THE Berlin GROUP

A EUROPEAN STANDARDS INITIATIVE

Joint Initiative pan-European Mobile P2P Interoperability

Mobile P2P Interoperability Framework

Implementation Guidelines

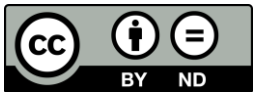
Version 1.2

06/11/2020

License Notice

This Specification has been prepared by the Participants of the Joint Initiative pan-European Mobile P2P Interoperability[*] (herafter: Joint Initiative). Participation to the Joint Initiative does not imply either endorsement of any of the solutions identified in this Specification or a commitment to implement them. This Specification is published by the Berlin Group under the following license conditions:

- "Creative Commons Attribution-NoDerivatives 4.0 International Public License"

  This means that the Specification can be copied and redistributed in any medium or format for any purpose, even commercially, and when shared, that appropriate credit must be given, a link to the license must be provided, and indicated if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. In addition, if you remix, transform, or build upon the Specification, you may not distribute the modified Specification.

- Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The Berlin Group or any contributor to the Specification is not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.
- The Specification, including technical data, may be subject to export or import regulations in different countries. Any user of the Specification agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import (parts of) the Specification.

[*] The 'Joint Initiative pan-European Mobile P2P Interoperability' brings together participants of the Berlin Group, infrastructure providers and participants from principle Mobile P2P scheme services in Europe. In January 2016, the participants to the Joint Initiative have published a Technical Feasibility Study on pan-European Mobile P2P Interoperability which can be downloaded from the Berlin Group website (http://www.berlin-group.org/mobile-p2p-interoperability).

Contents

1 Introduction

Background

A Mobile P2P Scheme is a solution where participants can transfer funds mostly in real-time or near real-time using there smart phones and mobile phone data as account proxy information. The underlying accounts can be bank accounts or any other form of accounts for electronic money. The Mobile P2P Scheme consists of a bundle of contracts and operational and technical rules as well as further added value services like payment requests or collecting funds as a group of members.

The Mobile P2P Scheme can be a scheme with a dedicated mobile app and dedicated contracts or can just be a payment function within a bank's generic mobile banking app. The contracts cited above are then part of the general customer contract with the bank. For the sake of simplicity, all these solutions are named as 'Mobile P2P Scheme' in this document and in the Framework documents referenced in section 6.

In Europe many of these solutions have been developed with the rise of smart phone usage. These solutions are today not interoperable, i.e. a participant of Scheme A cannot interact with a participant of Scheme B.

Mobile P2P Interoperability Framework

The Mobile P2P Interoperability Framework as defined by a Joint Initiative of the Berlin Group, infrastructure providers and participants from principle European Mobile P2P scheme services (hereafter: Joint Initiative) is a Framework for the European area for connecting Mobile P2P Schemes. This Framework is independent of the corresponding Mobile P2P Schemes and enables consumers to perform Mobile P2P transactions between each other in a situation where the consumers are participants of different Mobile P2P Schemes.

This Framework relies on the SCT INST infrastructure which is expected to be piloted in early 2018. Clearing accounts of the Mobile P2P Schemes should at least be reachable for SCT INST – the Framework does not require the participants accounts to be reachable.

There is also a variant using the SCT infrastructure for the period of migration of the banking industry towards SCT INST. If SCT is used, additional business agreements between the corresponding Mobile P2P Schemes might be needed dealing with the topic of a payment guarantee for the end-of-day batch processing after having initiated the underlying SCT payment successfully.

The Mobile P2P Interoperability Framework defines operational rules and interfaces for the Proxy Lookup Service, Clearing/Settlement of funds transfer and an optional Payment Notification on

Application Level within the scenario of direct booking to the Beneficiary Account or where SCT is used on the Clearing & Settlement Level.

Operational Rules

The complementary document [MP2P OR] of the Mobile P2P Interoperability Framework contains the definition of the roles within the framework, the operational rules and the abstract data model. The data model is a compilation of abstract message definitions for the repository level, clearing and settlement level and application level. Data attributes (AT-NN) are defined in the operational rules for the data model.

Aim and Structure of the Document

The aim of this document is to provide detailed message definitions and examples for repository level, clearing and settlement level and application level. The data attributes of the operational rules are referenced in the message definitions.

Section 2 of this document contains information on notation conventions and message format structures. Section 3 contains the schema definitions and message examples in XML and JSON representation for the repository look-up. Section 4 covers the definitions of the clearing and settlement level. Section 5 contains the definitions of the application level. The document then ends with a list of reference documents in Section 6.

Document History

Version	Change/Note	Approved
0.99	Market consultation version	03/02/2017
1.0	Results of market consultation acknowledged	09/06/2017
1.01	Adjusted to Creative Commons license 'BY ND'	31/08/2018
1.1	Change Requests from EPC resulting from the 2019 market consultation related to the EPC SPL Scheme. Major impact is • Introduction of Creation Date Time attributes also in proxy lookup response messages • Introduction of email as potential proxy type • Introduction of Non Euro currencies in proxy lookup messages	20/03/2020

Version	Change/Note	Approved
1.2	Change Requests from the EPC SPL preferred proxy provider: • Adopt the length of alias identification from Max16Text to Max140Text to allow also longer email aliases (Erratum). • The MP2P Receiver Scheme identification is not any more part of body encoding, but is solely addressed through the host domain specification. The dedicated path parameter has been taken out from the call definitions. Errata on the XML based version, resulting from changes in Version 1.1., which have not been fully applied yet.	06 November 2020 by MP2P Taskforce

2 Notation and Formats

2.1 Character Set

The following character set rules apply:

- In analogy to the UNIFI (ISO 20022), the XML and JSON messages used in this specification allow for the full range of global language requirements (UTF-8)
- Banks must be able to support the Latin character set commonly used in international communication, as follows:

  a b c d e f g h i j k l m n o p q r s t u v w x y z

  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

  0 1 2 3 4 5 6 7 8 9

  / - ? : ( ) . , ' +

  Space

However, there may be bilateral or multilateral agreements to support one or more sets of characters beyond the Latin character set referred to above. These rules only apply to message elements containing text (free text), i.e. for elements within remittance information and name and address elements. In all other fields, only the Latin character set mentioned above may be used.

2.2 Clearing and Settlement Level Message Specification Formats

This document relies on the ISO 20022 Message Definition Reports and EPC SCT INST documentation for the clearing related messages, which should be read in conjunction with these documents. The following specification format is used for the message definitions:

Mult	Message Element	MP2P Requirements
[1..1]	+ Transaction Information	
[1..1]	++ Payment Information Identification	
	++ Message Element that is not part of the Berlin Group Message	
[0..1]	++ Message Element that is part of the Berlin Group Message	Mandatory

Mult

This defines the multiplicity (i.e. occurrence) of the field presence, following the EPC Interbank format.

Message Element

Name as defined by ISO 20022. In addition, the structural depth of the Message Element is given by the number of "+" signs in front.

MP2P Requirements

The Mobile P2P Interoperability Framework distinguishes two occurrence definitions (colours of fields):

- White: This element is not used. It may only be used after bilateral agreement including the agreement of the relevant CSM infrastructure.
- Yellow: This is an element which is required to be supported. The Berlin Group then defines in this column additional format and usage rules for the element.

2.3 Repository and Application Level Message Specification Formats

2.3.1 XML Based Encoding

The following specification format is used for the XML message definitions of Repository and Application Level:

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[1..1]	+ Alias	<Als>		Currently only a mobile number or an email address in the form username@domainname is allowed as alias type.
[1..1]	++ Type	<Tp>	CodeSet	MSDN, EMAI
[1..1]	++ Identification	<Id>	Max140Text	AT-01 MSISDN or email address of the Beneficiary

Mult

This defines the multiplicity (i.e. occurrence) of the field presence, following the EPC Interbank format.

Message Element

Name is defined by this specification, where possible in analogy to ISO 20022. In addition, the structural depth of the Message Element is given by the number of "+" signs in front.

XML-Tag

Defines the XML tag, where possible in analogy to ISO 20022.

Type

Defines the type of the field, where possible in analogy to ISO 20022.

Mobile P2P Requirements

Defines the content of the field and the specific usage rules.

2.3.2 JSON Based Encoding

The following specification format is used for the JSON message definitions of Repository and Application Level:

Mandatory	Message Element	Tag	Type	Mobile P2P Requirements
yes	Alias	Als	AliasType	Currently only a mobile number or an email address in the form username@domainname is allowed as alias type.
yes	Originator Scheme	OrgSch	SchemeType	AT-02

Mandatory

Defines whether or not a field is mandatory.

Message Element

Name is defined by this specification, where possible in analogy to ISO 20022.

Tag and Type

Defines the **tag** identifier to be used in the JSON messages and defines the **type** of the field.

For composed data fields, the subfields contained within the given type are defined in a separate table.

Mobile P2P Requirements

Defines the content of the field and the specific usage rules.

3 Repository Level

The repository look-up messages are exchanged as online messages between a requesting party and a responding party. This scenario can be technically implemented as a client-server architecture. Two commonly used methods for data exchange in client-server systems are XML-based SOAP Web services and JSON-based REST services. Pros and cons for each method are discussed in chapter 3.1, especially with respect to security levels.

Chapters 3.3 and 3.4 define the request and response formats and provide example messages for the JSON and XML data representation, respectively. Both formats, XML and JSON, are identical in terms of content, but are slightly different in their technical representation of this content.

3.1 XML and JSON

Depending on the intended application of the Web service, XML and JSON each have advantages and disadvantages.

3.1.1 Security levels

In order to avoid security issues during data exchange, different kind of security measures can be implemented. End-to-end encryption is not supported by JSON REST services but is available for XML SOAP services. However, for the repository look-up, point-to-point encryption should be sufficient. 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.

Data exchange via internet shall be performed using virtual private networks (VPN) by using client certificates on transport level. Details will be defined bilaterally between Mobile P2P schemes.

Remark: The Berlin Group is working on a PSD2 Interoperability Framework. It is intended to re-use the infrastructure also for Mobile P2P Interoperability related services, i.e. to re-use the e-IDAS certificate approach also to secure the Repository Look-up. This adaption will be dealt with in a later release of the Framework.

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

In case of JSON encoding, Repository 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.

3.1.2 Miscellaneous criteria

Some other criteria should be considered before deciding to use either XML or JSON Web services such as performance, resource consumption, maintainability and ease of implementation.

A JSON-based REST-service will have higher performance, lower resource consumption (e.g. memory and cpu) and is easier to implement than an XML-based SOAP-service. On the other hand, a formal validation of request and response message is possible in XML via XSD validation. Validation for JSON needs to be implemented explicitly in all processing systems. This poses a larger risk for implementation errors.

Maintainability is more complex in the case of XML SOAP because XSDs and clients always need to be updated. In the case of JSON REST, attributes can be added to the interface without changing the client system.

3.1.3 Summary and Decision

The following table summarises the pros and cons of using XML- and JSON-based Web services.

	XML	**JSON**
point-to-point encryption	+	+
end-to-end encryption	+	-
performance and resources	o	+
maintainability	o	+
simple implementation	o	+
formal validation	+	-

Remark: Also the coding technology to be chosen will be harmonised with the upcoming Berlin Group PSD2 Interoperability Framework.

Decision:

It was decided to support a REST service approach only and go with priority to a JSON encoding of https body data. However, an XML encoding should still be considered within https body encoding as a second option till first feedback from market implementations.

3.2 Guiding Principles

3.2.1 Transport of Message Parameters

The Mobile P2P Interoperability Framework follows the REST service approach. This approach allows to transport message parameters at different levels:

- message parameters as part of the https level (https header)
- message parameters by defining the resource path (URL path information) and
- message parameters as part of the https body.

The content parameters will be encoded either in JSON or in XML syntax (XML syntax only as a second option for time being).

The following principle is applied when defining the API:

Message parameters as part of the https header:

- Definition of the content syntax

Message parameters as part of the path level:

- All data addressing a resource:
  - Receiver Mobile P2P Scheme identification (AT- 03),
  - Version of the interface
  - Service identification (Repository Look-Up or Application Level)

Message parameters as part of the https body:

- Business data content.

3.2.2 Mobile P2P Interoperability Interface API Structure

The MP2P Interoperability Interface is resource oriented. Resources to be addressed are

https://{provider}/v1/{resource}

using additional content parameters {parameters}

where

- {provider} is the host and path of the Receiver MP2P Scheme interface, providing the Repository Look-up service and a Payment Notification service respectively. The notion of this is not further mentioned throughout this document. In cases where the Receiver Scheme is not determined yet, the provider may stand for a central SPL service interface.
- v1 is denoting the first version of the interface
- {resource} has the values look_up, reachability_check and payment_notification
- {parameters} are content attributes defined in the following in an JSON or XML encoding

The structure of the request/response is described in the following in the categories

- Path: Attributes encoded in the Path, e.g. service related endpoint information
- Header: Attributes encoded in the https header
- Request: Attributes within the content parameter set of the request
- Response: Attributes within the content parameter set of the response.
- Response Code (https)

3.3 JSON Based Encoding

JSON message definitions are provided in Section 3.3.1. Examples for detailed XML messages are given in Section 3.3.2. The data attribute definitions of [MP2P OR] are referenced in the following tables. Some data fields are composed of multiple subfields. These composed data types are defined in separate tables further below.

3.3.1 Repository Look-Up

Call

POST /v1/look_up

Creates a Repository Look-up.

Path

No specific path parameter.

Header

Content Type: JSON

Request

Attribute	Tag	Type	Condition	Description
Transaction Identification	TxId	Max35Text	M	AT-05 Look-up Reference Data *Usage Rule:* • Maximum of 35 characters; no blanks are allowed • The first four characters uniquely identify the Originator Scheme. The fifth character is a minus sign. • The reference to the request in a transaction life cycle is unique per Originator Scheme and transaction.
Creation Date Time	CreDtTm	ISODateTime	M	AT-06 Timestamp of the processing time of the look-up request.
Alias Beneficiary	AlsBfy	AliasType	M	AT-01 Currently only a mobile number or an email address in the form

Attribute	Tag	Type	Condition	Description
				username@domainname is allowed as alias type.
Alias Originator	AlsOrig	AliasType	O	AT-13
Originator Scheme	OrigSch	SchemeType	M	AT-02
Transaction Amount	TxAmt	AmountType	O	AT-04 Amount: This amount might be used for risk management issues in a pre-validation. Default Currency: EUR Other currencies than Euro are allowed only after confirmation by the receiver of the message.

Response

Attribute	Tag	Type	Condition	Description
Transaction Identification	TxId	Max35Text	M	AT-05 Echo of the reference data from the request
Creation Date Time	CreDtTm	ISODateTime	M	AT-06 Timestamp of the processing time of the look-up response.
Response	Resp	ResponseType	M	AT-08 and AT-09
Originator Scheme	OrigSch	SchemeType, see Sect. 3.3.5	M	AT-02 Echo Originator Scheme of request message

Attribute	Tag	Type	Condition	Description
Receiver Scheme	RecSch	SchemeType, see Sect. 3.3.5	O	AT-03
Creditor Account	CdtrAcct	CreditorAccountType	Conditional	AT-10 and potentially AT-11 contained only in case of positive response Account data to be used for the inter Mobile-P2P scheme funds transfer. As type only "IBAN" is admitted.
Beneficiary Name	BfyNm	Max140Text	O	AT-12 contained only in case of positive response, even then it is optional In this field the legal name of the Beneficiary can be provided, dependent on data protection requirements of the Receiver Scheme. Usage Rule: 'Creditor Name' is limited to 70 characters in length.
Payment Notification Path	PmtNtfcPath	string	Conditional	AT-14 This data element is contained only if the Receiver MP2P Scheme is requiring a payment notification. In this case, this data element contains the Path to be used to post the payment notification.
Preference Indicator	PrfInd	ISODateTime	Optional	AT-15 *Usage Rule*: May only be used in positive responses, where an IBAN is contained. Is then optional.
Registration Timestamp	RegDtTm	ISODateTime	Conditional	AT-16

Attribute	Tag	Type	Condition	Description
				Usage Rule: Is only present in positive responses, where an IBAN is contained. In this case, it is mandated. It then contains the date and time when the Beneficiary has registered its account number with the Receiver Scheme.

Return Codes

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

3.3.2 Examples Repository Look-Up

Call with MSISDN Proxy

POST https://bizum.es/Interoperability/v1/look_up

```
{
   "TxId": "JFFY-20160606193626-000000001",
   "CreDtTm": "2016-06-06T19:36:26",
   "AlsBfy": {
     "Tp": "MSDN",
     "Id": "+341516024488"
   },
   "AlsOrig": {
     "Tp": "MSDN",
     "Id": "+391073044700"
   },
   "OrigSch": {
     "Nm": "JIFFY MP2P Scheme",
     "OrgId": “JIFFY”
   },
   "TxAmt": {
     "Amt": "22.00",
     "Ccy": "EUR"
   }
}
```

Call with Email Proxy

POST https://bizum.es/Interoperability/v1/look_up


```
{
   "TxId": "JFFY-20160606193626-000000001",
   "CreDtTm": "2016-06-06T19:36:26",
   "AlsBfy": {
     "Tp": "EMAI",
     "Id": "payeename@test-server.org"
   },
   "AlsOrig": {
     "Tp": "EMAI",
     "Id": "payername@test-server.org"
   },
   "OrigSch": {
     "Nm": "JIFFY MP2P Scheme",
     "OrgId": “JIFFY”
   },
   "TxAmt": {
     "Amt": "22.00",
     "Ccy": "EUR"
   }
}
```


Remark: This example is not presuming that Jiffy or Bizum actually support email as proxy type.

Positive Response

In the following example, the funds are cleared to the account of the Beneficiary.

HTTPS response code: 200.

The response body is:


```
{
   "TxId": "JFFY-20160606193626-000000001",
   "CreDtTm": "2016-06-06T19:36:27",
   "Resp": {
      "Rslt" : true
   },
   "OrigSch" :{
```

```
    "Nm": "JIFFY MP2P Scheme",
    "OrgId": "JIFFY"
  },
  "CdtrAcct": {
    "IBAN": "ES9910000000100000001234"
  },
  "BfyNm": "Pepe Lopez",
  "PmtNtfcPath": "v1/payment_notification/JFFY-20160606193626-000000001-99981",
  "PrfInd": "2016-02-20T20:45:03",
  "RegDtTm": "2016-02-20T19:15:03"
}
```


Negative Response (Alias not known)

HTTPS Response Code : 200


```
{
  "TxId": "JFFY-20160606193626-000000001",
  "CreDtTm": "2016-06-06T19:36:276",
  "Resp": {
    "Rslt": false,
    "RsltDtls": "NMMD"
  },
  "OrigSch": {
    "Nm": "JIFFY MP2P Scheme",
    "OrgId": "JIFFY"
  }
}
```


3.3.3 Reachability Check

This optional call checks the availability of the alias in a potential Receiver Mobile P2P Scheme.

Call

POST /v1/reachability_check

Path

No specific path parameter.

Header

Content Type: JSON

Request

Attribute	Tag	Type	Condition	Description
Transaction Identification	TxId	Max35Text	M	AT-05 Look-up Reference Data *Usage Rule:* • Maximum of 35 characters; no blanks are allowed • The first four characters uniquely identify the Originator Scheme. The fifth character is a minus sign. • The reference to the request in a transaction life cycle is unique per Originator Scheme and transaction.
Creation Date Time	CreDtTm	ISODateTime	M	AT-06 Timestamp of the processing time of the reachability check request.
Alias Beneficiary	AlsBfy	AliasType	M	AT-01 Currently only a mobile number or an email address in the form username@domainname is allowed as alias type.
Alias Originator	AlsOrig	AliasType	O	AT-13
Originator Scheme	OrigSch	SchemeType	M	AT-02

Response

Attribute	Tag	Type	Condition	Description
Transaction Identification	TxId	Max35Text	M	AT-05 Echo of the reference data from the request
Creation Date Time	CreDtTm	ISODateTime	M	AT-06 Timestamp of the processing time of the reachability check response.
Response	Resp	ResponseType	M	AT-08 and AT-09
Originator Scheme	OrigSch	SchemeType, see Sect. 3.3.5	M	AT-02 Echo Originator Scheme of request message
Receiver Scheme	RecSch	SchemeType, see Sect. 3.3.5	O	AT-03

Return Codes

Status Code	Message Code	Description
200		Transaction was correct, no Payment Advice required, IBAN might be contained or not
400 (Bad Request)		Validation error occurred or service not available.
401 (Unauthorized)	CERTIFICATE_NOT_VALID	
403 (Forbidden)	MP2P_NOT_ADMITTED	Initiating Party is not admitted to the system

3.3.4 Examples Reachability Check

Call with MSISDN proxy

POST https://bizum.es/Interoperability/v1/reachability_check

```
{
   "TxId": "JFFY-20160606193626-000000001",
   "CreDtTm": "2016-06-06T19:36:26",
   "AlsBfy": {
     "Tp": "MSDN",
     "Id": "+341516024488"
   },
   "AlsOrig": {
     "Tp": "MSDN",
     "Id": "+391073044700"
   },
   "OrigSch": {
     "Nm": "JIFFY MP2P Scheme",
     "OrgId": “JIFFY”
   }
}
```

Call with Email proxy

POST https://bizum.es/Interoperability/v1/reachability_check

```
{
   "TxId": "JFFY-20160606193626-000000001",
   "CreDtTm": "2016-06-06T19:36:26",
   "AlsBfy": {
     "Tp": "EMAI",
     "Id": "payeename@test-server.org"
    },
   "AlsOrig": {
     "Tp": "EMAI",
     "Id": "payername@test-server.org"
     },
   "OrigSch": {
     "Nm": "JIFFY MP2P Scheme",
     "OrgId": “JIFFY”
   }
}
```

Remark: This example is not presuming that Jiffy or Bizum actually support email as proxy type.

Positive Response

HTTPS response code: 200,
The response body then is:

```
{
   "TxId": "JFFY-20160606193626-000000001",
   "CreDtTm": "2016-06-06T19:36:27",
   "Resp": {
      "Rslt": true
   },
   "OrigSch : {
     "Nm": "JIFFY MP2P Scheme",
     "OrgId": "JIFFY"
   }
}
```

Negative Response (Alias not known)

HTTPS response code : 200

The response body then is:

```
{
   "TxId": "JFFY-20160606193626-000000001",
    "CreDtTm": "2016-06-06T19:36:276",
    "Resp": {
      "Rslt": false,
      "RsltDtls": "NMMD"
   }
   "OrigSch" : {
     "Nm": "JIFFY MP2P Scheme",
     "OrgId": "JIFFY"
   }
}
```

3.3.5 Complex Data Types

3.3.5.1 AliasType

Mandatory	Message Element	Tag	Type	Mobile P2P Requirements
yes	Type	Tp	CodeSet	permitted codes: MSDN, EMAI
yes	Identification	Id	Max140Text	AT-01 MSISDN or email address

3.3.5.2 AmountType

If the Transaction Amount field is present in the message, both subfields Amount and Currency are mandatory.

Mandatory	Message Element	Tag	Type	Mobile P2P Requirements
yes	Amount	Amt	Amount	Transaction amount with a maximum of 18 digits including 5 fraction digits
yes	Currency	Ccy	CodeSet	Alphabetic currency code compliant with ISO 4217 *Usage Rule: Only 'EUR' allowed.*

3.3.5.3 SchemeType

Manda-tory	Message Element	Tag	Type	Mobile P2P Requirements
yes	Name	Nm	Max70Text	Name of the Originator or Receiver MP2P Scheme *Usage Rule*: 'Name' is limited to 70 characters in length.
yes	Organisation Identification	OrgId	Max35Text	Unique and unambiguous identification of the Originator or Receiver Scheme

3.3.5.4 CreditorAccountType

Manda-tory	Message Element	Tag	Type	Mobile P2P Requirements
no	Scheme Account	SchAcct	Boolean	AT-11 Creditor Account Type Indicator: It has to be contained if the Credit Account does not equal the Beneficiary Account. Then, it contains the value: true
yes	IBAN	IBAN	IBAN2007Identifier	

3.3.5.5 ResponseType

Manda-tory	Message Element	Tag	Type	Mobile P2P Requirements
yes	Result	Rslt	Boolean	AT-08 true/false Indicates whether or not the requested alias could be matched to account data.
no	Result Details	RsltDtls	ResultCodes	AT-09 Not present in positive responses, optional in negative responses. See Section 3.3.5.6 for permitted codes.

3.3.5.6 ResultCodes (Reason codes AT-09)

List of allowed reason codes AT-09 to decline a request. These codes are independent of the data encoding (XML or JSON).

- 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

3.4 XML Based Encoding

The XML based encoding is defined as fall-back only. The optional reachability check service is not supported in XML encoding. In the following, XML body definitions are provided in Section 3.4.1. Examples for detailed XML messages are given in Section 3.4.2. All other definitions referring to https calls will be defined as described in Sections 3.2 and 3.3.

3.4.1 Schema definitions

The following tables contain the body definitions for the repository look-up request and response for the XML data representation. Where possible, message elements and data types were chosen in analogy to ISO 20022 definitions. The data attribute definitions of [MP2P OR] are referenced in the following tables.

Repository Look-up Request

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[1..1]	+ Message Root	<MP2PLkupReq>		
[1..1]	+ Transaction Identification	<TxId>	Max35Text	AT-05 Look-up Reference Data *Usage Rule:* • Maximum of 35 characters; no blanks are allowed. • The first four characters uniquely identify the Originator Scheme. The fifth character is a minus sign. The reference to the request in a transaction life cycle is unique per Originator Scheme and transaction.
[1..1]	+ Creation Date Time	<CreDtTm>	ISODateTime	AT-06 Timestamp of the processing time of the look-up request.
[1..1]	+ Alias Beneficiary	<AlsBfy>		Currently only a mobile number or an email address in the form username@domainname is allowed as alias type.
[1..1]	++ Type	<Tp>	CodeSet	MSDN, EMAI
[1..1]	++ Identification	<Id>	Max140Text	AT-01 MSISDN or email address of the Beneficiary

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[0..1]	+ Alias Originator	<AlsOrig>		Currently only a mobile number or an email address in the form username@domainname is allowed as alias type.
[1..1]	++ Type	<Tp>	CodeSet	MSDN, EMAI
[1..1]	++ Identification	<Id>	Max140Text	AT-13 MSISDN or email address of the Originator
[1..1]	+ Originator Scheme	<OrigSch>	Party-Identification32	AT-02
[1..1]	++ Name	<Nm>	Max70Text	Name of the Originator MP2P Scheme *Usage Rule*: 'Name' is limited to 70 characters in length.
[1..1]	++ Identification	<Id>	Party6Choice	
[1..1]	+++ Organisation Identification	<OrgId>	Organisation-Identification4	
[1..1]	++++ Other	<Othr>	Generic-Organisation-Identification1	
[1..1]	+++++ Identification	<Id>	Max35Text	Unique and unambiguous identification of the Originator Scheme

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[0..1]	+ Transaction Amount	<TxAmt>	CurrencyAndAmount	AT-04 Amount: This amount might be used for risk management issues in a pre-validation. Default Currency: EUR Other currencies than Euro are allowed only after confirmation by the receiver of the message. The currency is represented as an XML attribute 'Ccy'.

Repository Look-up Response

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[1..1]	+ Message Root	<MobP2PLkupResp>		
[1..1]	+ Transaction Identification	<TxId>	Max35Text	AT-05 Echo of the reference data from the request
[1..1]	+ Creation Date Time	<CreDtTm>	ISODateTime	AT-06 Timestamp of the processing time of the look-up response.
[1..1]	+ Response	<Resp>		
[1..1]	++ Result	<Rslt>	Boolean	AT-08 true/false Indicates whether or not the requested alias could be matched to account data.

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[0..1]	++ Result Details	<RsltDtls>	CodeSet	AT-09 Not present in positive responses, optional in negative responses
[1..1]	+ Originator Scheme	<OrigSch>	Party-Identification32	AT-02 Echo Originator Scheme of request message
[0..1]	+ Receiver Scheme	<RecSch>	Party-Identification32	AT-03
[0..1]	+ Creditor Account	<CdtrAcct>	CashAccount16	contained only in case of positive response
[0..1]	++ Scheme Account	<SchAcct>	Boolean	AT-11 Creditor Account Type Indicator: It has to be contained if the Credit Account does not equal the Beneficiary Account. Then, it contains the value: true
[1..1]	++ Identification	<Id>	AccountIdentification4Choice	AT-10 Account data to be used for the inter Mobile-P2P scheme funds transfer. As type only "IBAN" is admitted.
[1..1]	+++ IBAN	<IBAN>	IBAN2007Identifier	

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[0..1]	+ Name Beneficiary	<BfyNm>	Max 70Text	AT-12 contained only in case of positive response, even then it is optional In this field the legal name of the Beneficiary can be provided, dependent on data protection requirements of the Receiver Scheme. Usage Rule: 'Creditor Name' is limited to 70 characters in length.
[0..1]	+ Payment Notification Path	<PmtNtfcPth>	Max 140 Text	A hyperlink where to post a payment notification. This path might be present only in case of a positive response.
[0..1]	+ Preference Indicator	<PrfInd>	ISODateTime	Optional *Usage Rule:* May only be present in positive responses. If present, indicates that and when the Beneficiary has chosen (the app of) the Receiver Scheme as preference for receiving funds via MP2P.

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[0..1]	+ Registration Timestamp	<RegDtTm>	ISODateTime	Optional *Usage Rule:* May only be present in positive responses. If present, contains the date and time when the Beneficiary has registered its account number with the Receiver Scheme.

3.4.2 Examples

In this example, a Mobile P2P repository look-up request and a positive and negative response message are shown in XML data representation. The look-up request is sent from the Originator Scheme “JIFFY” to the Receiver MP2P Scheme "Bizum". The beneficiary is called Pepe Lopez, who is a customer of the Receiver MP2P Scheme “Bizum”.

Where possible, the tag structure and names were chosen in analogy to ISO 20022.

3.4.2.1 Request

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <xsi:MP2PLkupReq>
  <TxId>JFFY-20160606193626-000000001</TxId>
  <CreDtTm>2016-06-06T19:36:26</CreDtTm>
  <AlsBfy>
    <Tp>MSDN</Tp>
   <Id>+341516024488</Id>
  </AlsBfy>
  <AlsOrig>
    <Tp>MSDN</Tp>
   <Id>+391073044700</Id>
  </AlsOrig>
  <OrigSch>
   <Nm>JIFFY MP2P Scheme</Nm>
   <Id><OrgId><Othr><Id>JIFFY</Id></Othr></OrgId></Id>
  </OrigSch>
  <TxAmt Ccy="EUR">22.00</TxAmt>
```

```
  </MP2PLkupReq>
</Document>
```

3.4.2.2 Positive response

In the following example, the funds are cleared to the account of the Receiver Scheme.

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <xsi:MP2PLkupResp>
    <TxId>JFFY-20160606193626-000000001</TxId>
    <CreDtTm>2016-06-06T19:36:28</CreDtTm>
    <Resp>
      <Rslt>true</Rslt>
    </Resp>
    <OrigSch>
      <Nm>JIFFY MP2P Scheme</Nm>
      <Id><OrigId><Othr><Id>JIFFY</Id></Othr></OrgId></Id>
    </OrigSch>
   <CdtrAcct>
      <SchAcct>true</SchAcct>
      <Id><IBAN>ES9981000000010000000012345</IBAN></Id>
    </CdtrAcct> </CdtrAcct>
    <BfyNm>Pepe Lopez</BfyNm>
    <PmtNtfcPth> v1/payment_notification/JFFY-20160606193626-000000001-
99981</PmtNtfcPth>
    <PrfInd>2016-02-20T20:45:03</PrfInd>
    <RegDtTm>2016-01-11T13:10:08</RegDtTm>
  </MP2PLkupResp>
</Document>
```

3.4.2.3 Negative response

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <xsi:MP2PLkupResp>
    <TxId>JFFY-20160606193626-000000001</TxId>
    <CreDtTm>2016-06-06T19:36:28</CreDtTm>
    <Resp>
      <Rslt>false</Rslt>
      <RsltDtls>SYUA</RsltDtls>
    </Resp>
    <OrigSch>
```

```
      <Nm>JIFFY MP2P Scheme</Nm>
      <Id><OrgId><Othr><Id>JIFFY</Id></Othr></OrgId></Id>
    </OrigSch>
  </MP2PLkupResp>
</Document>
```

4 Clearing and Settlement Level

4.1 SCT INST solution

Clearing of Mobile P2P transactions in the context of this Interoperability Framework relies on the SCT INST clearing messages based on ISO 20022.

The settlement of the transaction is performed following the requirements in [EPC INRB]. There are no specific requirements by the Mobile P2P Interoperability Framework for the settlement.

4.1.1 Use of the FI to FI Customer Credit Transfer (pacs.008.01.02)

This message is used to transport the Mobile P2P Credit Transfer instruction from the Debtor Bank to the Creditor Bank, directly or through intermediaries. It is an SCT INST message as specified in [EPC INIG] with a specific purpose code, indicating a mobile P2P based message, and other Mobile P2P specific requirements.

The message caters for single credit transfer instructions only.

The following section describes the specific Mobile P2P Requirements for the SCT INST pacs.008.01.02 message format.

4.1.2 Group Header

In the group header the MP2P requirements are as follows:

- **<Payment Type Information>.<Category Purpose>**

  Optional

  Usage Rule: Depending on the agreement between the Originator and the Originator Bank, 'Category Purpose' may be forwarded to the Beneficiary Bank.

  Usage Rule: Only "MIOP" is allowed.

4.1.3 Credit Transfer Transaction Information

In the credit transfer transaction information block of the pacs-message, the MP2P requirements are as follows:

- **<Payment Identification>.<End to End Identification>**

Originator's Reference to the Credit Transfer (AT–05 Look-up Request Reference Data of the underlying MP2P transaction)

Usage Rule: This customer reference must be passed on in the end-to-end chain and is binding the clearing transaction to the Lookup-Request. If this field is not addressable by the Payment Initiator, this reference will be transported within the Remittance Information.

- **<Payment Type Information>.<Category Purpose>**

  See Section 4.1.2. Payment Type Information must be present either in the Group Header or in the Credit Transfer Transaction Information.

- **<Debtor Account>**

  Mandatory

- **<Debtor>.<Name>**

  Mandatory

  Usage Rule: Name of the Originator Mobile P2P Scheme, if the credit transfer is initiated on an account of the Mobile P2P Scheme, otherwise the Originator of the Mobile P2P transaction.

  Usage Rule: 'Name' is limited to 70 characters in length.

- **<Debtor>.<Identification>.<Private Identification>.<Other>.<Id>**

  Optional

  Alias (MSISDN) of the Originator (AT-13).

- **<Creditor>.<Name>**

  Mandatory

  Always contains the name of the Beneficiary (AT-12).

  Usage Rule: 'Name' is limited to 70 characters in length.

- **<Creditor>.<Identification>.<Private Identification>.<Other>.<Id>**

  Optional

  Alias (MSISDN) of the Beneficiary (AT-01).

- **<Creditor Account>**

  Mandatory

  Creditor Account from the Repository Look-up Response (AT-10).

- **<Purpose>.<Code>**

  Usage Rule: Only "MP2P" is allowed.

- **<Remittance Information>**

  This field is only used, when Creditor ID, Debtor ID or End-to-End-ID is not addressable by the Sending Scheme or if there is a remittance text from the Originator and no payment notification advice is used on application level.

  The Remittance Information is encoded following the EACT standard of the Association of European Treasurers on structuring the unstructured remittance information, by extending this standard by one tag "/DNR/" for Debtor Number.

  The following tags will be used

  /DNR/ for the alias of the Originator.
  /CNR/ for the alias of the Beneficiary.
  /DOC/ for the Reference Data of the corresponding Look-Up Request.
  /TXT/ for optional remittance text.

4.1.4 SCT INST Examples

Example Clearing Account to Private Account

In the following example, a Mobile P2P transaction is cleared between the clearing account of the Originator Scheme “JIFFY” and the private customer account of the Beneficiary Pepe Lopez, who is a customer of the Receiver MP2P Scheme “Bizum”. The originator is called Mario Rossi.

Remark: The rules of using the Clearing and Settlement Layer do not differentiate for the different account models. The Creditor Name is always the Name of the Beneficiary even if the receiving account is a clearing account of the Receiver Scheme.

<?xml version="1.0" encoding="UTF-8"?>

```
<Document xsi:schemaLocation="urn:iso:std:iso:20022:tech:xsd:sct:pacs.008.001.02
pacs.008.001.02.xsd" xmlns="urn:iso:std:iso:20022:tech:xsd:sct:pacs.008.001.02"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <FIToFICstmrCdtTrf>
    <GrpHdr>
      <MsgId>NBAGDE30XXXICF2015071300000004</MsgId>
      <CreDtTm>2016-06-06T19:36:36</CreDtTm>
      <NbOfTxs>1</NbOfTxs>
      <TtlIntrBkSttlmAmt Ccy="EUR">22.00</TtlIntrBkSttlmAmt>
      <IntrBkSttlmDt>2016-06-06</IntrBkSttlmDt>
      <SttlmInf>
        <SttlmMtd>CLRG</SttlmMtd>
        <ClrSys><Prtry>SCL</Prtry></ClrSys>
      </SttlmInf>
      <InstdAgt><FinInstnId><BIC>CreditorBankBIC</BIC></FinInstnId></InstdAgt>
    </GrpHdr>
    <CdtTrfTxInf>
      <PmtId>
        <EndToEndId>JFFY-20160606193625123456</EndToEndId>
        <TxId>NBAGDE3EXXX20150713282710023306096</TxId>
      </PmtId>
      <PmtTpInf>
        <SvcLvl><Cd>SEPA</Cd></SvcLvl>
        <LclInstrm><Cd>INST</Cd></LclInstrm>
        <CtgyPurp><Cd>MIOP</Cd></CtgyPurp>
      </PmtTpInf>
      <IntrBkSttlmAmt Ccy="EUR">22.00</IntrBkSttlmAmt>
      <ChrgBr>SLEV</ChrgBr>
      <InstgAgt><FinInstnId><BIC>DebtorBankBIC</BIC></FinInstnId></InstgAgt>
      <Dbtr>
        <Nm>JIFFY MP2P Scheme</Nm>
        <Id><Prvtd><Othr><Id>+391073044700</Id></Othr></PrvtId></Id>
      </Dbtr>
      <DbtrAcct><Id><IBAN>IT92Y360200300001112430</IBAN></Id></DbtrAcct>
      <DbtrAgt><FinInstnId><BIC>DebtorBankBIC</BIC></FinInstnId></DbtrAgt>
      <CdtrAgt><FinInstnId><BIC>CreditorBankBIC</BIC></FinInstnId></CdtrAgt>
      <Cdtr>
        <Nm>Pepe Lopez</Nm>
        <Id><PrvtId><Othr><Id>+3411112345678</Id></Othr></PrvtId></Id>
      </Cdtr>
      <CdtrAcct><Id><IBAN>ES9910000000100000001234</IBAN></Id></CdtrAcct>
      <Purp><Cd>MP2P</Cd></Purp>
```


```
    </CdtTrfTxInf>
  </FIToFICstmrCdtTrf>
</Document>
```

Example for Encoding the Remittance Information

In the following, some examples are given for using the remittance information field as a fall-back.

Example 1: No Payment Notification Advice is sent:

```
<RmtInf><Ustrd>/TXT/Greetings from Milano</Ustrd></RmtInf>
```

Example 2: The Debtor ID and Debtor ID field cannot be addressed by the Sending Scheme:

```
<RmtInf><Ustrd>/DNR/>+391073044700/CNR/+3411112345678</Ustrd></RmtInf>
```

Example 3: The End-to-End-Id cannot be addressed and no Payment Notification Advice is sent.

```
<RmtInf><Ustrd>/DOC/JFFY-20160606193625123456/TXT/Greetings from
Milano</Ustrd></RmtInf>
```

4.1.5 Usage of the Confirmation Message and Recall Function

In [EPC INIG], requirements on the definition of the payment status report and recall message related to an SCT INST message are defined. These requirements rely on the whole message flow starting with a specific SCT INST message.

There are no further requirements on these message definitions by the Mobile P2P Interoperability Framework.

4.2 Pre SCT INST solution

The specific Mobile P2P requirements for the usage of SCT INST as detailed in Section 4.1.3 apply also in a solution where SCT is used as clearing and settlement mechanism. This applies especially for the usage of the following SCT message fields:

- End-to-End Identification
- Debtor Name
- Debtor-ID

- Creditor Name
- Creditor-ID
- Category Purpose Code
- Purpose Code
- Remittance Information.

In addition, the following differences have to be taken into account:

- The Payment Notification Advice is mandatory
- The Local Instrument is not used for SCT within this specification whereas it is mandatory in SCT INST with fixed value "INST"
- Set Clearing and Settlement method in Payment Notification Advice accordingly.

5 Application Level

The Payment Notification is sent by the Originator Scheme to the Receiver Scheme as an online message to notify the Receiver Scheme of a successful clearing of a Mobile P2P transaction.

In analogy to the Repository Level, the message of the Application Level is defined both as XML and JSON data representation.

The Payment Notification is an advice message without a response message being sent back to the Originator Scheme other than a https return code.

5.1 JSON based Encoding

5.1.1 Payment Notification Advice

Call

POST /v1/payment_notification

Creates a Payment Notification.

Path

No specific path parameter.

Header

Content Type: JSON

Request

Mandatory	Message Element	XML-Tag	Type	Mobile P2P Requirements
yes	Transaction Identification	TxId	Max35Text	AT-05. The same reference as in the corresponding Look-up Request has to be used.
yes	Creation Date Time	CreDtTm	ISODateTime	AT-06 Timestamp of the processing time of the Notification.
yes	Alias Beneficiary	AlsBfy	AliasType, see Section 3.3.5	Currently only a mobile number or an email address in the form username@domainname is allowed as alias type. The same alias as in the corresponding Look-up Request has to be used.
no	Alias Originator	AlsOrig	AliasType, see Section 3.3.5	Currently only a mobile number or an email address in the form username@domainname is allowed as alias type. The same alias as in the corresponding Look-up Request has to be used.
yes	Originator Scheme	OrigSch	SchemeType, see Section 3.3.5	AT-02 Originator Mobile P2P Scheme The same values as in the corresponding Look-up Request have to be used.

Mandatory	Message Element	XML-Tag	Type	Mobile P2P Requirements
yes	Transaction Amount	TxAmt	AmountType, see Section 3.3.5	AT-04 The same amount as in the corresponding Look-up Request has to be used. Default currency is EUR. Other currencies than Euro are allowed only after confirmation by the receiver of the message.
no	Remittance Information	RmtInf	Max140Text	*Usage Rule:* Either 'Unstructured' or 'Structured' may be present. If present, the same Remittance Information has to be used as in the corresponding payment transaction.
yes	Clearing and Settlement Method	ClrgSttlmMtd	CodeSet	Clearing and Settlement indicator *Usage Rule:* The following values are allowed: • SCT • SCT-INST

Response Code

Status Code	Message Code	Description
201 (Created)		Payment Notification accepted.
400 (Bad Request)		Service not supported, resource not found or validation error occurred.
401 (Unauthorized)	CERTIFICATE_NOT_VALID	

403 (Forbidden)	MP2P_NOT_ADMITTED	Initiating Party is not admitted to the system

Response

No body data.

5.1.2 Examples

This example takes up the example data from Section 3.3.2.

POST https://bizum.es/Interoperability/v1/payment_notification/JFFY-20160606193626-000000001-99981

Body Parameter:

```
{
    "TxId" : "JFFY-20160606193626-000000001",
    "AlsBfy" : {
       "Tp": "MSDN"
       "Id:"+491516024488"
    },
    "AlsOrig": {
       "Tp" : "MSDN"
       "Id" : "+391073044700"
   },
   "OrigSch" : {
      "Nm" : "JIFFY MP2P Scheme",
      "OrgId" : "JIFFY"
   },
   "TxAmt" : {
      "Amt":"22.00",
      "Ccy":"EUR"
   },
   "RmtInf" : "Greetings from Milano",
   "CreDtTm" : "2016-06-06T19:36:40",
   "ClrgSttlmMtd" : "SCT-INST"
}
```

5.2 XML

The encoding of body parameters of the payment notification call encoded in XML syntax is only added as a fall-back solution. The XML encoding is contained in Section 5.2.1. Examples for detailed XML encodings are given in Section 5.2.2.

5.2.1 Schema definitions

The following tables contain the body definitions for the Payment Notification Advice for the XML data representation. Where possible, message elements and data types were chosen in analogy to ISO 20022 definitions. The data attribute definitions of [MP2P OR] are referenced in the following tables.

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[1..1]	+ Message Root	<MP2PNtfcAdv>		
[1..1]	+ Transaction Identification	<TxId>	Max35Text	AT-05 *Usage Rule:* • Maximum of 35 characters; no blanks are allowed. • The first four characters uniquely identify the Originator Scheme. The fifth character is a minus sign. The same reference as in the corresponding Look-up Request has to be used.
[1..1]	+ Creation Date Time	<CreDtTm>	ISODateTime	AT-13 Timestamp of the processing time of the Notification.
[1..1]	+ Alias Beneficiary	<AlsBfy>	-	Currently only a mobile number or an email address in the form username@domainname is allowed as alias type.
[1..1]	++ Type	<Tp>	CodeSet	"MSDN" or "EMAI" as code

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[1..1]	++ Identification	<Id>	Max140Text	AT-01 MSISDN or email address of the Beneficiary The same alias as in the corresponding Look-up Request has to be used.
[0..1]	+ Alias Originator	<AlsOrig>	-	Currently only a mobile number or an email address in the form username@domainname is allowed as alias type.
[1..1]	++ Type	<Tp>	CodeSet	"MSDN" or "EMAI" as code
[1..1]	++ Identification	<Id>	Max140Text	AT-13 MSISDN or email address of the Originator The same alias as in the corresponding Look-up Request has to be used.
[1..1]	+ Originator Scheme	<OrigSch>	Party-Identification32	AT-02 Originator Mobile P2P Scheme The same values as in the corresponding Look-up Request have to be used.
[1..1]	+ Transaction Amount	<TxAmt>	CurrencyAndAmount	AT-04 The same amount as in the corresponding Look-up Request has to be used. Default currency is EUR Other currencies than Euro are allowed only after confirmation by the receiver of the message.

Mult	Message Element	XML-Tag	Type	Mobile P2P Requirements
[0..1]	+ Remittance Information	<RmtInf>	Remittance Information 5	*Usage Rule:* Either 'Unstructured' or 'Structured' may be present. If present, the same Remittance Information has to be used as in the corresponding payment transaction.
{Or	++ Unstructured	<Ustrd>	Max140Text	*Usage Rule*: 'Unstructured' may carry structured remittance information, as agreed between the Originator and the Beneficiary.
Or}	++ Structured	<Strd>	Structured Remittance Information 7	*Format Rule*: 'Structured' can be used, provided the tags and the data within the 'Structured' element do not exceed 140 characters in length. *Usage Rule:* May only be used if agreed bilaterally between the Mobile P2P schemes.
[1..1]	+ Clearing and Settlement Method	<ClrgSttlmMtd>	CodeSet	Clearing and Settlement indicator *Usage Rule:* The following values are allowed: • SCT • SCT-INST

5.2.2 Examples

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <xsi:MP2PNtfcAdv>
    <TxId>JFFY-20160606193626-000000001</TxId>
    <CreDtTm>2016-06-06T19:36:36</CreDtTm>
    <AlsBfy>
      <Tp>MSDN</Tp>
      <Id>+491516024488</Id>
    </AlsBfy>
    <AlsOrig>
      <Tp>MSDN</Tp>
      <Id>+391073044700</Id>
    </AlsOrig>
    <OrigSch>
      <Nm>JIFFY MP2P Scheme</Nm>
      <Id><OrgId><Othr><Id>JIFFY</Id></Othr></OrgId></Id>
    </OrigSch>
    <TxAmt Ccy="EUR">22.00</TxAmt>
    <RmtInf><Ustrd>Greetings from Milano</Ustrd></RmtInf>
    <ClrgSttlmMtd>SCT-INST</ClrgSttlmMtd>
  </MP2PNtfcAdv>
</Document>
```

6 References

[MP2P OR] MobileP2P Interoperability Framework, Operational Rules, Joint Initiative pan-European Mobile P2P Interoperability, Version 1.2, 06 November 2020

This document contains a service description, the roles of the actors, an abstract data model for the messages to be used and a process description.

[EPC INRB] SCT INST Scheme Rulebook, EPC 004-16, Version 1.0, Date 30 November 2016

[EPC INIG] SCT INST Scheme Interbank Implementation Guidelines, EPC 122-16, Version 1.0, Date 30 November 2016