reception and validation of an IRP request by the SPL, the SPL shall apply the polling hierarchy in order to contact the participating RRP using the mobile phone number as a proxy. In order to request the information from the appropriate RRP the following polling hierarchy shall be executed, as defined in the Rulebook (Annex 3)

- **Step 1:** Local lookup: each IRP checks its own database before sending a request to the SPL (this is not part of the SPL logic itself but is a precondition for the IRP to make a request to the SPL);
- **Step 2:** Lookup request is sent to RRP that support the country code of the proxy
- **Step 3:** Lookup request to all remaining RRP.

If a result for the given proxy is found after step 2 or step 3 then the routing algorithm is executed, and no further polling is executed. In case there is no result returned by any RRP after the execution of step 3, a “Not Found” message shall be returned to the IRP by the SPL. This means that no participating RRP has enrolled the mobile phone number as a proxy for the SPL Service.

The SPL shall also proceed with the next logic process if no response is provided after a predefined timeout. In step 2 and step 3 the SPL shall wait for a response from all the RRP to whom a request was sent to until the timeout has been reached. It shall not proceed to the next logic process even if there is a response from one or more RRP before the expiration of the timeout.



5.8.3 Routing Algorithm

If the SPL receives one or more valid results during the execution of the polling hierarchy it shall execute the Routing Algorithm to decide which IBAN is returned to the IRP. The decision will be based on the number of returned IBANs and on the registration and preference time stamps:

- If there is only one RRP responding with an IBAN: After validation of the RRP message, the SPL shall forward the IBAN to the IRP in the response message (even if the RRP who responds has not implemented the preference feature there is no conflict).
- If there are more than one validated RRP responses, the SPL shall proceed as follows:
 - The SPL shall return to the IRP the IBAN that has been selected as preferred or if there is no “preferred” status it shall return the one with the “registration time stamp” indicating the most recently registered account.
 - If more than one participant (RRP) responds and they have both been selected as preferred, then the time of the preference time stamp will be checked. The SPL shall return to the IRP the IBAN with the most recently preference time stamp.

Note:

“Preference” relates to the fact that the customer opts to receive payments into a specific account (explicit consent is required). This is only possible if the RRP has developed this additional feature. This means that if the response of an RRP does not contain a preference time stamp then the RRP either has not developed this additional feature or the customer never has explicitly expressed the wish to use this account as a preferred account to receive payments.

5.9 SPL Security Architecture

5.9.1 Problem Statement

The compromise of the information provided by the SPL increases the risk of fraud resulting in financial losses for the end-users of the SPL Service.

The SPL is the intermediary entity that enables the service by conveying RRP-held account information about the beneficiary of the payment to the IRP. No direct communication is established between RRP(s) and IRP (s) participants in the scheme. The SPL is a centralised system and as such, constitutes a central point for a cyberattack. The technical choice is therefore not to store permanently sensitive payment information (e.g. IBAN) in the SPL computing facilities.

The security model assumes that:

- The RRP databases storing payment beneficiary information are safe.
- The originator knows the identity of the beneficiary of the payment and his/her mobile phone number as enrolled by the RRP.

The participants in the SPL Scheme, IRP(s), RRP(s) and the SPL Service Provider(s) are expected to implement a security architecture ensuring the integrity and/or the confidentiality of the exchanged information, in order to comply with the security objectives, set out in Section 5.9.2.



5.9.2 Security Objectives

O1	The databases required for the SPL service protect the integrity and the confidentiality of the enrolled customer personal data at rest.
O2	Only the registered participants in the SPL Scheme may have access to the data to be exchanged during a SPL transaction
O3	Only a legitimate customer of an IRP may initiate a payment
O4	Only a legitimate customer of an RRP may be the beneficiary of a payment
O5	Only the IBAN provided by the SPL service can be used as payment account identifier in the payment order generated by the payer PSP
O6	The SPL service cannot be misused for the purpose of retrieving information not intended to initiate a payment

5.9.3 Security Requirements

R1	The integrity of the proxy (mobile phone number) shall be preserved in transit: since the time it is entered in the mobile until the time it is polled by the SPL and received by the participant RRP
R2	The customer information provided during the enrolment process and stored in a record in an RRP database shall be accurate. This record information associates the identity of the customer, the mobile phone number, an IBAN, the enrolment date and other customer data, such as a preference level.
R3	The RRP security policy shall ensure the integrity of the customer database records
R4	Mutual authentication of the two communicating parties in any exchange during the SPL transaction shall be possible
R5	The RRP shall only facilitate customer information (e.g., IBAN) to a legitimate SPL
R6	The SPL shall not store the IBANs received from the RRP during the transaction
R7	The integrity and confidentiality of the IBAN information provided by the RRP to the SPL and then forwarded to the IRP shall be preserved all along the transaction
R8	Any pair (mobile phone number, IBAN) received by the SPL shall be the same than the one(s) enrolled by the RRP(s)
R9	The mobile payment application of the payer shall: <ul style="list-style-type: none">• verify the integrity and the origin of the data received from a SPL response• prevent the access of the payer to the IBAN of the beneficiary• not store the IBAN received from the SPL• provide a log mechanism• ensure that the IBAN used to generate the payment is the last one received in a validated response from an SPL



- | |
|---|
| <ul style="list-style-type: none">• provide a mechanism for the payer to confirm the identity of the beneficiary of the payment prior to the generation of the payment order• provide a mechanism to confirm to the payer that the payment has been executed |
|---|

5.9.4 Security architecture implementation aspects

In order to comply with the previously defined security requirements, the communication between the parties involved in the SPL service (IRP, RRP and SPL) has to be achieved via secure channels, which assures the integrity and the confidentiality of the transmitted data.

This can be achieved by using HTTPS and TLS transport layer encryption as defined in chapter 3.1.1 'Security levels' of the Mobile P2P Interoperability Framework Implementation Guidelines published by the Berlin Group. This provides a sufficient level of security and allows a lightweight implementation on the SPL site as well as on the IRP/RRP site.

5.9.4.1 Communication via HTTPS and TLS

The communication between the IRP and the SPL service and the SPL service and the RRP takes place via JSON REST services as defined in section 5.6.3 and section 5.6.4 of this specification. End-to-end encryption is not supported by JSON REST services. However, for the proxy lookup, point-to-point encryption should be sufficient.

The following minimum requirements have to be fulfilled:

- Encryption shall be performed on the transport layer via https using TLS 1.2 or higher versions of TLS.
- Lower SSL-versions shall not be allowed.
- Server and client qualified certificates shall be used to ensure secure mutual authentication.

Apart from encryption, the inherent security levels of both Web service methods are equal if best-practises of software implementation like parameter whitelisting are followed.

In case of JSON encoding, proxy look-up requests shall be sent via the http POST command. This avoids any URI length restrictions, possible security issues and data protection issues, which could arise using the http GET command. In the latter case the whole request would be sent as a URL and would be logged on the application level.

As an additional security measure, the SPL service shall maintain an IP address whitelist, which is updated during the on-boarding process of each IRP/RRP. The SPL service shall only accept connections from IP addresses of registered IRPs. The RRP in turn shall also restrict the access to the look-up service only to requests originating from the public IP address of the SPL service.

5.10 Data Protection Requirements ('Data Protection by Design and by Default')

The SPL service requires the exchange of customers' personal data between the participants in the SPL Scheme. It is of the utmost importance that personal data is only processed by authorised parties for the purpose of the payment, in accordance with the mandatory provisions of applicable rules and regulations related to data protection and privacy, notably the GDPR.

In order to avoid erroneous payments, which could be detrimental to the reputation of the SPL Scheme, the SPL service and relevant stakeholders, certain traceability



requirements are to be fulfilled, in full compliance with the GDPR requirements of data protection by design and by default (Article 25 GDPR).
