SCP2P 034-17
Version 1.0
Date issued: 21 December 2017

[X] Public – [ ] Internal Use – [ ] Confidential – [ ] Strictest Confidence
Distribution: Steering Committee of the Mobile Proxy Forum

Mobile Proxy Forum

Request for Proposal to Provide a Standardised Proxy Look-up (SPL) service

Table of Contents

1 Introduction

For the last couple of years, we have seen instant payment solutions emerging around Europe most recently with the launch of SEPA Instant Credit Transfer. One of the big drivers for these payments are mobile person-to-person (P2P) payments however most of the existing solutions are domestic solutions that do not allow cross-border payments.

The Mobile Proxy Forum ("MPF") seeks to create interoperability between these existing services by creating a Standardised Proxy Look-Up service ("SPL") that enables a domestic solution in one country to inquiry about a proxy and related payment details in another country. The service must be operational by October 2018.

This document outlines the procedure that the MPF will apply. It includes a description of the Request for Proposal ("RFP") scope, conditions, award criteria and details of how the candidate should respond to it in order to be eligible.

The RFP includes, but is not restricted to, delivering the SPL service, the software and the services related to it. It also includes setup, operations and maintenance.

1.1 Introduction to the Mobile Proxy Forum

The MPF is a cross-industry working group set up under the auspices of the Euro Retail Payments Board (ERPB), with the following key objectives:

- The setup of an interoperability framework and Standardised Proxy Lookup (SPL) service which allows person-to-person (P2P) payment data to be securely exchanged on a pan-European level, in accordance with the recommendations and mandate of the ERPB.
- Initially the focus will be on using mobile telephone numbers as a proxy for IBAN, but the MPF will have regard to future support for additional proxy types and account identifiers.
- The main goals are to have solutions that are interoperable and user friendly, as well as to foster choice and competition.

To date the work plan of the MPF has included;

- Creation of the Steering Committee (done).
- Creation of a Technical Working Group (done).
- Creation of a Legal Working Group (done).
- Creation of a Market Implementation Working Group (done).
- Set-up of a pan-European SPL service, which includes e.g.:
  - development of rules (done).
  - definition of a polling hierarchy logic (done).
  - issuing a Request for Information in order to do a commercial review of appointing one or more suppliers of the SPL service (done).
  - preparation of the RFP for the selection of technology providers (done).
  - creation of a new legal entity[1].

1.2 Definitions

In this document words in the singular will also include the plural and words in the plural will also include the singular. Words importing the masculine shall include the feminine and the neuter and words importing persons shall include bodies incorporated and unincorporated.

The designations "we" and "our" are all used for Mobile Proxy Forum as the party initiating this RFP.

[1] Subject to the outcome of the RFP and decision of the MPF Steering Committee.

The party answering to the RFP (making the bid) is referred to as 'candidate'.

1.3 Abbreviations

Abbreviation	Long Form
MPF	Mobile Proxy Forum
SPL	Standardised Proxy Look-up Service
P2P	Person-to-Person payments
ERPB	Euro Retail Payments Board
IRP	Initiating Registry Provider
RRP	Responding Registry Provider
MIWG	Market Implementation Working Group
TWG	Technical Working Group

2 Practical information

This chapter contains all of the formalities and practicalities surrounding the RFP process.

2.1 Timeline

This section outlines the deadline for each stage of the RFP process:

Stage	Activity Deadline	Deadline Date
1	Publication of the RFP and invitations to RFP dispatched to RFI responders and selected candidates.	December 21st 2017
2	Final date for candidates to submit written questions concerning the RFP documents.	January 17th 2018
3	Final date for candidates to request a questions and answers (Q&A) session with MIWG.	January 17th 2018
4	Q&A sessions (60 minutes) between the candidates and the Market Implementation WG of the MPF. Sessions can be by video, online or teleconference meeting.	January 22nd – 26th 2018
5	Final date for receipt of RFP responses (See section 3.9 Guide for submission of… ” for details on how to submit your RFP response documents.)	February 9nd 2018 6.pm CET
6	The MIWG will analyse the RFP responses. In case there is a need for clarification as to elements of the response to the RFP the MIWG will contact the RFP respondent via email. The respondent will have 5 business days to reply.	March 1st 2018 is final date that an RFP candidate can receive questions from the MIWG.
7	MPF informs candidates of the outcome of the RFP processand, subject to that, the process going forward.	March 23rd 2018

2.2 Formalities

All candidates must organise their response to the RFP in accordance with the outline detailed in section 3 “Preparation and outline of RFP” of this document. This is to ensure comparability and that all relevant issues are dealt with. It is also essential that all items, requirements and expressed preferences are dealt with and replied to.

The candidate may supplement the outline with matters considered relevant by them. MPF reserves the right to disregard RFP responses in which the candidate deviates from the outline to a significant extent.

If the candidate finds that there are unclear items, the candidate must specify the conditions on which the RFP is based.

It should be noted that all or parts of the candidate’s response, as chosen by MPF, may form part of a final contract between the parties.

2.3 Terms & Conditions of Response

Every proposal received by the MPF is deemed to have been made subject to these conditions. No other terms will be deemed to be accepted by the MPF or incorporated into any contract between the MPF and any candidate unless they are expressly accepted in writing by an authorised signatory of the MPF.

Confidentiality	Responses of candidates to the present RFP will be evaluated by the Market Implementation Working Group (MIWG) of the Mobile Proxy Forum. The final selection of the supplier will be subject to endorsement by the Steering Committee of the Mobile Proxy Forum, a 'de facto association' in accordance with the relevant provisions of Belgian law. The members of the MIWG are bound by a dedicated confidentiality agreement. Notably, the Steering Committee may not be provided with individual, non-anonymised confidential information related to the submitter of a response to this RFP, and/or the services or products offered by such submitter. Once the endorsement of a candidate has been decided, the identity of that candidate will be made public.
Examination and explanation of RFP documents	The candidate shall be responsible for carefully examining the complete Request for Proposal, with any addenda, and making whatever further arrangements as may be required such that the candidate is fully informed and acquainted with all the circumstances and matters which might in any way affect the performance or cost of the services which are the subject matter of the candidate's response (the "Services"). Failure to do so is at the sole risk of the candidate and no relief shall be given for errors or omissions in the response to the RFP in estimating the difficulty or cost of performing the Services successfully. Should the candidate find discrepancies in, or omissions from, the Request for Proposal or relevant documents, or should these appear to be obscure or ambiguous, the candidate shall at once contact the MPF for clarification or correction thereof before submitting its proposal. Any candidate making a request for clarification or correction will be solely responsible for the timely receipt of such request by the MPF. Replies to such enquiries may be made in the form of written addenda that will be issued simultaneously to all candidates.
Unsolicited revisions to proposals	Unsolicited revisions to proposals will not be received favourably unless the candidate can substantiate to the MPF's satisfaction that a genuine error occurred during preparation of the original proposal. The MPF is under no obligation to accept such a revision.
Modification to RFP Documents	The MPF reserves the right to revise any provisions of the Request for Proposal. Such revisions, if any, will be in the form of written addenda which will be issued simultaneously to all candidates. Candidates shall immediately acknowledge receipt of the addenda by e-mail.
RFP Expenses	All costs and expenses incurred by the candidates in the preparation and submission of their response or in attending subsequent discussions or negotiations with the MPF, are entirely for their own account and the MPF shall not be responsible for such expenses.
Currency and language	All amounts will be in euro (EUR). All proposals, correspondence and communications shall be in the English language.

Form of proposal	The candidate shall base its response on the requirements of the MPF as stated in this Request for Proposal. However, should any candidate be unable to fulfil any of these requirements it must state clearly any and all exceptions to such requirements that it may have made with words such as "This response is subject to the following qualifications: ….
Submission of proposal	Proposals submitted shall be properly executed and completed by a representative of the respondent authorised to commit the candidate.
Closing Date	Proposals must be received by the MPF at the email address and no later than the Closing Date mentioned in sections 2.1 and 3.9 No late proposals will be considered.
Withdrawal	The MPF reserves the right to withdraw the RFP and not to award work or compensation to any party.
Awarding Authority	The MPF will enter into a formal agreement with the selected submitter(s) on terms and conditions to be finalised once the successful submitter(s) have been selected. A heads of agreement will be provided to short-listed submitters. The future governance structure of the Steering Committee of the MPFhas not yet been decided upon. It is possible that a central body would be set up as a dedicated legal entity, which would – amongst other things – govern the relationship with the selected submitter(s) of a response to this RFP. In sending a response, submitters agree that their response may be made available by the Steering Committee to such future body, which on the basis thereof may engage in further contractual negotiations. If no central body would be established, the decision to select one or more candidates will be made by the Steering Committee itself, on the basis of the recommendations made by the MIWG. In deciding the Steering Committee will strive for unanimous consensus. If no unanimous consensus could be reached, the Steering Committee will vote on the submitter(s) recommended by the MIWG. [Each Steering Committee member has one (1) vote. The decision to select one or more submitters shall be validly adopted if it obtains a qualified majority of two thirds (2/3) of the votes cast by the Steering Committee members present or represented (i.e. voting quorum). Blank votes, invalid votes and abstentions do not count. No decision may be passed if more than half of the Steering Committee members are not present or represented (i.e. presence quorum).]

2.3.1 Minimum period the candidate is required to keep open the offer

The RFP response must be open for acceptance up to three months from the closing date of the RFP. Any reservations in this regard must be specified in the RFP response.

2.3.2 Length of contract

The RFP response must take into account a contract length of minimum 3 years and maximum 5 years.

2.3.3 Preparation of RFP response

The RFP response shall be prepared according to the instructions given by the MPF in section 3 “Preparation and outline of RFP response” and must be written in English.

2.3.4 Consideration of questions

Questions concerning the RFP documents shall be sent by email as outlined in section "3.9 Guide for submission of proposal , queries and request for Q&A session". If possible, all questions must refer specifically to an exact reference in the RFP documents. Questions can be submitted on an ongoing basis, and the MPF may choose to send out replies successively. All questions and related answers will be made publicly available in an anonymised version on the EPC website.

3 Preparation and outline of the RFP response

3.1 RFP document

The candidate must organise their RFP response in accordance with section 3.

3.2 Background and introduction

3.2.1 Introduction to the candidate

The candidate must provide a description of their organisation, competencies, and key personnel in relation to the RFP response.

This includes a brief description of the candidate's production, delivery and service organisation as well as who are engaged in development, delivery and maintenance of the type of solution that is covered by the RFP.

3.2.2 Contact(s)

The candidate must specify the name, address, telephone number, email address and any other relevant contact information of the person at the candidate who is familiar with the RFP response and who can be contacted by the MPF.

3.2.3 Reservations

The candidate shall clearly indicate any reservations and conditions for assuming responsibility and undertake contractual guarantees according to the RFP documents.

Moreover, the possible implications of these reservations to the solution must be stated.

3.2.4 Sub-contractor(s)

The candidate must provide a listing of sub-contractors used to provide the solution, with a short description of each and information on which parts of the RFP they will be involved with. Any changes of sub-contractors during the project must be agreed with the MPF.

3.2.5 Business / cost model

Please provide a summary of the business / cost model of the project delivery, operations and maintenance.

3.3 Description of the solution

The candidate shall give a summary of the general description of the solution and how it will fulfil the needs and requirements of the MPF.

The description should at least include:

- Message flowchart

- Technical setup
- Security setup
- Maintenance
- Other functionality such as billing, administration etc.

The description should include general functionality and maintenance (if applicable) and the technical setup.

3.4 Project delivery

A high-level project plan indicating development and testing phases and expected resources needed from the MPF and P2P solutions that would connect to the SPL.

The service must be operational by October 2018 as a minimum viable product. The MPF expects that on boarding information to P2P solutions should be available in June 2018 and access to testing for P2P solutions should be available mid-August 2018 at the latest.

3.5 Conditions

3.5.1 Licences

The candidate must include a description of any licences included in the offered solution as well as the specific conditions under which these licenses are valid. This should include information on the need for registered single user licenses and/or concurrent user licenses. Furthermore, the candidate must describe included functionalities/user rights under each license type(s).

3.5.2 Quality

The candidate's quality system/policy must be outlined.

3.5.3 3.5.3 Risk-analysis

The candidate must include a description of the largest risks, as determined by them, in an infrastructure project, including:

- Project related risks such as resources, schedule, etc.
- MPF related risks such as resources, availability, etc.
- Candidate related risks such as software, sub-contractors, etc.

3.6 Requirements

The candidate must provide an answer to each individual requirement detailed in:

- Appendix A: Functional Requirements
- Appendix B: Non-functional Requirements
- Appendix C: Legal and compliance Requirements
- Appendix D: Financial Requirements

3.6.1 Appendix A: Functional Requirements

Please fill out the columns under "Candidate response".

If your solution cannot support a specific requirement please state "N/A" in the column "Solution description".

3.6.2 Appendix B: Non-functional Requirements

Fill out the columns under “Candidate response”.

3.6.3 Appendix C: Legal and Compliance Requirements

Fill out the columns under “Candidate response”.

3.6.4 Appendix D: Financial Requirements

Fill out the columns under “Candidate response”

3.7 Response to questions addressed to the Candidate

If applicable, the candidate should outline their response to the questions addressed to the candidate in section 10 of this document.

3.8 Miscellaneous

Here, the candidate may describe other conditions that are considered relevant to the MPF’s evaluation of the RFP response such as datasheets, brochures, certifications, etc.

3.9 Guide for submission of proposal, queries and request for Q&A session

All RFP response documents, including correspondence and questions, must be submitted to MPF electronically. Emails must be sent in the format:

To:

CC:

Subject MPF RFP [*candidate name*] – [*brief description of email content]*

Files must be attached to the email in the following format:

Document	Filename	File Format
RFP document	MPF [*candidate name]* RFP version [#]	.docx or .pdf
Appendix A: Functional Requirements	MPF [*candidate name]* appendix A version [#]	.docx or .pdf
Appendix B: Non-functional Requirements	MPF [*candidate name]* appendix B version [#]	.docx or .pdf
Appendix C: Legal and compliance requirements	MPF [*candidate name]* appendix C version [#]	.docx or .pdf
Appendix D: Financial requirements	MPF [*candidate name]* appendix D version [#]	.docx or .pdf
Other documents relevant to the RFP as determined by the candidate	MPF {*candidate name*] [*relevant file name*]	as applicable
Presentation of the solution/RFP	MPF [*candidate name]* solution presentation version [#]	.pptx or .pdf

The email to be used is: p2pmobile@epc-cep.eu

Candidates must ensure that any emails sent to p2pmobile@epc-cep.eu are free from any virus or other malware. In consideration of their participation in the RFP process, each candidate agrees to indemnify the EPC from and against all costs, expenses, losses or damages that may result from the electronic copy being infected by a virus or other malware.

4 Functional requirements

4.1 Overview of SPL requirement

The SPL is intended to enable interoperability between registry providers who in the line of their business enable a mobile phone number with international prefix to be used to retrieve a linked IBAN for the (sole) purpose of initiating a payment to the holder of that IBAN. In its initial application, this is intended to enable mobile P2P payments to be made between existing mobile payments based schemes within countries in the Single Euro Payments Area (SEPA).

The MPF has created a set of rules for the functioning of the SPL service. These can be found at the European Payment Council website here.

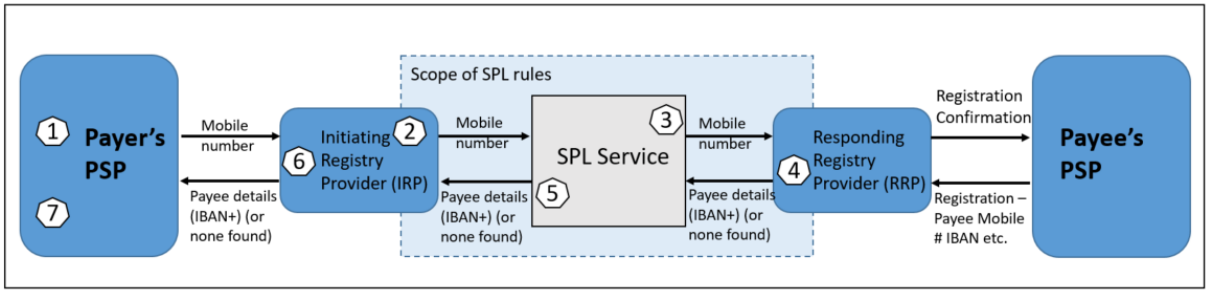
4.2 Overview of SPL capability requirement

Service consists of a messaging infrastructure being able to interconnect different registry providers that will be capable to convert a proxy (initially a mobile phone number but some others are foreseen to be adopted in the future) into an IBAN in real time, for the purpose of payment initiation. The Payment itself is considered out of scope of the SPL. The SPL's sole purpose is to provide sufficient information so that a payment can be initiated by the payer's PSP.

Actors participating:

- SPL Scheme Manager: Entity in charge of defining SPL Service rules and scheme.
- SPL Service Operator: Technical provider in charge of supplying and maintaining SPL Service.
- IRP (Initiating Registry Provider): entity that makes a lookup request into SPL Service and receives a single response with conversion required.
- RRP (Responding Registry Provider): entity owning a directory of proxy to IBAN conversion that responds to a lookup request from SPL Service.

Scope and use case of SPL is as per figure that follows:

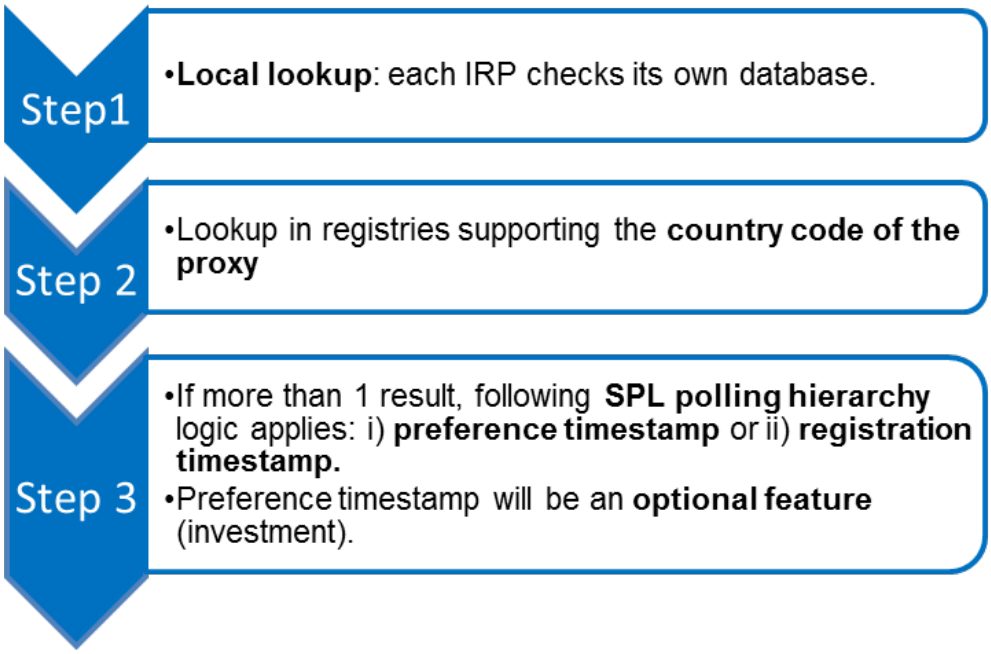


Workflow will be as follows:

1) Payer uses mobile app to enter payee's mobile #. PSP requests payee info from IRP.

2) IRP (proxy service) checks own database for mobile#. If unsuccessful, request is passed to SPL.
3) SPL uses polling hierarchy rules to send request to RRP(s)
4) On receipt of message from SPL, RRP checks database and responds to SPL service with payee's IBAN if available and possible additional information (e.g. name of account holder).
5) On receipt of request, SPL replies to IRP with payee's IBAN + additional information if available. In case of more than 1 result, the SPL applies polling hierarchy logic before passing on the single response.
6) IRP forwards payee's details or null response to Payer's PSP.
7) Payer receives confirmation of payee ID and instructs PSP to make payment.

The polling hierarchy is defined by the Steering Committee of the MPF in the SPL rules for operating, joining and participating on the SPL (please refer to page 5 here and diagram below).



Functional requirements:

Reference	Functional requirements
FU-R1	The SPL must be compliant with the SPL rulebook v. 1.1. which is available at the EPC website. A direct link is here.
FU-R2	The technical working group of the MPF has defined APIs that can be used in the solution to maximize interoperability. The APIs are designed to be in alignment with the Berlin Group standard. The current version of the API standards document is version 0.5 and can be found in Appendix E.

4.3 FU-R1 – The SPL must be compliant with the SPL rules

The MPF have defined a set of rules for the functioning of the SPL. The current version of the rules is v.1.1 which will be the reference for this RFP. The document (SCP2P 018-16 V1.1) can be found here.

In case the SPL rules are updated, the SPL must implement the changes. A process for this will be set up depending on the outcome of the RFP.

4.4 FU-R2 – The SPL should use the APIs defined by the MPF

In order to ensure interoperability across Europe the TWG group has developed a set of APIs. The current version of the API specification is v.0.5 and it can be found in Appendix E. Candidates may include comments on this document in their response.

In case the candidate already has an out-of-the box solution which uses other standards these can be suggested in the RFP response. Please note that these standards must then be made available to any P2P solution provider who wants to join the SPL service.

5 Non-functional requirements

The SPL solution for MPF will at least be governed by the following set of non-functional requirements:

Reference	Non-functional requirements
NF-R1	Volumes
NF-R2	Availability and Performance
NF-R3	Data retention and data protection
NF-R4	Security
NF-R5	Statistics
NF-R6	Billing

Proposals for the SPL solution can provide guidance on other relevant non-functional assets but from the MPF's perspective the above set of non-functional requirements defines at a minimum the SPL system's overall properties that go across all functional capabilities and requirements.

5.1 NF-R1 - Volumes

According to the latest study on the use of cash published in November 2017 by the ECB there were about 6 billion non-POS ("P2P") cash payments in the euro area in 2016. Assuming a conservative 2% share of cross-border payments this would mean that there could be some 120 million cross-border non-POS ("P2P") cash payments per year in the euro area.

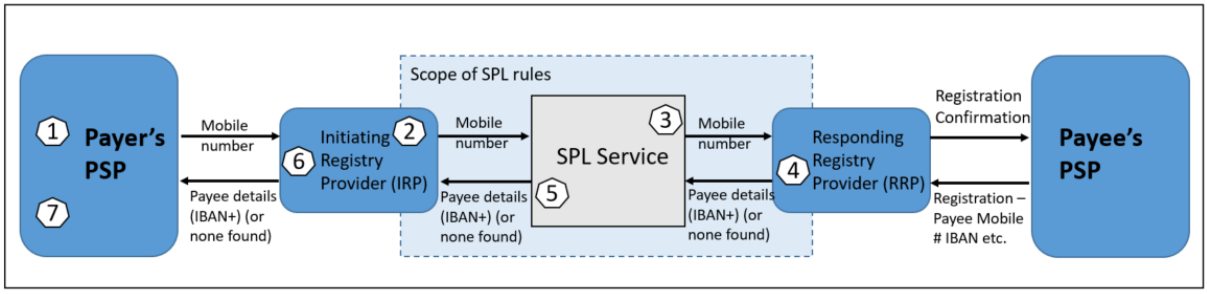
Applying the estimated average preference for non-cash payments (43%) would yield a potential of about 56 million cross-border non-POS ("P2P") non-cash transactions per year in the euro area. This implicitly assumes the lack of any alternative to cash for settling cross-border "P2P" "face-to-face transactions" in the euro area currently (i.e., in 2016); if this assumption were to be too conservative the above-mentioned potential number would be higher. The SPL solution has to be able to eventually service these volumes. However, we recognise that this will not be a big bang and lower volumes are expected initially.

- Initial volumes from 1 million per annum growing to 20 million transactions during the 5 year contract; however, the volume could increase significantly in case person-to-business ("P2B") services would be added;
- scalable to accommodate higher volumes;
- number of connected IRPs/RRPs: 10 – 50 (within the 5 years);
- peak hourly volumes at least at 10% of average daily volumes;

5.2 NF-R2 – Availability and Performance

With P2P/P2B as a significant use case for Instant Payment Services, especially those provided under the SCT Inst scheme, the SPL solution requires continuous availability. Therefore, the SPL solution has to offer:

- 24/7 with target of 100% availability;
- maximum switching time per message: 50 ms please refer to step 3 and 5 in the diagram below



Please refer to section 4.2 for an explanation of each step.

- An operational and technical helpdesk must be available during regular business hours
- Contingency procedures must be available in case there are operational incidents outside regular business hours.

5.3 NF-R3 – Data retention and data protection

Because the SPL solution is strictly a messaging platform and not a database or registry service, data retention of request and response logs and audit trails for supporting services (invoicing, billing, reporting, dispute handling etc.) should be securely stored for at least 3 months. The system and access mechanisms must enable compliance with the relevant European data protection rules and regulations.

5.4 NF-R4 – Security

The following security requirements are considered relevant for the SPL solution:

- not create additional vulnerabilities to the connected registry providers' systems;
- support secure communication channels and industrial strength security software and procedures for data storage protection, aligned with the functional requirements;
- support key data encryption at end transmission points;
- achieve "zero fault tolerance" in all operational controls;
- support an Information Security Policy with regular internal or external security audits;
- support a Physical Security Policy with authentication and access controls to validate access to systems and data centres;
- support a comprehensive Business Continuity Management concept with procedures and a Disaster Recovery Plan with procedures;
- support Organisational Security based on recognised standards (BS7799, ISO 27001);
- support systems development guidelines based on recognised standards;
- compliance with all applicable national and European (EEA/EU) cross-border laws and regulations on payment systems (including data privacy);
- In case the solution includes elements of the Connect Europe eDelivery service please state this explicitly.

- In case the candidate decides to follow the API standard specified by the technical working group of the Mobile Proxy Forum the security requirements mentioned in the 'Standardised Proxy Lookup API Specification' v. 0.5 document must also be followed. The document can be found in Appendix E.

5.5 NF-R5 – Statistics

The statistics capability should collect data for analysis on performance improvement, possible reporting to competent authorities etc.

The key business deliverables for this capability are:

- Statistics on number of queries and response time per IRP and RRP.
- Statistics on number of unsuccessful queries.
- When/if more proxies are introduced basic statistics for each proxy type b
- The statistics must be made available to the MPF in a machine-readable format.

5.6 Billing

The RFP provider will directly bill the participating P2P solutions.

- A billing functionality must be in place

5.7 Potential usage of the European Commission's eDelivery Service

If a candidate expects to include elements of the European Commission's eDelivery Service this should be explicitly mentioned.

6 Legal and compliance requirements

Exchanging proxies such as mobile phone numbers with personal information such as the IBAN and name of the account holder touches upon among others data protection regulations across Europe.

Reference	Legal requirements
LC-R1	Compliance with European regulations

6.1 LC-R1 – Compliance with European regulations

The solution must be compliant with current European regulations and the respondents must describe how compliance with these regulations are envisioned. Required to stay compliant with future European regulations at respondent's own costs.

7 Financials

The Mobile Proxy Forum expects that any costs of the SPL will be covered by the participating services via the operational fees and a possible initial entry fee.

Reference	Financial requirements
FI-R1	Commercial model for the SPL
FI-R2	Low entry barriers

Reference	Financial requirements
FI-R3	Additional costs

7.1 FI-R1 – Commercial model for the SPL

The initial project costs, development costs, test costs and operational costs must all be covered by a commercial transparent model that either covers all costs via the operational fees or a mix of operational fees and a fixed entry fee.

7.2 FI-R2 – Balanced commercial model

The commercial model must be balanced so that small new entrants can join and use the service at reasonable costs but large and very active participants should also benefit for provided scale.

7.3 FI-R3 – Additional costs

Please describe any costs on optional services that may or may not be offered beyond the scope of this RPF.

8 Evaluation criteria

Responses of candidates to the present RFP will be evaluated by the Market Implementation Working Group (MIWG) of the MPF. The final selection of the supplier will be subject to endorsement by the Steering Committee of the MPF, a 'de facto association' in accordance with the relevant provisions of Belgian law. The members of the MIWG are bound by a dedicated confidentiality agreement. Notably, the Steering Committee may not be provided with individual, non-anonymised confidential information related to the submitter of a response to this RFP, and/or the services or products offered by such submitter.

MPF will evaluate the proposals based on, but not limited to, the following criteria: which are not listed in a prioritised order, however criteria listed in **bold** must in any event be fulfilled:

- **Capability to meet desired functional and non-functional requirements.**
- The requirements for the commercial model and the envisioned fees.
- Experience with similar kind of implementation.
- Experience with operating a similar type of service.
- **Capability to meet compliance and legal requirements.**
- Future roadmap for the solution.

9 Questions addressed to Candidate

This section includes questions to the candidates that are not specifically related to our functional and non-functional requirements.

Answers to these questions should be detailed as outlined in section 3.1.6 "Response to questions addressed to the candidate".

No.	Question
1	What additional functionality is provided other than specifically referred to in our functional or non-functional requirements? If applicable, please provide a summary description.

2	How do you envisage a future roadmap for the solution? Which additional services do you expect to add over the next 3-5 years?

10 Appendix A – Functional Requirements

Reference	Candidate response	Solution description
F-R1		
F-R2		
F-R3		
F-R4		

11 Appendix B – Non-functional Requirements

Reference	Candidate response
NF-R1	
NF-R2	
NF-R3	
NF-R4	
NF-R5	
NF-R6	

12 Appendix C – Legal and Compliance Requirements

Reference	Candidate response
LC-R1	

13 Appendix D – Financial Requirements

Reference	Candidate response
FI-R1	
FI-R2	
FI-R3	

14 Appendix E – Standardised Proxy Look-Up API Specification V0.5

THE PRESENT DOCUMENT CONSTITUTES THE DRAFT VERSION 0.5 OF THE "STANDARDISED PROXY LOOK-UP API SPECIFICATION", DATED 20 DECEMBER 2017. IT HAS BEEN DRAFTED BY THE TECHNICAL WORKING GROUP OF THE MOBILE PROXY FORUM, A 'DE FACTO ASSOCIATION' IN ACCORDANCE WITH THE RELEVANT PROVISIONS OF BELGIAN LAW.

THIS DRAFT VERSION 0.5, WHICH MAY BE SUBJECT TO FURTHER CHANGE, IS PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED. THE MOBILE PROXY FORUM DOES NOT ACCEPT LIABILITY FOR ANY ERRORS OR OMISSIONS. THE MOBILE PROXY FORUM WILL NOT BE LIABLE FOR ANY CLAIMS OR LOSSES OF ANY NATURE ARISING DIRECTLY OR INDIRECTLY FROM USE OF ANY INFORMATION, DATA, DOCUMENTATION OR OTHER MATERIAL RELATED TO THIS DOCUMENT.

STANDARDISED PROXY LOOKUP SPECIFICATION

1- SCOPE

This document is an implementation specification of a Standardised 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 Standardised Proxy Lookup (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:

a) The description of the Standardised Proxy Lookup (SPL) service and roles;

b) The SPL functional model list as a system made up of logical components and interfaces;

c) The API for the communication between the Initiator Registry Provider and the SPL;

d) The API for the communication between the SPL and the Responder Registry Provider(s);

e) The list of Data Elements required to support the communication through both APIs;

f) A standard algorithm to be executed by the SPL for the selection of a unique IBAN;

g) A security architecture.

It is out of the scope of this document:

1. The effective execution of the mobile person-to-person payment;
2. 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.

2- INTRODUCTION

The Mobile Proxy Forum is an organization intended to specify and operate a pan-European scheme for a service of mobile person-to-person payments (P2P).

Three types of entities, Initiator Registry Providers (IRP), Responder Registry Providers (RRP) and an intermediary Standardised Proxy Lookup (SPL) are needed to provide the service. The IPR and the RRP don't 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:

- Ch6 sets out the functionalities and requirements for the entities participating in the service;
- Ch7 specifies the two APIs offered by the SPL to the enrolled IRP(s) and IRP(s);
- Ch8 identifies the list of Data Elements to be used during the SPL transaction;
- Ch9 specifies the Standardised Proxy Lookup Service Algorithm;
- Ch10 sets out a security architecture for the SPL service; and

- Ch11 discusses and proposes some Data Protection requirements.

The SPL service is intended to enable mobile person-to-person (P2P) payments to be made between existing mobile payment base schemes within countries adhering to the Single Euro Payments Area (SEPA). This specification assumes that the payer is a natural individual and the beneficiary is a natural person or a small business entity legally recognized as a “person”.

The payment is settled between two bank payment accounts, the payment account of the originator and the payment account of the beneficiary, identified by the IBAN returned by the SPL. It is assumed that both banks have access to a common Clearing and Settlement Mechanism (CSM).

The mechanism used by the originator and the originator’s bank to initiate and complete the payment is out of the scope of this specification.

3- TERMINOLOGY

1. SPL Cache

SPL storage of a directory associating mobile phone numbers and the RRP(s) where the associated IBAN is available.

2. Standardised Proxy Lookup

Directory service which forwards to the IRP an IBAN associated to a mobile phone number provided by a RRP.

3. Initiator Registry Provider (IRP)

Entity that queries the Standardized Proxy Lookup for the IBAN associated to the mobile phone number of the beneficiary of the payment.

4. Responder Registry Provider (RRP)

Entity that upon request by the Standardised Proxy Lookup provides the IBAN associated to the mobile phone number of a customer.

5. Proxy

Data required by the SPL service in order to retrieve a payment account identifier. In this specification, the proxy is the mobile phone number of the beneficiary of the payment.

6. Standardised Proxy Lookup Service Operator

Entity designated to operate the Standardised Proxy Lookup service by offering API's for the connection of the IRP(s) and RRP(s) participating in the Mobile Proxy Forum scheme.

7. Time stamp

Data encoding the enrolment and preference date of a customer by an RRP.

There are two types of time stamps:

- Preference time stamp (optional) is the time at which a preference was explicitly indicated by the customer (beneficiary);
- Registration time stamp (mandatory) is the time at which the customer registered with the service.

8. Standardised Proxy Lookup Service Algorithm

Algorithm to be implemented by the Standardised Proxy Lookup service to select just the IBAN to be transmitted to the IRP when there is more than one responding RRP (two or more IBANs received by the SPL).

9. 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.

4- LIST OF ACRONYMS

- IRP Initiator Registry Provider
- IBAN International Bank Account Number
- PLA Standardised Proxy Lookup Service Algorithm
- RRP Responder Registry Provider
- SPL Standardised Proxy Lookup

5- APPLICABLE DOCUMENTATION

D1. Mobile Proxy Forum Steering Committee: Rules for operating, joining and participating in the Standardised Proxy Lookup (SPL) service

D2. Berlin Group Mobile P2P Interoperability Framework Operational Rules v1.0

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

6- REQUIREMENTS FOR THE ENTITIES PARTICIPATING IN THE STANDARDISED PROXY LOOKUP SERVICE

1. Components and Interfaces for Interoperability

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

1. The Initiator Registry Provider (IRP), for instance a financial institution, which offers the service to customers acting as originator.
2. The Responder Registry Provider (RRP), which enrols customers acting as beneficiaries 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).
3. A Standardised Proxy Lookup (SPL) service, which intermediates 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 Initiator Registry Provider (IRP), acting as an agent of the originator, interacts with the Standardised Proxy Lookup 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 Responder Registry Providers (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 Initiator Registry Provider (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 Ch8 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 Initiator Registry Provider, and the beneficiary has a contractual agreement with a second entity, the Responder Registry Provider. Both the Initiator Registry Provider and the Responder Registry Provider have a contractual agreement with the Standardised Proxy Lookup Service (SPL), which is operated by a third entity.

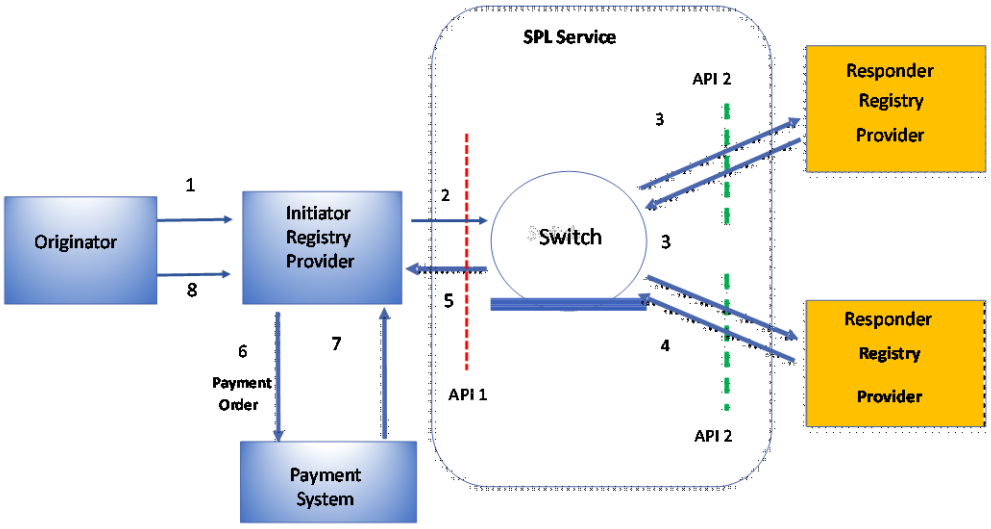


Figure 1 High Level Functional Model for the Proxy Lookup

2. List of functionalities to be supported by the SPL Operator

i. SPL Operator management responsibilities

1. Provide an interface to contract with both IRP(s) and RRP(s) for access to the SPL service providing a sufficient level of information;
2. Assign a unique identifier for the enrolled IRP(s) and RRP(s) to be used in the corresponding Data Element(s) of Ch8;
3. Authenticate both the IRP and the RRP identities during a transaction;
4. Validate any IRP request;
5. Forward exclusively to the RRP(s) validated IRP requests using the identifier of the IRP;
6. Validate RRP(s) responses;
7. Provide the IRP with only one IBAN associated with a validated RRP response;
8. Establish a secure communication channel with either the IRP or the RRP when required;

9. Maintain a transaction log without storing personal data (originator and/or beneficiary of the payment) for at least a three-month period;
10. Facilitate any audit upon request by the Mobile Proxy Scheme entity;
11. Certify operational practices as well as sensitive components required for the SPL operation: APIs, cryptographic devices, storage, processing and communication hardware and software components;
12. Maintain its own technical infrastructure according to future evolutions of this specification.

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

ii. Infrastructure components under the responsibility of the SPL Operator

The SPL Operator shall be responsible to develop and made available an implementation of this technical specification.

Therefore, the SPL Operator shall implement and maintain the following computing, storage and processing components:

1. An API supporting a Request/Response exchange with the SPL initiated by an IRP according to the requirements set out in Ch7 using the list of Data Elements in Ch8 (Request by the IRP, Response by the SPL);
2. A polling process according to the requirements set out in Ch7 for API-2;
3. An implementation of the Standardised Proxy Lookup Service Algorithm (PLA) as specified in Ch9;
4. Authentication servers for the authentication of the IRP(s) and the RRP(s) according to the requirements set out in Ch10;
5. Cryptographic devices and associated components (see Key Management Systems, 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 Ch10;
6. Databases for the SPL transaction data log, protected according to the requirements set out in Ch11;
7. 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 RRPs are out of the scope of the specification;
- The Scheme may propose a contractual “Service Level Agreement” to the Service Proxy Look Up operator.

iii. List of optional functionalities

SPL optional functionalities refer to:

- Internal arrangements of the SPL Operator in order to improve the quality of the service. An example is the implementation of a SPL cache. This cache may store a directory associating mobile phone numbers and a reference to the RRP(s) where the associated IBAN is available. In that case, the cache helps the SPL to connect directly to a particular RRP to retrieve the IBAN instead of performing a query addressed to all the enrolled RRPs;
- Support of Data Elements for Value Added Services

    - Ch8 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 bank 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;
- Other (TBD).

3. Responsibilities of the IRP

The IRP shall:

- Enrol with the Mobile Proxy Scheme and contract with the SPL for the service;
- Provide a mobile phone mechanism for access of the originator to the Standardised Proxy Lookup 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;
- 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 the IBAN to initiate the payment order;
- Not to store the IBAN of the beneficiary of the payment once the payment has been executed;
- Provide SPL transaction data required to resolve a dispute;
- Certify the components required for access to the service according to the Mobile Proxy Certification program.

4. Responsibilities of the RRP

The RRP shall:

- Enrol with the Mobile Proxy Scheme and contract with the SPL 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 Ch9 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 authorization 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 provide the IBAN associated to the received mobile phone number;
- Upon request provide SPL transaction data evidence for the resolution of a dispute;
- Certify the components required for access to the service according to the Mobile Proxy Certification program.

7- API Specifications

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 steering committee of the Mobile Proxy Forum.

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 lockup mechanism, and the corresponding API, which are relevant for the SPL service.

The Berlin Group specification supports both a centralized and a decentralized 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 will be used to implement the technical interfaces of the SPL service.

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 1.0 (09/06/2017): 5.1.1 Repository Lookup;
- Mobile P2P Interoperability Framework Implementation Guidelines 1.0 (09/06/2017): 3.3.1 Repository Lookup;
- Mobile P2P Interoperability Framework Implementation Guidelines 1.0 (09/06/2017): 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 chapter 10 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.

3. API for the communication between the IRP and the SPL

If the IRP makes a request to the SPL in order to lookup for 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 chapter 8.2, it executes the SPL algorithm which is specified in chapter 9 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 RRPs following the SPL algorithm execution nor gets any information about the details of the execution of the routing algorithm and the poling hierarchy. The SPL shall only return the IBAN, if one could be identified, and the supporting information as described in chapter 8.3.

4. API for the communication between the SPL and the RRP

During the execution of the polling hierarchy the SPL contacts one or several RRPs as described in chapter 9.2. 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 RRPs via the JSON-

based REST service API, containing the information described in chapter 8.2, 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 on 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 chapter 8.3.

8- DATA ELEMENTS

1. Introduction

The Data Elements referred in this chapter shall be used:

a. In the messages exchanged between the IRP and the SPL; and
b. In the messages exchanged between the SPL and the RRP.

These Data Elements are listed in the two tables below. Please find below the figure adopted by the Technical WG 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.

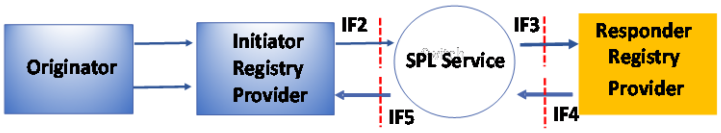


Figure 2 Interfaces (IF2-IF3-IF4-IF5) for the Data Elements to be exchanged in the APIs

1. The first Table summarizes the Data Elements needed to execute a Lookup Request. These Data Elements are conveyed in the interface IF2 (between the Initiator Registry Provider "IRP" and the SPL service) and in the interface IF3 (between the SPL service and the Responder Registry Provider "RRP");

2. The second Table summarizes the Data Elements needed to execute a Lookup Response. These Data Elements are conveyed in the interface IF4 (between the Responder Registry Provider "RRP" and the SPL service) and in the interface IF5 (between the SPL service and the Initiator Registry Provider "IRP").

Both Tables contain six columns organized as follows:

C1: Data Elements, respecting the name and identifier assigned by the Berlin Group;

C2: "Purpose" is a rewording of the Berlin Group definition of the Data Element;

C3: 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;

C4: Indicates if the Data Element is Mandatory/Optional in the Berlin Group Specifications (noted "BG" M/O);

C5: Proposal for the Data Element to be Mandatory/Optional in the MPF API Specification. Note that the Data Element may also be "Conditional". The meaning of Conditional is explained.

2. List of Data Elements for the SPL Request

C1 Data Element	C2 Purpose	C3 Interface		C4 Berlin Group (M/O)	C5 MPF (M/O)
		IRP –> SPL (IF2)	SPL-> RRP (IF3)		
Mobile Number Beneficiary (AT 01)	Encodes the alias (phone number) of the beneficiary	**X**	**X**	**M**	**M**
Mobile Number Originator (AT – 13)	Encodes the phone number of the originator The Receiver Scheme can mandate to provide personal IBAN data only to Originators which are on a customer's white list	**X**	**X**	**O**	**O**
Originator Scheme ID (AT – 02)	Identifies the Originator Scheme by a unique identifier (*to be specified*)	**X**	**X**	**M**	**M**
Receiver Scheme ID (AT – 03)	Identifies the Receiver Scheme by a unique identifier (*to be specified*)	**X** Conveys the scheme ID of the SPL	**X** Conveys the scheme ID of the RRP contacted by the SPL	**M**	**M**
Transaction Amount (AT – 04)	The transaction amount in Euros	**X**	**X**	**O**	**O**

Lookup Request Reference Data (AT – 05)	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**	**M**
Time stamp Request (AT – 06)	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**	**M**

3. List of Data Elements for the SPL Response

Data Element	**Purpose**	**Interface**		**BG (M/O)**	**MPF(M/O)**
		SPL –> IRP (IF5)	**RRP -> SPL (IF4)**		
Lookup Request Reference Data (AT – 05)	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**	**M**
Response Result Yes/No (AT – 08)	Indicates whether the alias could be matched to account data or not.	**X**	**X**	**M**	**M**
Reason Code (AT– 09)	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”	**C** Conditional: Mandatory only if AT-08=”No match”
Originator Scheme ID (AT – 02)	Identifies the Originator Scheme by a unique identifier (*to be specified*)	**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**	**M**
Receiver Scheme ID (AT – 03)	Identifies the Receiver Scheme by a unique identifier (*to be specified*)	**X** Conveys the SPL scheme ID or the scheme ID of the	**X** Conveys the scheme ID(s) of the RRP(s) contacted by the	**M**	**M**

		single RRP selected by the polling hierarchy is to be included	SPL that is responding to the request		
Creditor Account Data (IBAN, Type "IBAN") (AT – 10)	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 RRPs	**C** Conditional: Mandatory only if AT-08="match"	**C** Conditional: Mandatory only if AT-08="match"
Creditor Account Type Indicator (AT – 11)	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.	**C** Conditional: Mandatory only if credit account does not equal the beneficiary account.
Name Beneficiary (AT – 12)	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**	**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)	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**	**O**
Preference Indicator (AT – 15)	The Beneficiary might be registered in more than one Mobile P2P Scheme with the same MSISDN. Some schemes	**X** In case of eDelivery Implementation this	**X**	**O**	**O**

	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.	information is needed by the IRP, but is delivered through the eDelivery metadata not through this Data Element.			
Registration Time stamp (AT – 16)	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** In case of eDelivery Implementation this information is needed by the IRP, but is delivered through the eDelivery metadata not through this Data Element.	**X**	**M**	**M**

9- Standardised Proxy Lookup (SPL) service logic

1. Overview

This chapter describes the logic of the SPL service which has been agreed on in the "Rules for operating, joining and participating in the Standardised Proxy Lookup (SPL) service" by the MPF. The logic takes care of making the requests to the different participants (RRPs) in the service and to evaluate the answers to requests and decide, 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:

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

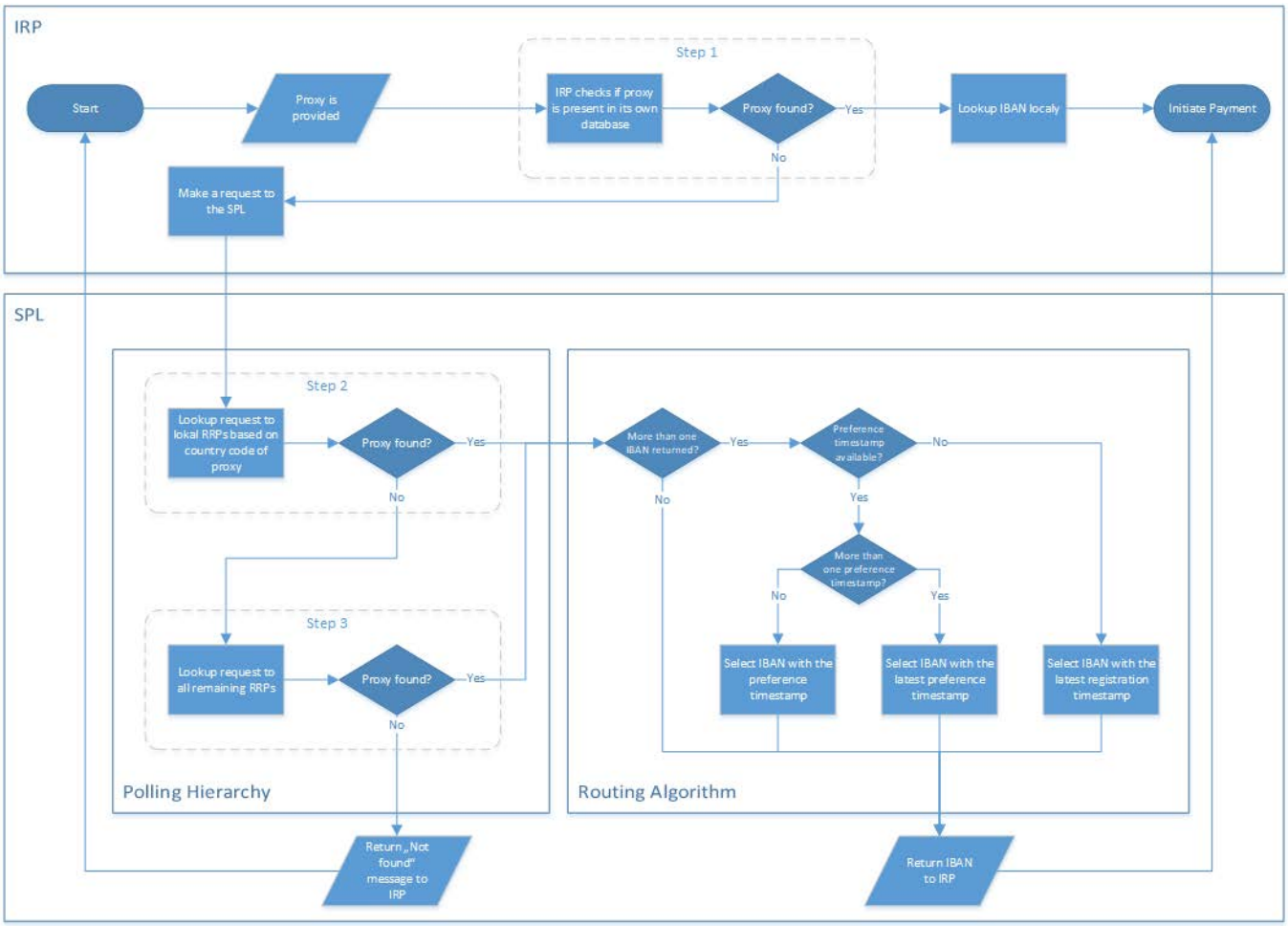


Figure 3 Flow of an SPL lookup request

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

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 RRPs using the mobile phone number as a proxy. In order to request the information from the appropriate RRPs the following polling hierarchy shall be executed, as defined in the "Rules for Operating, Joining and Participating in the SPL Service":

- **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 to local RRPs based on the **country code of the proxy;**
- **Step 3:** Lookup request to all remaining RRPs.

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 (*message structure and encoding to be decided*) 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 Standardised Proxy Lookup Service. In this case the payment cannot be initiated and

the user has to start over with a different phone number or the payment service may offer to send a notification to the beneficiary to ask him to register for the service.

The SPL shall also proceed with the next logic process if no response is provided after a predefined timeout (e.g. within 1 second). In step 2 and step 3 the SPL shall wait for a response from all RRP a request was sent to until the timeout has reached. It shall not proceed to the next logic process even if there is a response from one or more RRPs before the expiration of the timeout.

Note:

The timeout value still has to be defined.

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:

4. 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).
5. If there are more than one validated RRP response, 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.

10- SPL SECURITY ARCHITECTURE

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 Mobile Proxy Scheme.

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 centralized 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:

(1) The RRP databases storing payment beneficiary information are safe.
(2) 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 Mobile Payment Scheme, IRP(s), RRP(s) and the SPL Operator 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 Chapter 10.2.

2. Security Objectives (TBC)

O1: The databases required for the SPL service protect the integrity and the confidentiality of the enrolled customer personal information at rest

O2: Only the legitimate participants in the 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 bank

O6: The SPL service cannot be misused for the purpose of retrieving information not intended to initiate a payment

3. Security Requirements (TBC)

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 RRPs

R2: The customer information provided during the enrolment process and stored in a record in a 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 RRPs 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 in the payer shall:

- 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
- 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

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 assure 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. While we think this provides a sufficient level of security and allows a lightweight implementation on the SPL site as well as on the IRP/RRP site, an additional layer of security can be achieved by optionally implementing the AS4 protocol for the communication between IRP and SPL and RRP and SPL. The following chapters provide some more detailed information on both approaches.

i. 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 chapter 7.3 and chapter 7.4 of this specification. End-to-end encryption is not supported by JSON REST services. However, for the proxy look-up, 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 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 RRPs 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.

ii. Communication via AS4

Optionally the communication can be achieved via AS4 which is part of the eDelivery service specified by the European Commission. See URL bellow.

AS4 is based on a four-corner messaging topology that provides secure channels between access points. The communication between the access points is done via an asynchronous model in comparison to the synchronous communication model described in the previous chapter.

Although AS4 is capable of transporting any kind of payload between the access points the standard approach is to exchange XML based messages through the secure channel. To facilitate the implementation and to leverage on a proven approach the SPL service also shall communicate via XML based SOAP messages in contrary to chapter 7.2 which requires the implementation of the API as a JSON-based REST service.

This means that in case the SPL implementation uses AS4 chapter 3.4 XML Based Encoding instead of chapter 3.3 JSON Based Encoding of the Mobile P2P Interoperability Framework Implementation Guidelines 1.0 (09/06/2017) shall be implemented in the SPL as well as in the IRP and RRP.

For the implementation of the AS4 access points within the SPL service and the IRP and RRP the following specification shall be followed:

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-SENS+AS4+-+1.12

iii. Comparison of HTTPS and AS4

HTTPS via TLS	AS4
Synchronous communication	Asynchronous communication but in a way that a synchronous communication may be “almost” emulated
Point-to-Point communication	Four-Corner topology
Straight forward implement at IRP and RRP site	Integration of the access points and APIs needed
Quick time to market	Some (limited) additional implementation time for SPL and IRP/RRP

Proven security at network level based on HTTPS, TLS and mutual authentication through certificates.	Additional protection via a secure channel: Integrity Protection and Non-Repudiation of Origin, Confidentiality, Non-Repudiation of Receipt and Authorization

11- DATA PROTECTION REQUIREMENTS

The SPL service requires the exchange of personal information between the participants in the Scheme. It matters that the personal information be disclosed to only authorized parties for the purpose of the payment.

A trade-off traceability vs privacy is to be found because wrong Instant Credit Transfers will cause an unacceptable financial loss to the payer:

- A mechanism to confirm that the beneficiary of the payment will be the one intended by the payer is necessary. That means the storage and transfer of some personal identity attribute. This information is to be minimized but must be sufficient for the purpose of the confirmation of the identity of the payment beneficiary.
- The resolution of disputed payments requires the storage of transaction information by the parties participating in the payment (payer, beneficiary, IRP, SPL, RRP, payer bank, payee bank, C&S facility).
    - This information is again (1) to be minimized (2) fit for purpose (3) not facilitating fraud if compromised but sufficient to establish the respective liabilities

NOTE

The financial institutions involved in the payment: the payer bank and the beneficiary bank must comply with their legal duties in terms of Customer Due Diligence according to the EU Anti-Money Laundering Legal Framework. In particular the legal identity of the beneficiary of the payment is to be included in the payment order generated by the payer bank. This identity is available in the RRP customer record and could therefore be transmitted to the IRP by the SPL. This identity information associated to a phone number and an IBAN represent a piece of personal sensitive information to be protected according to the European Legal Framework on Data Protection.

However, the present version of the specification does not address the transmission of personal identity information (name of the beneficiary).