MONTRAN

National Bank of Georgia

Inception Report – Annex D – IPS-Participant Interface Specification

Instant Payments System

Version: 1.00

Date: 2025-06-13

DOCUMENT CONTROL

Title:	Inception Report – Annex D – IPS-Participant Interface Specification
Code:	GE_IPS_Inception_Report_Annex_D_IPS-Participant_Interface_Specification
Project:	GE_IPS_2023
Confidentiality:	BUSINESS USE ONLY
Integrity:	HIGH
Availability:	MEDIUM
Deliverable:	YES
Version:	1.00

DOCUMENT OWNERSHIP

NATURE OF INVOLVEMENT	NAME	INSTITUTION	ROLE
Owned by:	Sebastian Stefan	Montran	Technical Team Lead
First Draft by:	Romana Salageanu	Montran	Business Analyst
Last Verified by:	Sebastian Stefan	Montran	Technical Team Lead
Reviewed/QA by:	Sebastian Stefan	Montran	Technical Team Lead
Approved by:	NBG Payments, IT & Security teams	NBG	NBG Payments, IT & Security teams
Distributed to:	Nino Dziguashvili	NBG	Project Manager

DOCUMENT HISTORY

DATE	VERSION & STATUS	CHANGES
2024-02-05	0.01 DRAFT	First draft
2024-08-20	0.02 DRAFT	Second draft
2024-11-26	0.03 DRAFT	Montran replies to NBG comments from 11.11.24
2025-02-14	0.04 DRAFT	Montran updates onsite together with NBG, to NBG feedback from 26.12.24 starting on 16.01, continued by Montran based on the onsite discussions.
2025-04-03	0.05 DRAFT	Montran updates based on NBG feedback from 17.03.25.

DOCUMENT HISTORY		
DATE	**VERSION & STATUS**	**CHANGES**
2025-04-24	0.06 DRAFT	No feedback received to previous version. NBG requested to update document as pe last meetings based on Field Mapping Excel Spreadsheet. Montran updates brought and shared with NBG.
2025-05-14	0.07 DRAFT	Montran updates based on NBG feedback from 7.05.25 and based on field mapping conclusions from 30.04.2025.
2025-06-06	0.08 DRAFT	Updates during joint NBG – Montran call on 5.06.2025 and follow up by Montran. Sent to NBG on 06.06.25.
2025-06-10	0.09	Revision for final version, comments from NBG from 09.06.25.
2025-06-11	0.10	Amendment of lines in section 7.1.2 as per Montran recommendation and NBG confirmation.
2025-06-12	0.11	Small adjustment in section 7.1.2 as per NBG suggestion. Final version sent for review and confirmation.
2025-06-13	1.00 APPROVED	Clean version based on NBG confirmation from June 12th, 2025.

Table of Contents

List of Acronyms

BIC	Business Identifier Code
EPC	European Payments Council
GUI	Graphical User Interface
HTTPS	Hyper Text Transfer Protocol Secure
IBAN	International Bank Account Number
IPS	Instant Payments System
ISO	International Organization for Standardization
ISO20022	International Standard prepared by ISO Technical Committee TC68 Financial Services.
MCC	Merchant Category Code
MMC	Module for Management and Control
PM	Processing Module
STP	Straight-Through-Processing
UTC	Universal Time Coordinated

1. Introduction

This document describes the technical specification of the **Straight-Through-Processing (STP)** communication interface that the central **Instant Payments System (IPS)** provides for the communication with Participants. The document contains the following information:

1. A general presentation of the system's architecture.
2. Functions provided by the STP interface.
3. HTTPS communication protocol.

The specification for the Proxy solution is described in a separate document Annex E.

1.1. System Architecture

The Participant's information system contains the following components for accessing the IPS:

- **STP application** through which IPS messages are sent and received to and from the Central IPS.

  ⟶ This component is developed and managed by each IPS Participant.

- **User Workstation** through which the **Graphic User Interface (GUI)** of the Module for Management and Control can be accessed. This module is managed by the IPS Operator. The Participants manage the Workstation.

The central IPS consists of two main modules:

1. The **Processing module (PM)** that offers the STP interface for Participants' payment messages. PM exposes an API through which participants send messages, payments, proxy messages.
2. The Module for **Management and Control (MMC)** that provides the monitoring and control functions, using a graphical user interface.

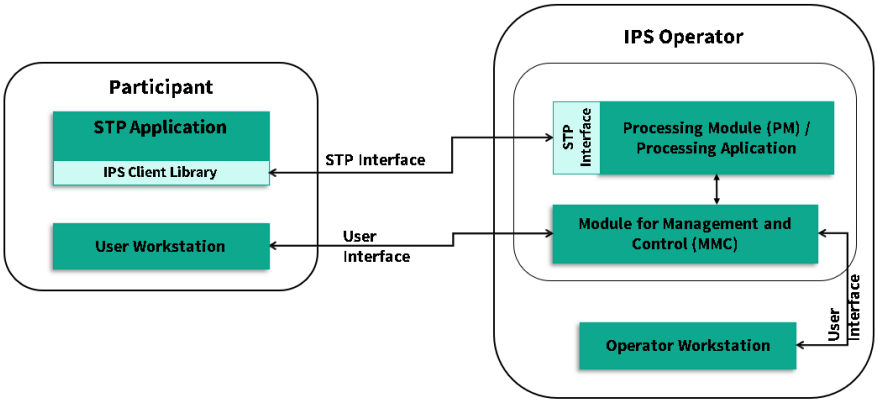


FIGURE 1. SYSTEM ARCHITECTURE

2. Straight-Through-Processing Interface Operations

The STP Interface offers the following Participant operations:

- Send messages according to the ISO20022 schemas.
- Receive messages (both for ISO20022 schemas and additional reconciliation messages or general notifications generated by the central IPS).
- Send confirmation message – pacs.002 for a received credit transfer instruction – pacs.008.
- Send confirmation of received messages (only for messages different from pacs.008, pacs.008 confirmation is described above).
- Queries for: technical accounts' positions, available balance for own account.
- Queries for positions, available balance for Indirect Participants.

The STP interface is developed using the HTTPS client-server protocol, through which the Participants' STP applications constantly request the central IPS to execute synchronous operations. This means that the Customer application initiates a request and waits to receive an answer from the central system (server).

IPS implements a duplication-detection algorithm so that sending and re-sending of a message to IPS means that IPS processes the first received message.

The STP communication protocol is stateless, i.e., each operation is completely independent of the others. The interface allows accessing a single function for the execution of a business operation.

2.1. Send Messages

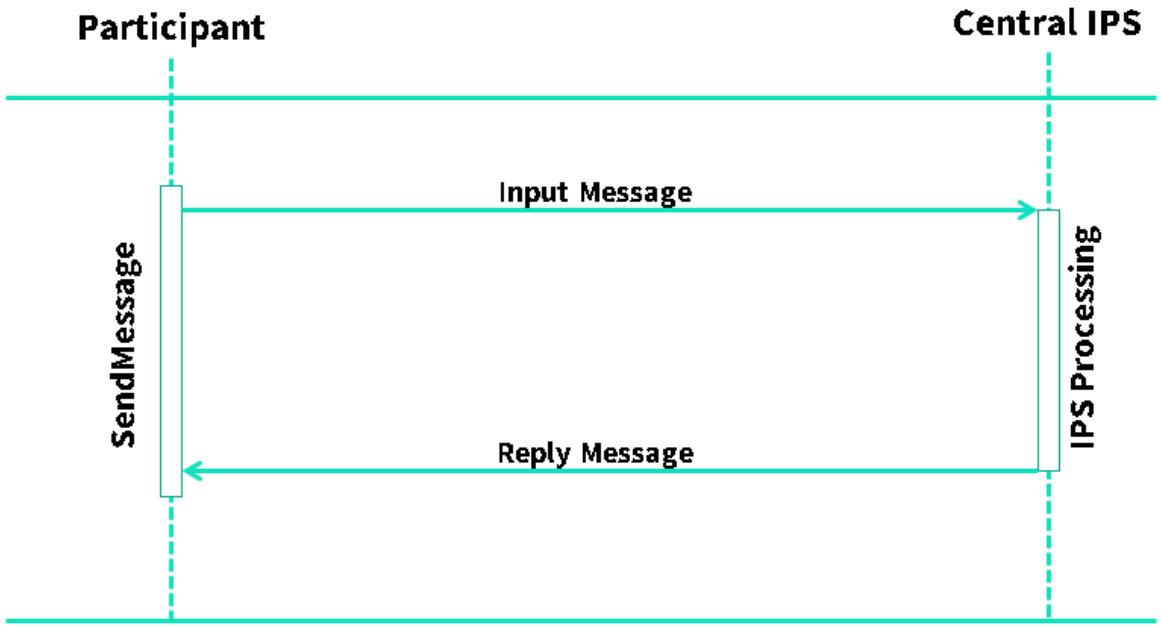


FIGURE 2. MESSAGE SENDING FLOW

The message types processed by the IPS system are presented in the table below. In addition to the ISO20022 Schema messages, the IPS also has some proprietary messages.

TABLE 1. IPS RECEPTION – ACCEPTED MESSAGES FOR ISO20022

MESSAGE RECEIVED BY IPS (EITHER BY SENDER OR BY BENEFICIARY)	DESCRIPTION	MESSAGE SENT BY IPS AS REPLY
pacs.008	ISO20022 message **Instant Credit Transfer**	pacs.002
Pacs.009	ISO20022 message Financial Institution Instant Credit Transfer	Pacs.002
pacs.004	ISO20022 message **Positive reply to Request for Recall** (cam.056)	pacs.002
pacs.002	ISO20022 message **Confirmation or Rejection to Instant Credit Transfer** (ConfirmationMessage)	pacs.002
camt.056	ISO20022 message for **Request for Recall of an Instant Credit Transfer**	pacs.002

camt.029	ISO20022 **rejection message to Request for Recall** (cam.056)	pacs.002
pacs.028	ISO20022 message for **information request about the status of a previously processed Instant Credit Transfer instruction, RTP and Recall**	pacs.002
pain.001	ISO20022 message for Customer Credit Transfer Initiation	pain.002
pain.002	ISO20022 message for Customer Payment Status Report	pacs.002
camt.055	ISO20022 message for Customer Payment Cancellation Request	pacs.002
pain.013	ISO20022 message for **Request to Pay**	pain.014
pain.014	ISO20022 message for **Response to Request to Pay**	
positions.001	**Custom XML message used to summarize a Participant's current technical account's position.**	

For processing of instant credit transfers, the central IPS sends a **pacs.002 Reply Message** if the sending, validation, and processing have been executed. The receiver bank generates a pacs.002 **Confirmation Message** to the central IPS to report the result of its internal verification (timeout/account availability/AML/etc.). This way, the central IPS will have all the information necessary to complete the transaction clearing.

In some cases, when messages other than the Instant pacs.008 and Instant pacs.028 are used, the sender Participant receives a reply message from the central IPS **immediately after the execution of the validation and processing of the initial message**. This processing **does not mean** that the receiver Participant has received the message generated by the central IPS as a result of the initial sender's message processing.

When a pacs.008 message initiates a real-time payment, the receiver Participant's **time interval for the payment's processing is between sending the initial message (InputMessage pacs.008) and receiving the reply from the receiver Participant (ReplyMessage pacs.002).** Thus, the sending Participant receives **only one final reply message about the status of the initiated payment**.

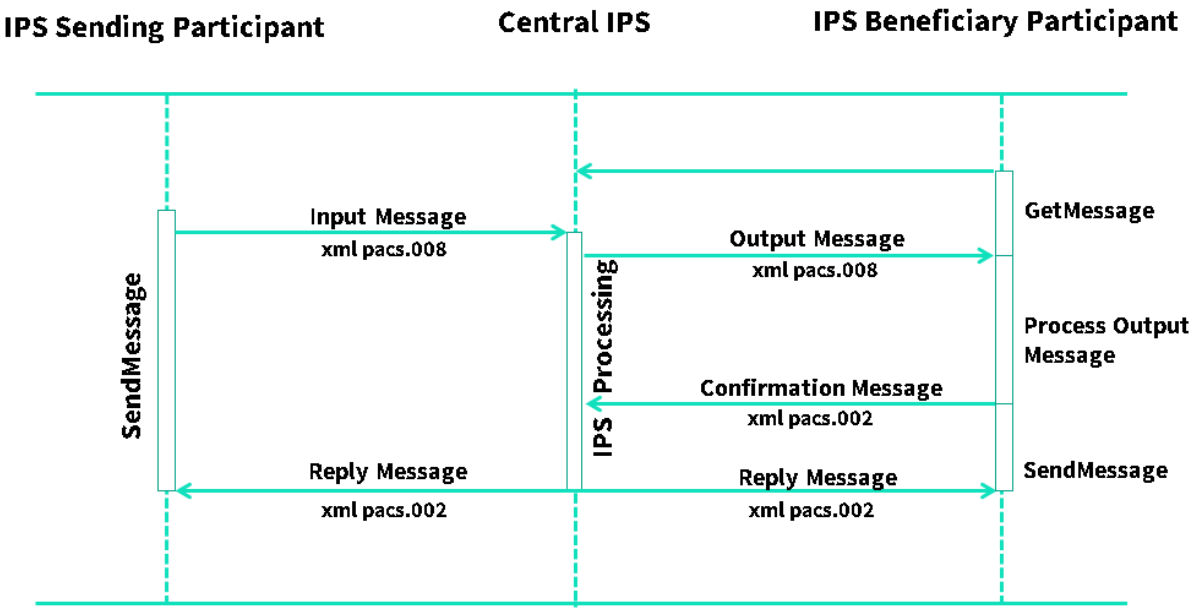


FIGURE 3. SENDING AND RECEIVING FLOW OF A PACS.008 IPS MESSAGE BY PARTICIPANTS

2.2. Receive Messages

Participants perform polling on the IPS API to request the next message. If the central IPS has no message to deliver to Participants, the IPS waits before sending the reply for a certain time interval, in the event that a message becomes available, e.g., another Participant sends a payment instruction. When the **receive function** has awaiting status, and a message is received, the message is immediately delivered to the Participant.

If no message is available for the receive function by the end of the maximum awaiting time period[1], the receive function sends a null value and the Participant's application tries again.

[1] Right now, this parameter (HTTPS Long-Polling) is set in the central IPS to 5 seconds but it is configurable.

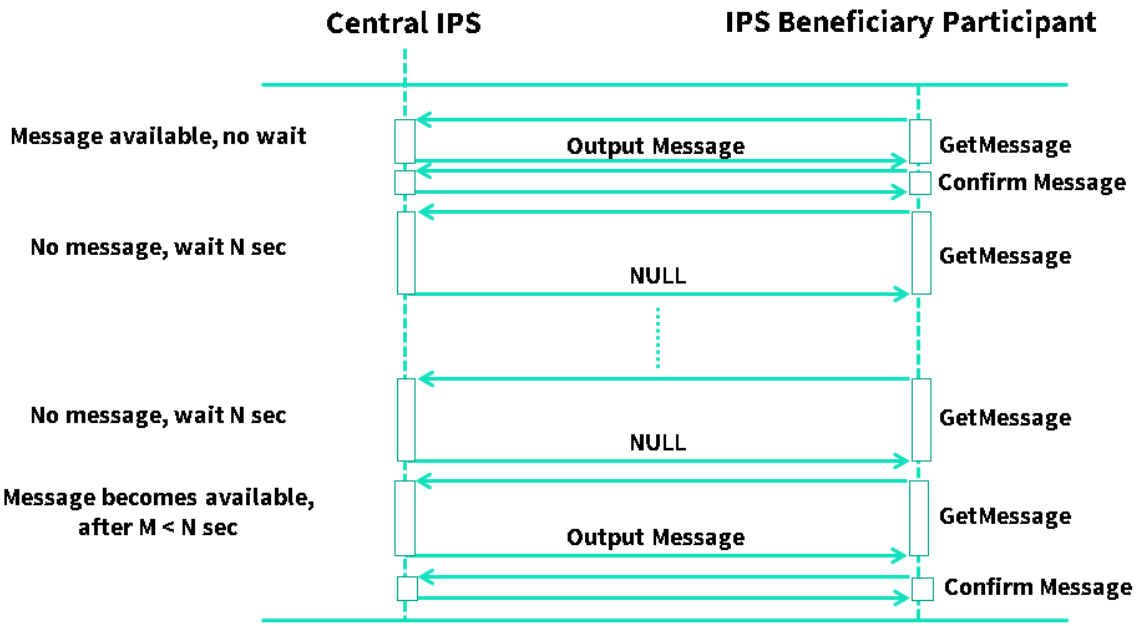


FIGURE 4. RECEIVE FUNCTION FLOW

This procedure permits monitoring of the Participant's connections to the central IPS. Technically, the Participant's STP application initiates a connection only when a message needs to be sent. But in the context of 24/7 operating time, for receiving messages, the STP application must be connected to the central IPS (almost) permanently. The IPS detects the receive operations' frequency of a Participant by calling the ONLINE status for a Participant that calls the receive message function at a time interval equal or less than 5 seconds[2]. If the STP application does not call the receive message function within a time period of less than 5 seconds, the Participant's status becomes OFFLINE for the central IPS system[3].

The messages that Participants receive from the central IPS must be confirmed using a specific function. The confirmation operation signals the central IPS that the Participant's system succeeded to store and processes the message and therefore, the central IPS message can delete that message from its internal queues. If the central IPS does not receive the Participant's confirmation, the central IPS will resend the unconfirmed messages to the receiver Participant after a few seconds. The messages are re-sent aftertimeout (configurable as a system parameter called output redelivery time) until confirmation by participant or until the Participant's status becomes "OFFLINE" (and resumed after they become "ONLINE" again . Participants should thus be ready to receive duplicates, the API assists them in handling this by providing a possible duplicate header **X-MONTRAN-IPS-PossibleDuplicate.** The messages are enqueued for delivery according to priority (SLA messages are higher priority) and can be consumed by the participant at their own rate. If the participant is offline, then transactions where that participant is the receiver are rejected instantly, and no further messages are enqueued for that participant.

[2] System parameter "Participant Connection Timeout".
[3] Instant payment messages (pacs.008) with an Offline receiving Participant are rejected by the IPS.

The confirmation operation must be executed for all XML message types belonging to the ISO20022 schema, except for the execution of pacs.008, for which, according to the processing flow, the Participant system must send a confirmation/rejection pacs.002 message. This pacs.002 message also confirms receipt of the pacs.008 message.

3. Message Processing

In case of any discrepancies between Inception Report (including annexes) statements/detailed descriptions and XML messages, the statements will prevail, since at this stage NBG cannot check the XML messages.

Messages will be compatible with ISO20022 latest version full set and implementation guidelines SEPA Instant Credit Transfer Inter-PSP Implementation Guidelines (EPC004-16/ 2025 Version 1.0, EPC122-16 / 2025 Version 1.0) and Inter-RTP Service provider SRTP Implementation Guidelines (latest versions - EPC014-20 / Version 4.0, EPC259-22/ Version 3.0), so if there will be difference between initial report and the guidelines, guidelines will prevail, and responsibility of correction will be on Montran side.

Part of the updates to IGs, a communication process between Operator and Montran will precede the actual implementation of changes.

3.1. Message Structure

The IPS system uses XML messages that contain two different parts:

1. A common **Business Application Header**, with an identical structure for all messages.
2. A **message body**, different for each message type.

The Business Application Header respects the ISO 20022 head.001.001.01 schema and entails the following:

1. Routing information: sender and receiver institution.
2. Digital signature information.
3. Type of business message.

Please see a detailed presentation of the header in section Message Header (App Hdr) – head.001.001.03.xsd.

The message body is specific to each message type handled by the IPS system: pacs.008, pacs.002, pacs.004, camt.056, camt.029, pacs.028, pain.013, pain.014, camt.053, pain.001, camt.055, pain.002, participants.001, pacs.009.

The schemas employed for the ISO20022 support UTF-8 by default, allowing all text in English and Georgian to be exchanged.

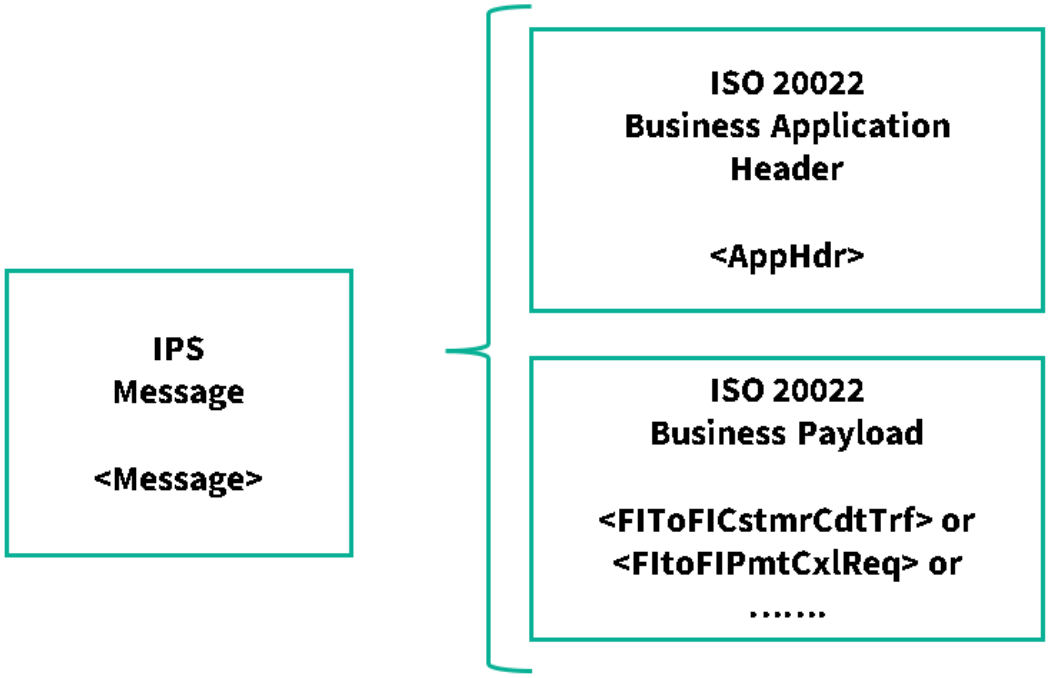


FIGURE 5. MESSAGE STRUCTURE

3.2. Message Validation within the Central Instant Payments System

The central IPS processes funds transfers that are based on the identified Participant. The IPS identifies the Participant using the mandated agent identifier (e.g., BIC for the SEPA ICT rulebook). The IPS then produces accounting based on that and passes the account information of the payee or payer to the receiving Participant for booking.

For all messages received by IPS a validation is performed against the current XML schema version, as defined by ISO20022 standard. All the rules described in the XSD files are automatically checked by IPS and if the message does not comply it is rejected with a specific error code (FF01).

The limits used by IPS to validate amounts and timeouts are defined in the Payment Schema menu in MMC, which is configurable by the Operator. During message processing, IPS matches the current message with a payment schema based on payment schema filter parameters and participant mapping. The payment schema filter parameters are: Local Instrument and Category Purpose, which can also be set to “ALL” (meaning it applies to all messages). The mapping between payment schemas and participants is managed by the Operator and there are no restrictions about which payment schema can be mapped to which participant. The same payment schema can be mapped to all participants.

IPS validations which are based on on/off parameter managed by Operator are:

- IBAN validation – if enabled, IPS will also validate checksums

- RTP attachment – if disabled, IPS will reject RTP messages which contain embedded attachments.

The central IPS validates the messages received from Participants and generates a pacs.002 message that comprises the validation result. The pacs.002 messages are received by calling the receive message method.

IPS uses the Debtor/Creditor agent tags (CdtrAgt - FinInstnId - BIC, DbtrAgt - FinInstntId - BIC) to identify the participants (either direct or indirect clearing), adjusted for R messages. The routing information is included in the Business Application Header (AppHdr – Fr, AppHdr – To) and in specific tags in the business payload.

The Business Application Header must be present on all ISO20022 messages exchanged between IPS and Participants. The routing information is described in the following tags:

XML Tag	Routing information
AppHdr/Fr	The message sender. On messages sent to IPS, it is validated to be the same as channel sender. On messages generated/forwarded by IPS it is set to IPS BIC.
AppHdr/To	The message receiver. On messages sent to IPS, it is validated to be the IPS BIC. On messages generated/forwarded by IPS it is set to receiver participant.

The routing information in the business payload is described in the following tags:

XML Tag	Message type	Routing validation
GrpHdr/InstgAgt	pacs.x	Message sender On messages sent to IPS, it is validated to be the same as channel sender (BIC defined in HTTPS header and matched with SSL certificate). On messages forwarded by IPS it is removed.
GrpHdr/InstdAgt	pacs.x	Message receiver On messages sent to IPS, it is restricted.

		Added to messages forwarded/generated by IPS, to identify the message receiver (direct clearing participant).
Assgnmt/Assgnr	camt.x	Message sender On messages sent to IPS, it is validated to be the same as channel sender Added to messages forwarded/generated by IPS, as the IPS BIC.
Assgnmt/Assgne	camt.x	Message receiver On messages sent to IPS it is validated to be the same as IPS BIC. Added to messages forwarded/generated by IPS, to identify the message receiver (direct clearing participant).
GrpHdr/InitgPty	pain.x	Message sender On messages sent to IPS, it is validated to be the same as channel sender Note: not updated on messages forwarded by IPS.

For messages that are forwarded by IPS to another participant, a new BAH is generated in IPS and the routing details are overwritten as well. For example, during the processing of an instant credit transfer, sent from direct clearing participant A to direct clearing participant B (indirect clearing participants omitted from this example since they are not included in routing anyway), the routing information is set as follows:

1. Pacs.008 message from participant A (details set by participant A)
    a. AppHdr/Fr: BIC of participant A
    b. AppHdr/To: BIC of IPS
    c. GrpHdr/InstgAgt: BIC of participant A
    d. GrpHdr/InstdAgt: restricted

2. Pacs.008 message forwarded from IPS to participant B (details set by IPS)
    a. AppHdr/Fr: BIC of IPS
    b. AppHdr/To: BIC of participant B
    c. GrpHdr/InstgAgt: removed
    d. GrpHdr/InstdAgt: BIC of participant B
3. Pacs.002 Reply sent from participant B (details set by participant B)
    a. AppHdr/Fr: BIC of participant B
    b. AppHdr/To: BIC of IPS
    c. GrpHdr/InstgAgt: BIC of participant B
    d. GrpHdr/InstdAgt: restricted
4. Pacs.002 status from IPS to participant A
    a. AppHdr/Fr: BIC of IPS
    b. AppHdr/To: BIC of participant A
    c. GrpHdr/InstdAgt: BIC of participant A
5. Pacs.002 status from IPS to participant B
    a. AppHdr/Fr: BIC of IPS
    b. AppHdr/To: BIC of participant B
    c. GrpHdr/InstdAgt: BIC of participant B

The same rules apply to all the other message flows. For each step of the flow, the corresponding message BAH reflects current sender and receiver (including IPS).

Besides routing, the following tags are used to identify if the creditor or debtor participant is an indirect clearing participant:

XML Tag	Message Type	Validation
CdtTrfTxInf/**DbtrAgt**/FinInstntId/BIC	pacs.008, pacs.009	Must be equal to the channel sender or the BIC of an indirect clearing participant mapped to it. Must identify an ACTIVE participant in the system.
TxInf/OrgnlTxRef/**DbtrAgt**/FinInstntId/BIC	pacs.004	Must identify an ACTIVE participant in the system. If it's an indirect clearing participant,

		then IPS will route the message to its direct clearing participant.
Undrlyg/TxInf/OrgnlTxRef/**DbtrAgt**/ FinInstntId/BIC	camt.056	Must be equal to the channel sender or the BIC of an indirect clearing participant mapped to it. Must identify an ACTIVE participant in the system.
CxlDtls/TxInfAndSts/OrgnlTxRef/ **DbtrAgt**/FinInstntId/BIC	camt.029	Must identify an ACTIVE participant in the system. If it's an indirect clearing participant, then IPS will route the message to its direct clearing participant.
TxInfAndSts/OrgnlTxRef/**DbtrAgt**/ FinInstntId/BIC	pacs.002	Must identify an ACTIVE participant in the system. If it's an indirect clearing participant, then IPS will route the message to it's direct clearing participant.
PmtInf/**DbtrAgt**/FinInstnId/BIC	pain.001, pain.013	Must identify an ACTIVE participant in the system. If it's an indirect clearing participant, then IPS will route the message to it's direct clearing participant.
OrgnlPmtInfAndSts/TxInfAndSts/ OrgnlTxRef/**DbtrAgt**/FinInstnId/BIC	pain.002, pain.014	Must be equal to the channel sender or the BIC of an indirect clearing participant mapped to it. Must identify an ACTIVE participant in the system.
Undrlyg/OrgnlPmtInfAndCxl/TxInf/ OrgnlTxRef/**DbtrAgt**/FinInstnId/BICFI	camt.055	Must identify an ACTIVE participant in the system. If it's an indirect clearing participant, then IPS will route the message to it's direct clearing participant.
CdtTrfTxInf/**CdtrAgt**/FinInstnId/BIC	pacs.008, pacs.009	Must identify an ACTIVE participant in the system. If it's an indirect clearing participant, then IPS will route the message to it's direct clearing participant.
TxInf/OrgnlTxRef/**CdtrAgt**/FinInstntId/BIC	pacs.004	Must be equal to the channel sender or the BIC of an indirect

		clearing participant mapped to it. Must identify an ACTIVE participant in the system.
Undrlyg/TxInf/OrgnlTxRef/**CdtrAgt**/ FinInstntId/BIC	camt.056	Must identify an ACTIVE participant in the system. If it's an indirect clearing participant, then IPS will route the message to it's direct clearing participant.
CxlDtls/TxInfAndSts/OrgnlTxRef/ **CdtrAgt**/FinInstntId/BIC	camt.029	Must be equal to the channel sender or the BIC of an indirect clearing participant mapped to it. Must identify an ACTIVE participant in the system.
TxInfAndSts/OrgnlTxRef/**CdtrAgt**/ FinInstntId/BIC	pacs.002	Must identify an ACTIVE participant in the system. In the case of indirect clearing participant, it must identify a participant mapped to the original message receiver.
PmtInf/CdtTrfTx/**CdtrAgt**/FinInstnId/BIC	pain.001, pain.013	Must be equal to the channel sender or the BIC of an indirect clearing participant mapped to it. Must identify an ACTIVE participant in the system.
OrgnlPmtInfAndSts/TxInfAndSts/ OrgnlTxRef/ **CdtrAgt**/FinInstnId/BIC	pain.002, pain.014	Must identify an ACTIVE participant in the system. If it's an indirect clearing participant, then IPS will route the message to it's direct clearing participant.
Undrlyg/OrgnlPmtInfAndCxl/TxInf/ OrgnlTxRef/**CdtrAgt**/FinInstnId/BICFI	camt.055	Must be equal to the channel sender or the BIC of an indirect clearing participant mapped to it. Must identify an ACTIVE participant in the system.

For all flows in which a message is forwarded from a participant to another (pacs.008, pacs.004, etc.), IPS will generate a new message in order to write the BAH and routing details described above and to apply digital signature. Besides this, the business payload is copied into the new message as it was transmitted by the sender participant.

3.2.1. Instant Credit Transfer Message Validation – pacs.008.001.12

The IPS's validation process for the received pacs.008 payment messages follows the steps:

1. Validate https request header. Each HTTPS request to the system must have the X-MONTRAN-IPS-Channel request header which indicates the Participant's communication channel. If this header is missing or incorrect then the PM https reply will have **error code 401 Unauthorized**.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation, which is relevant for all types of message headers and covers the following:

FIELD	ERROR CODE[4]
Sender BIC	1018, 1021
Receiver BIC	1027
Message Identification	101
Signature	3001, 3002, 3003, 3004

4. Message business fields' validation:
    a. **TtlIntrBkSttlmAmt,** with **Ccy** attribute – payment amount and currency for Instant transactions. These must be valid according to the predefined payment schema.
    b. **IntrBkSttlmDt** – payment date, must be the current calendar day (exception for instant is described in the note below).
    c. Static message fields: **ClearingSystem**, **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes.**
    d. **LocalInstrument –** Accepted values for instant include: INST.

[4] Refer to section

Annex 2 – Error Codes for a description of the error codes.

e. **CtgyPurp** –Codes (option **Cd**) are validated according to a list maintained by the system operator in MMC and presented in the Inception Report, section 3.5.6 External Codes.

f. **InstgAgt** – BIC of sender Participant. It must identify an ACTIVE Participant in the system. This BIC must identify the sender Participant detected at the sending channel. In case of payments originated from an indirect clearing participant then this field will identify the direct clearing participant.

g. **InstdAgt –** restricted.

h. **DbtrAgt** – BIC of debtor Participant. This must be equal to **InstgAgt** for direct clearing Participants or to one of the sender's indirect clearing Participants and not blocked for debit.

i. **CdtrAgt** – BIC of creditor Participant. This must identify an ACTIVE and not blocked for credit Participant, This Participant must be connected to the system (must have ONLINE status).

j. **IntrBkSttlmAmt** – values equal to the ones in **TtlIntrBkSttlmAmt**.

k. **DbtrAcct** and **CdtrAcct** – IBAN codes must be valid: structure and checksum (ISO 7064). Checksum is validated according to System Parameter configured by Operator

l. **Ref** (RmtInf – Strd – CdtrRefInf), combined with **Prtry** (RmtInf – Strd – CdtrRefInf – Tp – CdOrPrtry - Prtry). If Prtry code exists and is set to fixed text "MCC" then IPS will interpret the Ref value as the Merchant Category Code, otherwise no additional validation is performed. For each instant credit transfer, IPS parses the MCC code, and if it exists then it validates it according to the list maintained in MMC by the Operator. If Prtry code is set to fixed text "SERV" then the value of Ref is a service identifier/code or order number, and no validation is performed by IPS.

m. **RmtId (**CdtTrfTxInf - RltdRmtInf**) -** Initiation Channel and Instrument – if present, they should follow the rule: 4 uppercase alphabetic characters (channel code) followed by ":" followed by 4 uppercase alphabetic characters (instrument code). There may be multiple instrument codes. If channel code or any of the instruments is "PRXY" then IPS marks transaction as initiatied after proxy lookup and stores this flag in the database.

5. **For pain.013 initiated instant credit transfers**, the payment is reconciled with the original request when the EndToEndId starts with an RTP stub (RTP-). In this case the following validations are performed:

a. **EndToEndId** – it contains a message reference corresponding to an in-progress pain.013 –**PmtInfId**.

b. **Acceptance Date Time** – It is within the timeout defined in the Payment Schema for fast RTP. For fast RTP flow it is validated with the original RTP message.

c. The sender of the pacs.008 is the receiver of the pain.013.

d. Currency, Creditor and Debtor accounts are the same as in the original pain.013 (for fast RTP flow).

e. InstrPrty (GrpHdr - PmtTpInf) – either “HIGH” or “NORM” to identify RTP fast or slow flow.

6. **For pain.001 initiated instant credit transfers,** the payment is reconciled with the original request when the EndToEndId starts with an initiation stub (PSP-). In this case the following validations are performed:

   a. **EndToEndId** – it contains a message reference corresponding to an in-progress pain.001 – **PmtInfId.**

   b. **Acceptance Date Time –** it is equal to the timestamp of the in-progress pain.001 CreDtTm. The timeout of the instant credit transfer is the same as the one for regular pacs.008, defined in Payment Schema – Initiation Deadline, Timeout Deadline.

   c. The sender of the pacs.008 is the receiver of the pain.001.

   d. Creditor Agent, Currency, Amount, Creditor and Debtor accounts are the same as in the in-progress pain.001.

7. Timestamp validation

   a. Late initiation message – the system checks if the time in the field **Acceptance Date Time** (AT-50) is not exceeded by the current processing time with more than the **Initiation Deadline** parameter configured in the payment schema. This check is done to allow enough time for the receiver to process the payment within the SLA.

   b. expired message – the system checks if the time in the field **Acceptance Date Time** (AT-50) is not exceeded by the current processing time with more than the **Timeout Deadline** parameter configured in the payment schema. After the initiation deadline validation, the application also runs a timer to check if the payment is completed before the timeout deadline and cancels it otherwise.

8. Duplicate message verification. For this purpose, the IPS compares the message reference (field **MsgId**) with all references of messages that the system received from the same Participant (DebtorAgent) during the last 24 hours. Also the item reference (field **TxId**) is compared with all item references that the system received from the same Participant during the last 24 hours.

9. Validation of digital signature.

During this validation process, the IPS reports only the first detected error by replying with a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

Fields which are included in the message, to transmit certain information between the participants, but are not validated by IPS (besides the XML schema rules) are presented below:

- **CreDtTm** - The exact time at which the PSP (direct participant in the system) technically receives the order from customer or indirect participant.
- **ElctrncAdr** (CdtTrfTxInf - RltdRmtInf - RmtLctnDtls) - The coordinates of the POS/device which was used for the payment.
- **Ustrd** (CdtTrfTxInf - RmtInf) – payment details
- **AddtlRmtInf (**CdtTrfTx – RmtInf – Strd) – additional purpose of payment
- **Id** (CdtTrfTxInf - CdtrAcct-Id-Othr) – treasury code .
- **Id** (CdtTrfTxInf - DbtrAcct-Id-Othr) – treasury code .
- **Nm** (CdtTrfTxInf - Dbtr) – ordering customer name.
- **Nm** (CdtTrfTxInf - UltmtDbtr) – third party ordering name
- **Nm (**CdtTrfTxInf - Cdtr**) –** beneficiary customer name.
- **Nm (**CdtTrfTxInf – UltmtCdtr) – third party beneficiary name
- **PstlAdr (**CdtTrfTxInf – Dbtr) – payer information (adress).
- **DtAndPlcOfBirth** (CdtTrfTxInf – Dbtr – Id – PrvtId) – payer information (birth info)
- **PstlAdr (**CdtTrfTxInf – Cdtr) – payee information (adress)
- **DtAndPlcOfBirth** (CdtTrfTxInf – Cdtr – Id – PrvtId) – payee information (birth info)
- **Id** (CdtTrfTxInf - Dbtr – Id – OrgId – Othr) – , combined with **Cd (**Dbtr – Id – PrvtId – Othr – SchmeNm). Special values for Cd: “BILL” (value of id is service user identifier for bill payments). If no code is set, then value of id is “ordering organization id”. In case of BILL payments, both the BILL identifier and personal id will be present under separate Othr tags.
- **Id (**CdtTrfTxInf - Dbtr – Id – PrvtId - Othr**) –** combined with **Cd (**Dbtr – Id – PrvtId – Othr – SchmeNm). Special values for Cd: “BILL” (value of id is service user identifier for bill payments). If no code is set, then value of id is “personal id”. In case of BILL payments, both the BILL identifier and personal id will be present under separate Othr tags.
- **Id** (CdtTrfTxInf - Cdtr – Id – OrgId – Othr) – beneficiary organization id.**Id** (CdtTrfTxInf - Cdtr – Id – PrvtId – Othr) – beneficiary person id
- **Id (**CdtTrfTxInf - UltmtDbtr – Id – OrgId - Othr**) –** third party ordering organization id
- **Id (**CdtTrfTxInf - UltmtDbtr – Id – PrvtId - Othr**) –** third party ordering person id
- **Id (**CdtTrfTxInf - UltmtCdtr – Id – OrgId - Othr**) –**third party beneficiary organization id
- **Id (**CdtTrfTxInf - UltmtCdtr – Id – PrvtId - Othr**) –**third party beneficiary person id

The various timeouts have been illustrated in diagrams below to provide more clarity to these flows. Note that the timeout validations which imply a decision (such as accept or reject message based on timestamp) have been illustrated with the negative outcome only for the purpose of these diagrams: to showcase what happens when various timeouts are breached. Decision points which are not part of the sequence indicated by arrows are part of automatic IPS timers (which monitor transaction expiration for example). The happy flows are described in the diagrams with the complete flows.

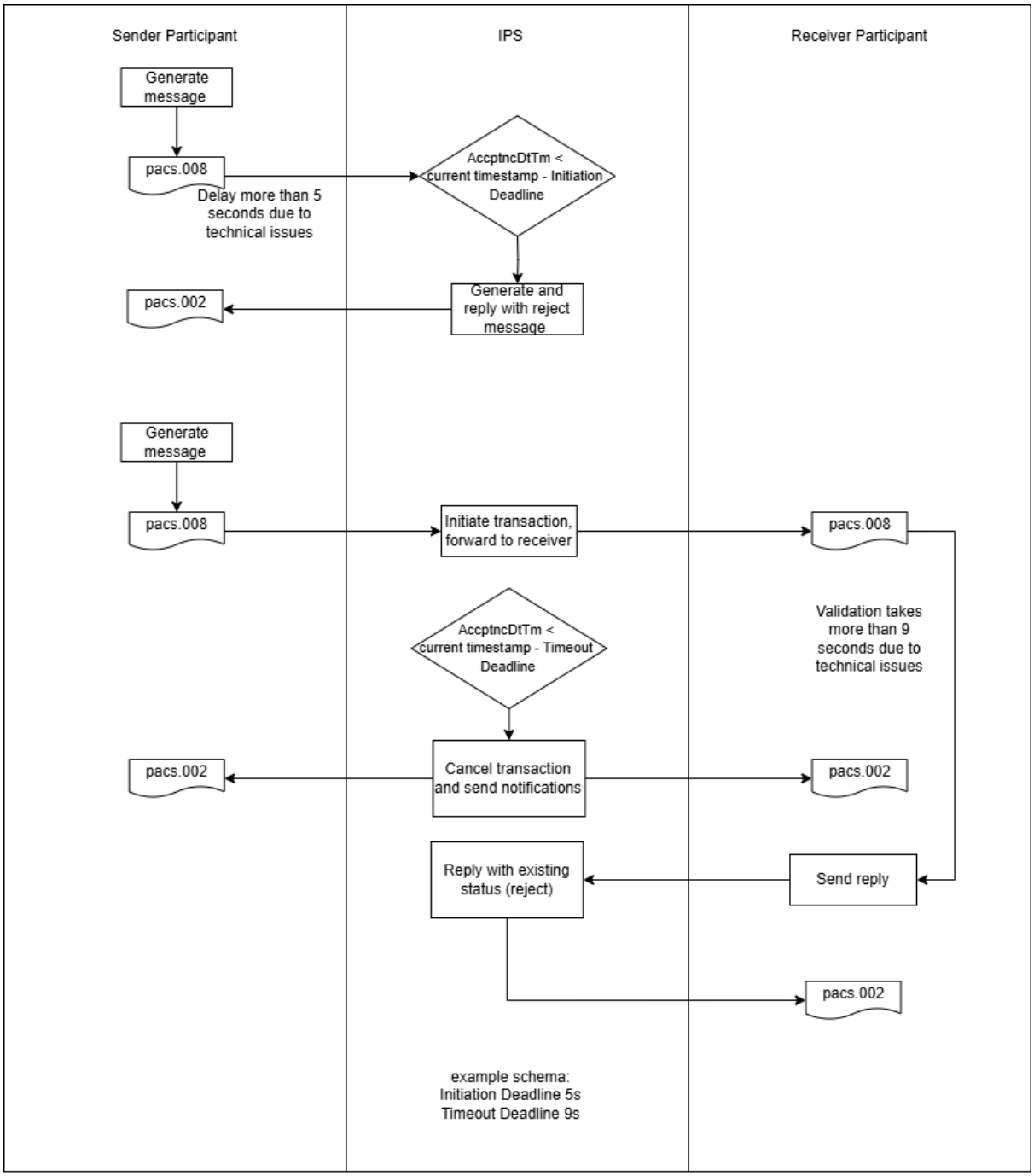


FIGURE 6. TIMEOUT VALIDATION FOR PACS.008

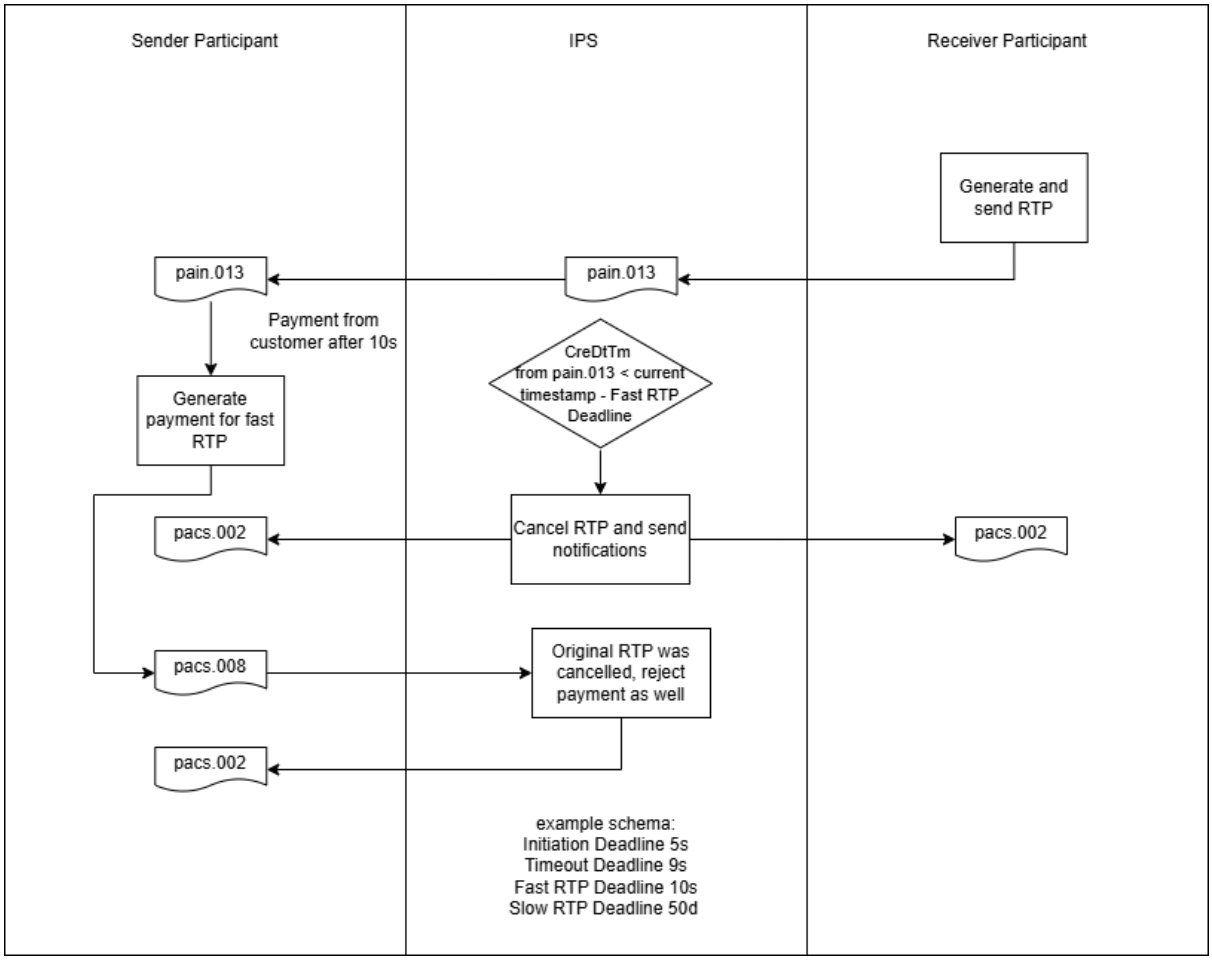


FIGURE 7. TIMEOUT VALIDATION FOR PACS.008 INITIATED AFTER RTP

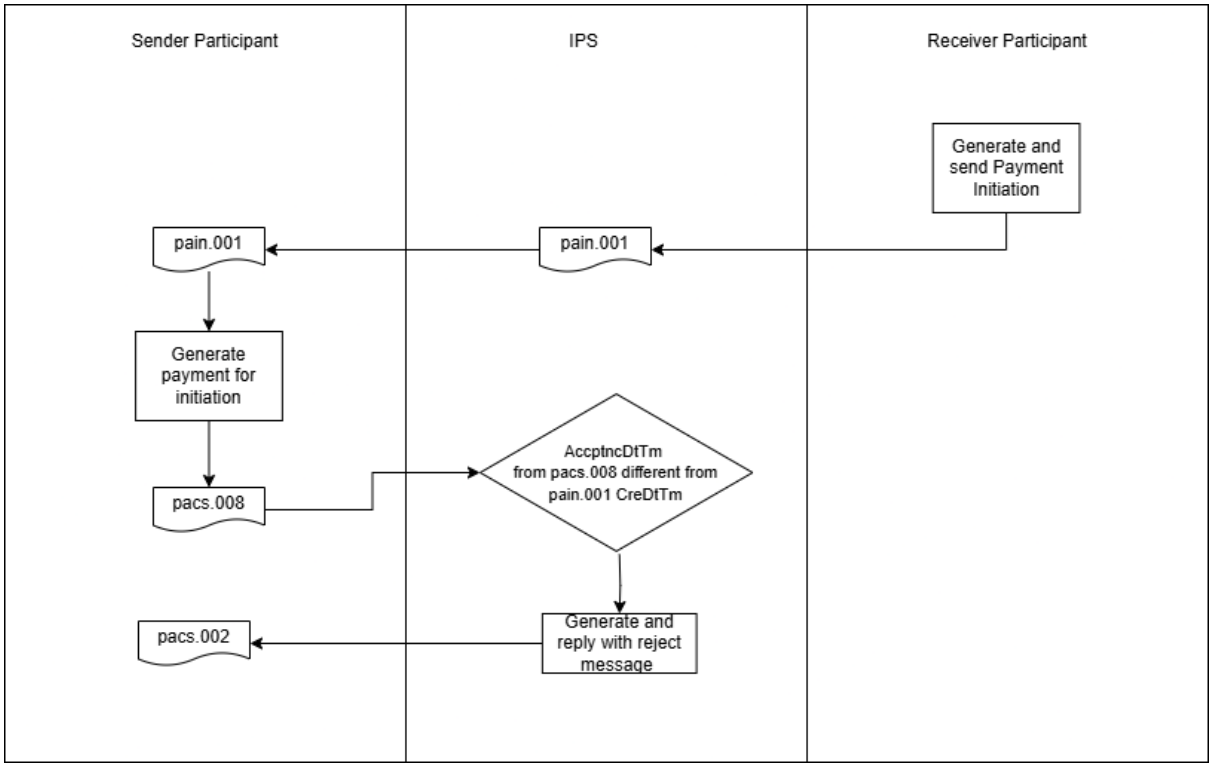


FIGURE 8. TIMEOUT VALIDATION FOR PACS.008 AFTER PAIN.001

Note: Detailed validation of the payment date: The system accepts payments initiated by a Participant even before 00:00, e.g. 23:59:59 on payment date T-1, if these messages are received and processed on date T until 00:00+"grace-time", where "grace-time" is a parameter equal to Timeout Deadline (default 20 seconds). In this case, the system only accepts payments instructions with payment date (**IntrBkSttlmDt**) equal to T-1 is 00:00:20.

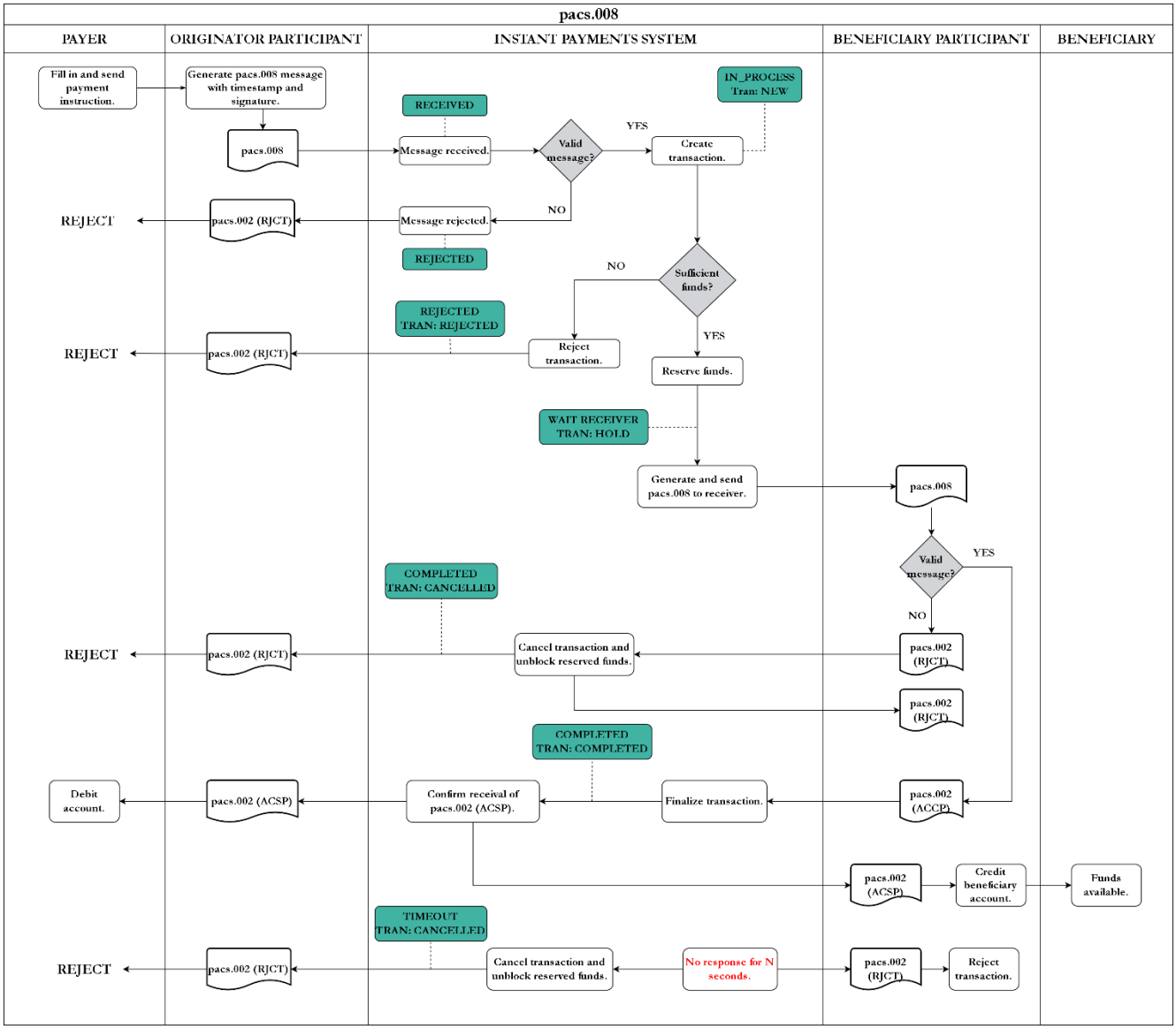


FIGURE 9. STATUS TRANSITION FLOW OF INSTANT PACS.008 PAYMENT MESSAGE

3.2.2. Financial Institution Instant Credit Transfer Message Validation– pacs.009.001.11

This message can be used by Participants for liquidity lending. The usage described here applies only within IPS (the usage of pacs.009 for Liquidity Adjustment is not in scope of this document). Lending functionality is allowed at any time, regardless of RTGS settlement window status.

This message will transfer funds from the technical account of an IPS participant to another's. It will not impact the overall balance in the system (the total in the IPS pool account stays the same), the funds movement is only within IPS.

A validation is performed such that the maximum amount is within the payment schema threshold and the lending participant's account balance will not drop below low limit.

The IPS's validation process for the pacs.009 payment messages sent and received between Participants within the IPS follows the steps:

1. Validate https request header. Each HTTPS request to the system must have the X-MONTRAN-IPS-Channel request header which indicates the Participant's communication channel. If this header is missing or incorrect then the PM https reply will have **error code 401 Unauthorized**.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation, which covers the following:

FIELD	ERROR CODE[5]
Sender BIC	1018, 1021
Receiver BIC	1027
Message Identification	101
Signature	3001, 3002, 3003, 3004

4. Message business fields' validation:
    a. **TtlIntrBkSttlmAmt** – payment amount and currency for Instant transactions. These must be valid according to the predefined payment schema.

[5] Refer to section

Annex 2 – Error Codes for a description of the error codes.

b. **IntrBkSttlmDt** – payment date, must be the current calendar day (exception for instant is described in the note below).

c. Static message fields: **ClearingSystem**, **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes .**

d. **LocalInstrument –** Accepted values for instant include: INST.

e. **CtgyPurp** –Codes (option **Cd**) - **will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes.**

f. **InstgAgt** – BIC of sender Participant. It must identify an ACTIVE Participant in the system. This BIC must identify the sender Participant detected at the sending channel.

g. **DbtrAgt** – BIC of debtor Participant. This must be equal to **InstgAgt** for direct connection participants or to one of the sender's indirect participants and not blocked for debit.

h. **CdtrAgt** – BIC of creditor Participant. This must identify an ACTIVE and not blocked for credit Participant. This participant must be connected to the system (ONLINE).

i. **IntrBkSttlmAmt** – values equal to the ones in **TtlIntrBkSttlmAmt**.

j. **DbtrAcct** and **CdtrAcct** – if present, IBAN codes must be valid: structure and checksum (ISO 7064). Checksum validation is done only if System Parameter is set.

5. Duplicate message verification. For this purpose, the IPS compares the message reference (field **MsgId**) with all references of messages that the system received from the same Participant (DebtorAgent) during the last 24 hours. Also the item reference (field **TxId**) is compared with all item references that the system received from the same Participant during the last 24 hours.

6. Validation of digital signature.

During this validation process, the IPS reports only the first detected error by replying with a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

Note: Detailed validation of the payment date: The system accepts payments initiated by a Participant even before 00:00, e.g. 23:59:59 on payment date T-1, if these messages are received and processed on date T until 00:00+"grace-time", where "grace-time" is a parameter equal to Timeout Deadline (default 20 seconds). In this case, the system only accepts payments instructions with payment date (**IntrBkSttlmDt**) equal to T-1 is 00:00:20.

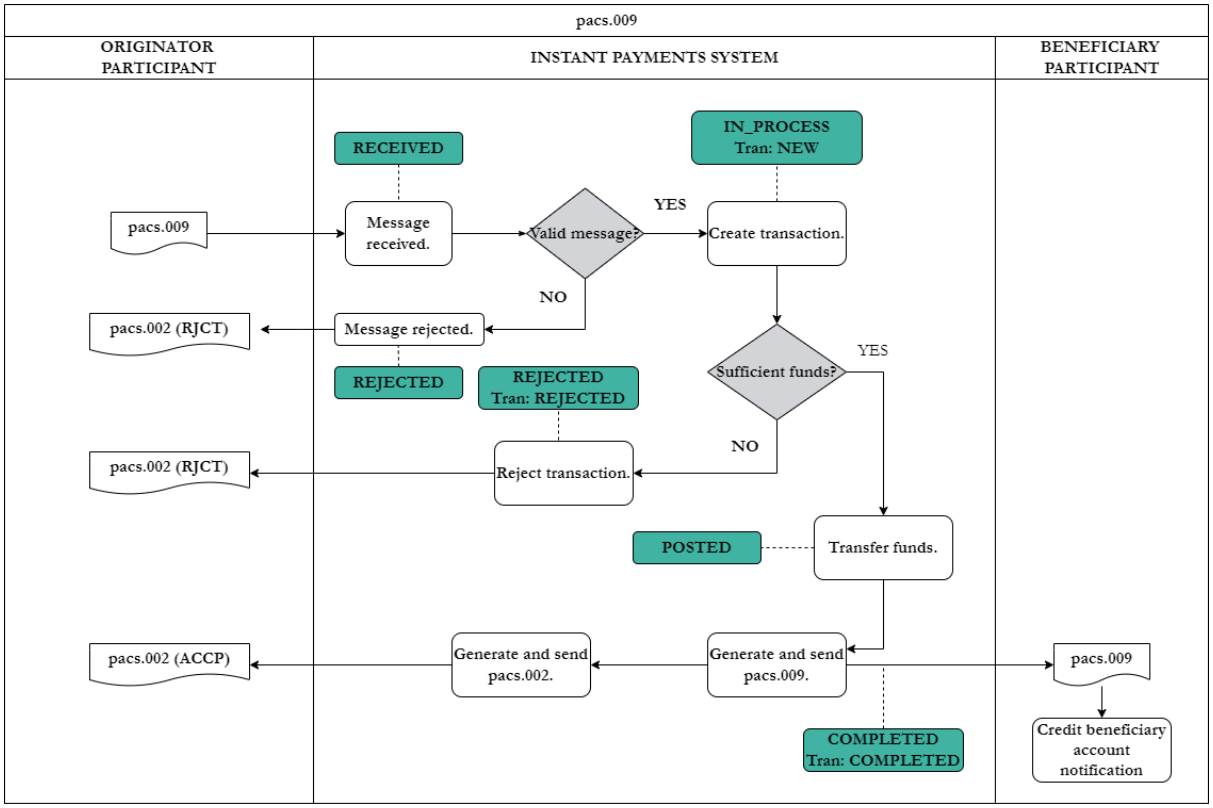


FIGURE 10. STATUS TRANSITION FLOW OF INSTANT PACS.009 PAYMENT MESSAGE

3.2.3. Payment Return/Positive Answer to Request for Recall Message Validation – pacs.004.001.13

The IPS's validation process for the received pacs.004 payment messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation.
4. Message business fields' validation:
    a. **TtlIntrBkSttlmAmt** – payment amount and currency for Instant transactions. These must be valid according to the predefined payment schema.
    b. **IntrBkSttlmDt** – payment date, must be the current calendar day (exceptions for Instant transactions is described in the note from section 4.2.1. – Credit Transfer/Instant Credit Transfer Message Validation pacs.008).
    c. Static message fields: **ClearingSystem**, **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes**.
    d. **InstgAg**t – BIC of sender Participant. It must identify an ACTIVE Participant in the system. This BIC must identify the sender Participant detected at the sending channel.
    e. **DbtrAgt** (from OrgnlTxRef) – BIC of debtor Participant (original). This must identify an ACTIVE Participant and not blocked for credit.
    f. **CdtrAgt** (from OrgnlTxRef) – BIC of creditor Participant (original). This must be equal to **InstAgt** for direct connection participants or to one of the sender's indirect participants, ACTIVE and not blocked for debit.
    g. **RtrdIntrBkSttlmAmt** –values less or equal to the ones in **TtlIntrBkSttlmAmt**.
    h. **DbtrAcct** and **CdtrAcct** (from OrgnlTxRef) – IBAN codes must be valid: structure and checksum (ISO 7064). Checksum validation is done only if System Parameter is set.
    i. The code of the Instititution that generated the reply message filled in field **BICFI** must be equal to **CdtrAgt**.
    j. Reason Code – only FOCR code is allowed for Instant transactions.
5. Duplicate message verification. For this purpose, the IPS compares the message reference (field **MsgId**) with all references of messages that the system received from the same Participant (Creditor Agent) during the last 24 hours for instant transactions. Also the item

reference (field **RtrId**) is compared with all item references that the system received from the same Participant during the last 24 hours.

6. Validation of digital signature.

During this validation process, the IPS system reports only the first detected error by replying a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

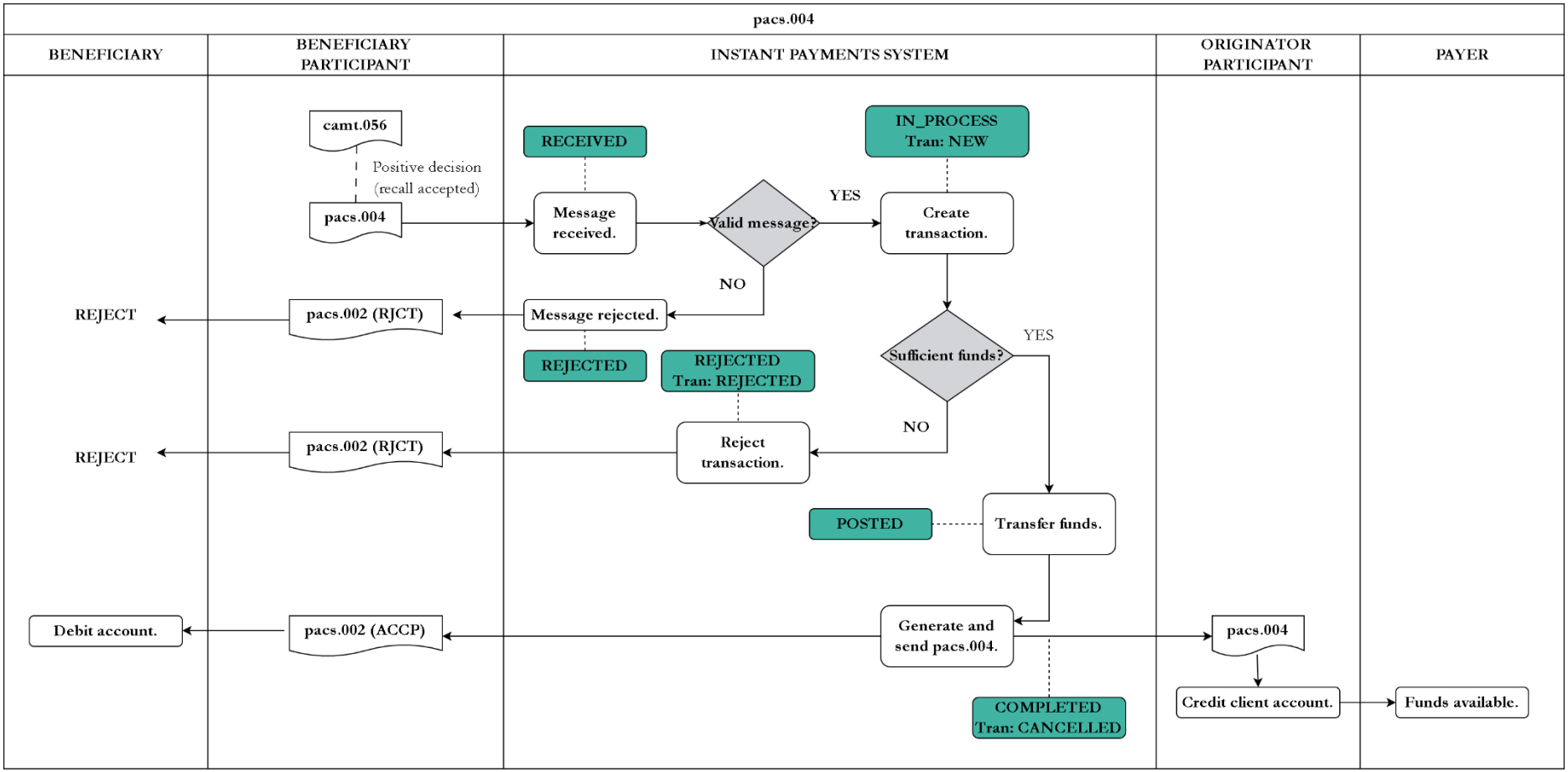


FIGURE 11. STATUS TRANSITION FLOW OF PACS.004 PAYMENT MESSAGE

3.2.4. Request for Recall Message Validation – camt.056.001.11

The IPS's validation process for the received camt.056 payment messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation.
4. If the beneficiary participant is not online at the moment of validation, the transaction is rejected.
5. Message business fields' validation:
    a. Static message fields: **ClearingSystem**, **ServiceLevel**, **LocalInstrument– will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes**.
    b. **Reason for Cancellation** – **will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes – Recall Reasons**.
    c. **Assigner** – BIC of sender Participant. It must identify an ACTIVE Participant in the system. This BIC must identify the sender Participant detected at the sending channel.
    d. **Assignee** – IPS's BIC.
    e. **OrgnlIntrBkSttlmDt** – date of original payment. It must fall within the parameters of the payment schema. The following validations are performed:
        i. **OrgnlIntrBkSttlmDt** must not be in the future.
        ii. **OrgnlIntrBkSttlmDt** must not be older than the current date minus the timeout defined in payment schema for the recall reason specified in the message (FRAD, DUPL, other).
    f. **DbtrAgt** (from OrgnlTxRef) – BIC of debtor Participant (original). This must be equal to **Assigner** for direct connection participants or to one of the sender's indirect participants.
    g. **CdtrAgt** (from OrgnlTxRef) – BIC of creditor Participant (original). This must identify an ACTIVE Participant.
    h. **DbtrAcct** and **CdtrAcct** (from OrgnlTxRef) – IBAN codes must be valid: structure and checksum (ISO 7064). Checksum validation is done only if System Parameter is set.

i. The code of the Institution that generated the reply message filled in field **BICFI** must be the same as the one filled in field **DbtrAgt**.

6. Duplicate message verification. For this purpose, the IPS system compares the item/message reference (field **Id**) with all references of messages that the system received from the same Participant (Debtor Agent) during the last 24 hours for Instant transactions. Also the item reference (field **CxlId**) is compared with all item references that the system received from the same Participant during the last 24 hours.
7. Validation of digital signature.

During this validation process, the IPS system reports only the first detected error by replying with a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

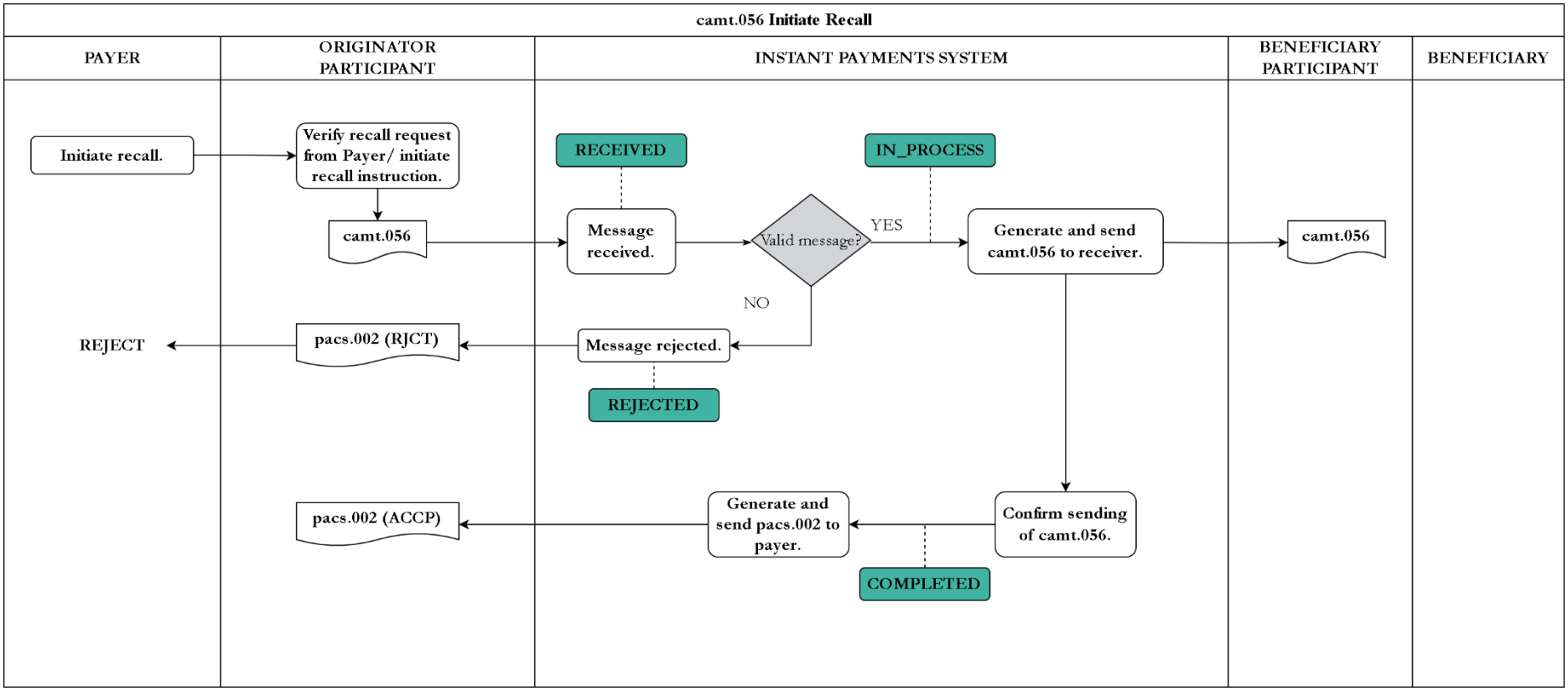


FIGURE 12. STATUS TRANSITION FLOW OF CAMT.056 PAYMENT MESSAGE

3.2.5. Negative Answer to Request for Recall Message Validation in case of camt.056;– camt.029.001.13

The IPS's validation process for the received camt.029 payment messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation.
4. Message business fields' validation:
    a. Static message fields: **ClearingSystem**, **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes**.
    b. OrgnlMsgNmId (from OrgnlGrpInfAndSts) **–** fixed text "camt.056.001.11".
    c. **Reason for negative answer** – – **will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes – Recall Nack Reasons** .
    d. **Assigner** – BIC of sender Participant. It must identify an ACTIVE Participant in the system. This BIC must identify the sender Participant detected at the sending channel.
    e. **Assignee** – IPS's BIC.
    f. **IntrBkSttlmDt** (from OrgnlTxRef) – date of original payment. Validated for recalls. It must fall within the parameters of the payment schema. The following validations are performed:
        i. **IntrBkSttlmDt** must not be in the future
        ii. **IntrBkSttlmDt** must not be older than the current date minus the timeout defined in payment schema for the recall reason specified in the message (FRAD, DUPL, other)
    g. **CdtrAgt** (from OrgnlTxRef) – BIC of creditor Participant (original). This must be equal to **Assigner** for direct connection participants or to one of the sender's indirect participants.
    h. **DbtrAgt** (from OrgnlTxRef)– BIC of debtor Participant (original). This must identify an ACTIVE Participant.
    i. **DbtrAcct** and **CdtrAcct** – IBAN codes must be valid: structure and checksum (ISO 7064). Checksum validation is done only if System Parameter is set.

j. The code of the Instititution that generated the reply message filled in field **TxInfAndSts/CxlStsRsnInf/Orgtr/Id/OrgId/AnyBIC** must be the same as the one filled in field **CdtrAgt**.

5. Duplicate message verification. For this purpose, the IPS system compares the message reference (field **Id**) with all references of messages that the system received from the same Participant (CreditorAgent) during the last 24 hours for Instant transactions. Also the item reference (field **CxlStsId**) is compared with all item references that the system received from the same Participant during the last 24 hours.

6. Validation of digital signature.

During this validation process, the IPS system reports only the first detected error by replying with a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

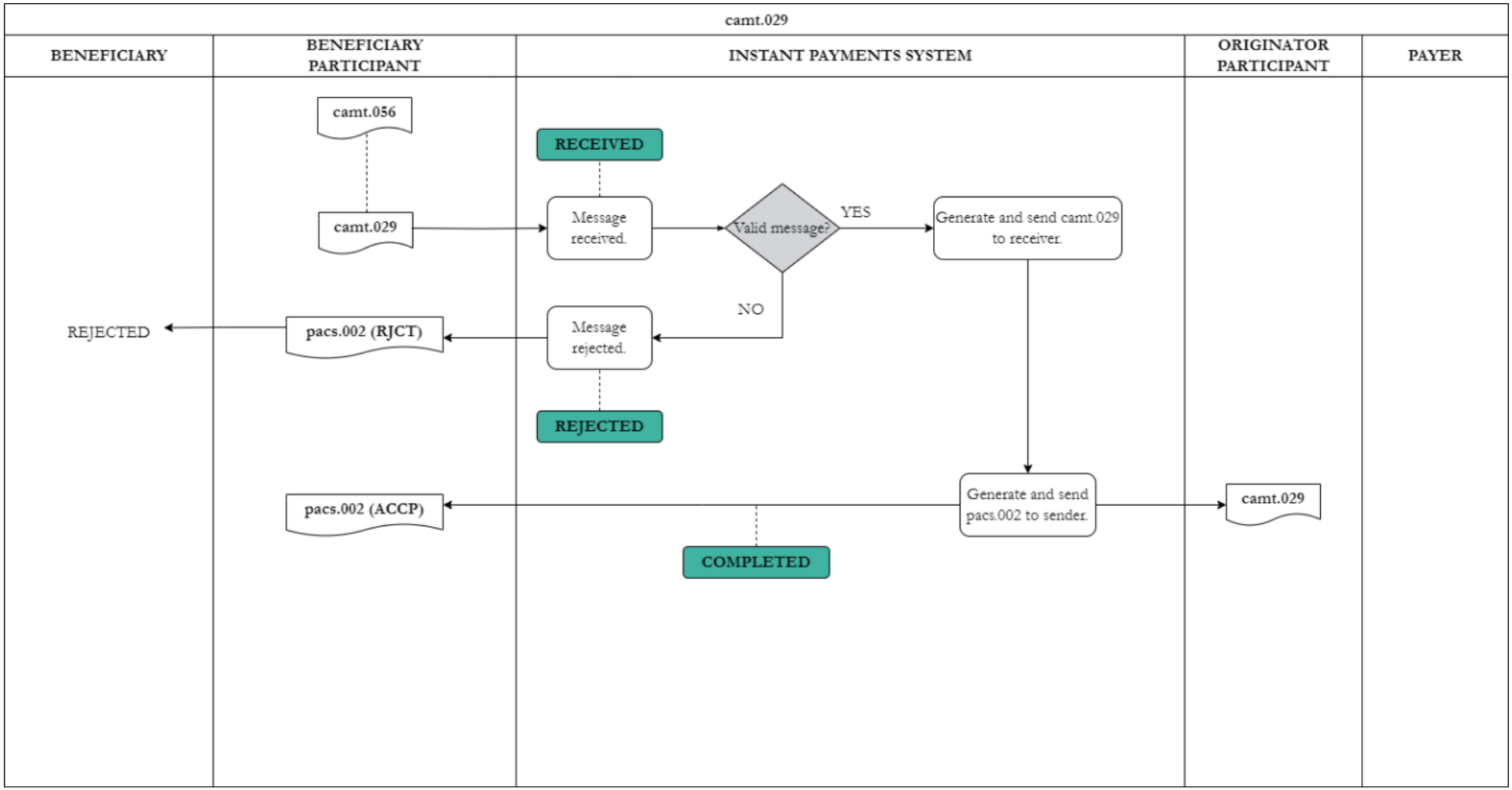


FIGURE 13. STATUS TRANSITION FLOW FOR CAMT.029 – NEGATIVE ANSWER FOR RECALL.

3.2.6. Negative/Positive Answer to Request for Cancellation in case of camt.055 for pain.013 or pain.001– camt.029.001.13

The IPS's validation process for the received camt.029 payment messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation.
4. Message business fields' validation:
    a. Static message fields: **ClearingSystem**, **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes**.
    b. **OrgnlMsgNmId** (from OrgnlGrpInfAndSts) **–** fixed text "pain.013.001.11" or 'pain.001.001.012'.
    c. **Conf** (from Sts) – set to CNCL (positive answer to request for cancellation) or RJCR (negative answer to request for cancellation, negative answer to recall)
        i. If the status is CNCL, then the original RTP will also be moved to CANCELLED status in the MMC.
    d. **Assigner** – BIC of sender Participant. It must identify an ACTIVE Participant in the system. This BIC must identify the sender Participant detected at the sending channel.
    e. **Assignee** – IPS's BIC.
    f. **CdtrAgt** (from OrgnlTxRef) – BIC of creditor Participant (original). This must be equal to **Assigner** for direct connection participants or to one of the sender's indirect participants.
    g. **DbtrAgt** (from OrgnlTxRef)– BIC of debtor Participant (original). This must identify an ACTIVE Participant.
    h. **DbtrAcct** and **CdtrAcct** – IBAN codes must be valid: structure and checksum (ISO 7064). Checksum validation is done only if System Parameter is set.
5. Duplicate message verification. For this purpose, the IPS system compares the message reference (field **Id**) with all references of messages that the system received from the same Participant (CreditorAgent) during the last 24 hours for Instant transactions. Also the item reference (field **CxlStsId**) is compared with all item references that the system received from the same Participant during the last 24 hours.
6. Validation of digital signature.

During this validation process, the IPS system reports only the first detected error by replying with a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

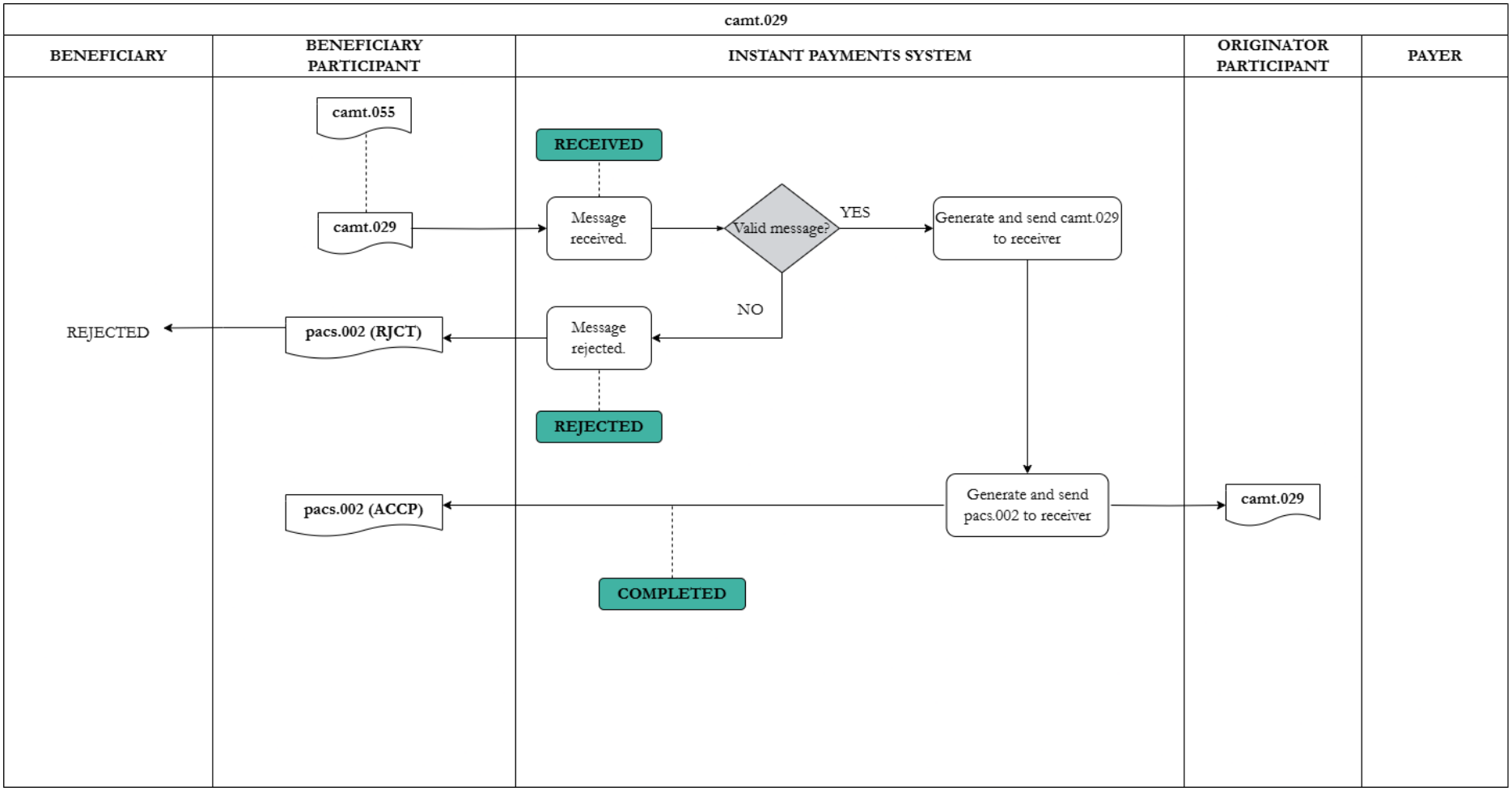


FIGURE 14. STATUS TRANSITION FLOW FOR CAMT.029 - RESPONSE TO REQUEST FOR CANCELLATION

3.2.7. Request to Pay Message Validation – pain.013.001.11

This message is to collect funds from a debtor by a creditor entity. The IPS's validation process for the received pain.013 payment messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation.
4. Validate message reference. The reference must start with the current date in the format YYYYMMDD. This rule was done as an optimisation in the RTP flow. The payment is not rejected even if slow RTP has expired.
5. Message business fields' validation:
    a. Static message fields: **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes**.
    b. **InitgPty**– BIC of sender Participant. It must identify an ACTIVE Participant in the system.
    c. **ReqdExctnDt** – requested execution date.
    d. **XpryDt** – expiration date, **either DtTm or Dt is allowed**; Used to update status of RTP to expired if no reply from the receiver participant is processed until this date.Despite the expiration of the (slow) RTP, payment followed RTP is not rejected by the system.
    e. **DbtrAgt**– BIC of debtor Participant. This must identify an ACTIVE participant.
    f. **CdtrAgt**– BIC of creditor Participant. This must be equal to the **InitgPty** for direct connection participants or to one of the sender's indirect participants.
    g. **Id** (Cdtr – Id – OrgId – Othr or Cdtr – Id – PrvtId - Othr) – creditor identification; combined with corresponding **Cd** (Cdtr – Id – OrgId – Othr – SchmeNm or Cdtr – Id – PrvtId – Othr - SchmeNm). If one of OrgId/Othr or PrvtId/Othr and the corresponding SchmeNm/Cd tag exists and is set to "BDID", then IPS will interpret that the value of **Id** is the Merchant Category Code, otherwise no additional validation is performed. For each RTP, IPS parses the MCC code, and if it exists it validates it according to the list maintained in MMC by the Operator.
    h. **DbtrAcct** and **CdtrAcct**– IBAN codes must be valid: structure and checksum (ISO 7064). Checksum is validated according to System Parameter configured by Operator.
    i. **InstrPrty (**PmtInf – PmtTpInf**) -** to indicate either the fast or slow RTP flow (presented in the diagrams below); according to schema the field has only two

possible values: HIGH (used to indicate the RTP fast flow) and NORM (used to indicate the RTP slow flow).

6. Duplicate message verification. For this purpose, the IPS system compares the item/message reference (field **MsgId**) with all references of messages that the system received from the same Participant (CreditorAgent) during the last 24 hours for Instant transactions. Also the item reference (field **PmtInfId**) is compared with all item references that the system received from the same Participant during the last 24 hours.
7. Validation of digital signature.
8. Timestamp validation
    a. Late initiation message – For the fast flow; the system checks if the time in the field **Creation Date Time** (AT-50) is not exceeded by the current processing time with more than the **Initiation Deadline** parameter configured in the payment schema. This check is done to allow enough time for the originator to initiate the payment within the SLA.

During this validation process, the IPS system reports only the first detected error by replying with a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

The **processing of a RTP fast flow** (i.e. payment at a physical merchant) contains the following steps:

1. The beneficiary initiates a request to pay through its bank's interface.
2. The bank sends a pain.013 message to IPS and waits for a synchronous response (either pacs.002 or pain.014).
3. IPS performs the validation steps described in this chapter. In case of validation failure, a pacs.002 message with the status is generated for the beneficiary participant.
4. In case of successful validation, IPS forwards the pain.013 message to the payer's bank.
5. The bank performs an initial validation of the message (existing account, etc.). In case of failure, it sends a pain.014 to IPS for which it receives a pacs.002 (delivery confirmation). IPS forwards the final pain.014 to the beneficiary participant, as a reply to the original request, which notifies the client.
6. If the message is valid, the originator participant presents RTP to the customer to accept or decline the request to pay. In case of decline, a pain.014 message is generated by the originator. It sends the pain.014 to IPS for which it receives a pacs.002 (delivery confirmation). IPS forwards the final pain.014 to the beneficiary participant as a reply to the original request, which notifies the client.
7. If the customer accepts the RTP, then the originator participant sends a pacs.008 and the Instant Credit Transfer flow as described in section 3.2.1 is executed. At any time after acceptance of Request to Pay, the originator participant must send a pain.014 message to indicate that the RTP was accepted, but it's not part of the synchronous flow for

performance reasons. The pain.014 flow are described in section 3.2.8 Answer to Request to Pay Message.

8. Upon the completion of the Instant Credit Transfer flow, IPS will generate a pacs.002 with the payment status as a reply to the original pain.013 request.
9. If the Fast RTP timeout defined in the Payment Schema has passed and there is no reply from the originator participant, then the pain.013 is marked as cancelled and a pacs.002 status message is generated for the beneficiary participant. If the payment is still in progress, then the expiration timer will wait until completion to generate the status message, which is then generated only in case of payment failure (not to report an RTP expiration if the payment is completed at the same time).
10. If the fast RTP is cancelled due to timeout, payments initiated afterwards for that RTP will be rejected by IPS.

The **processing of RTP messages (slow flow)** contains the following steps:

1. The beneficiary initiates a request to pay through its bank's interface.
2. The bank sends a pain.013 message to IPS.
3. IPS performs the validation steps described in this chapter.In case of validation failure, a pacs.002 message with the status is generated for the beneficiary participant.
4. In case of successful validation IPS forwards the pain.013 message to the payer's bank for the presentment to the payer and generates a pacs.002 for the beneficiary bank to confirm that RTP was forwarded successfully.
5. The originator participant based on acceptance/refusal of the payer sends a rejection (pain.014), or an acceptance (pain.014)) and the payment immediately or later (pacs.008). The pain.014 flows are described in section 3.2.8 Answer to Request to Pay Message.

RTP Statuses

The IPS keeps track of the statuses of RTP messages. For the slow flow this tracking is performed only in MMC. For the fast flow, the RTP tracking is also performed on PM, to identify initial RTP in case of payment and to cancel the RTP automatically.

RTP messages have 2 separate statuses: one for the RTP message itself and one for the payment based on RTP.

SLOW RTP

After the message is validated, it will move into either REJECTED (didn't pass validation) or SENT(valid and forwarded to receiver participant). If the originator participant does not reply in the interval specified in XpryDt, then the RTP is moved in status EXPIRED..

If the originator participant replies with pain.014 "reject", then the RTP status will be updated to REFUSED.

If the the originator participant replies with pain.014 “accept”, then RTP status will be updated to ACCEPTED.

If the RTP is cancelled through a camt.055 Cancellation Request then it will be updated to status CANCELLED.

The originator can send one or multiple payments for the RTP and the status will be updated to PAID or PAID_PART, depending on the total amount. Despite the RTP message expiration, based on that RTP executed payments should not be rejected by IPS.

RTP messages have separate statuses regarding Payments followed by RTP: If the full amount is paid, then RTP status will be updated to PAID; or if the full amount is not paid, the status will be updated to PAID_PART.

Fast RTP:

For the fast flow, due to strict SLAs, only the following statuses are possible HOLD (RTP is being processed), REJECTED (invalid message, REFUSED/ACCEPTED (negative/positive pain.014), EXPIRED (timeout defined in Payment Schema has passed without reply).

RTP messages have a separate status regarding Payments followed by fast flow RTP: PAID (the amount is fully paid positive answer flow.

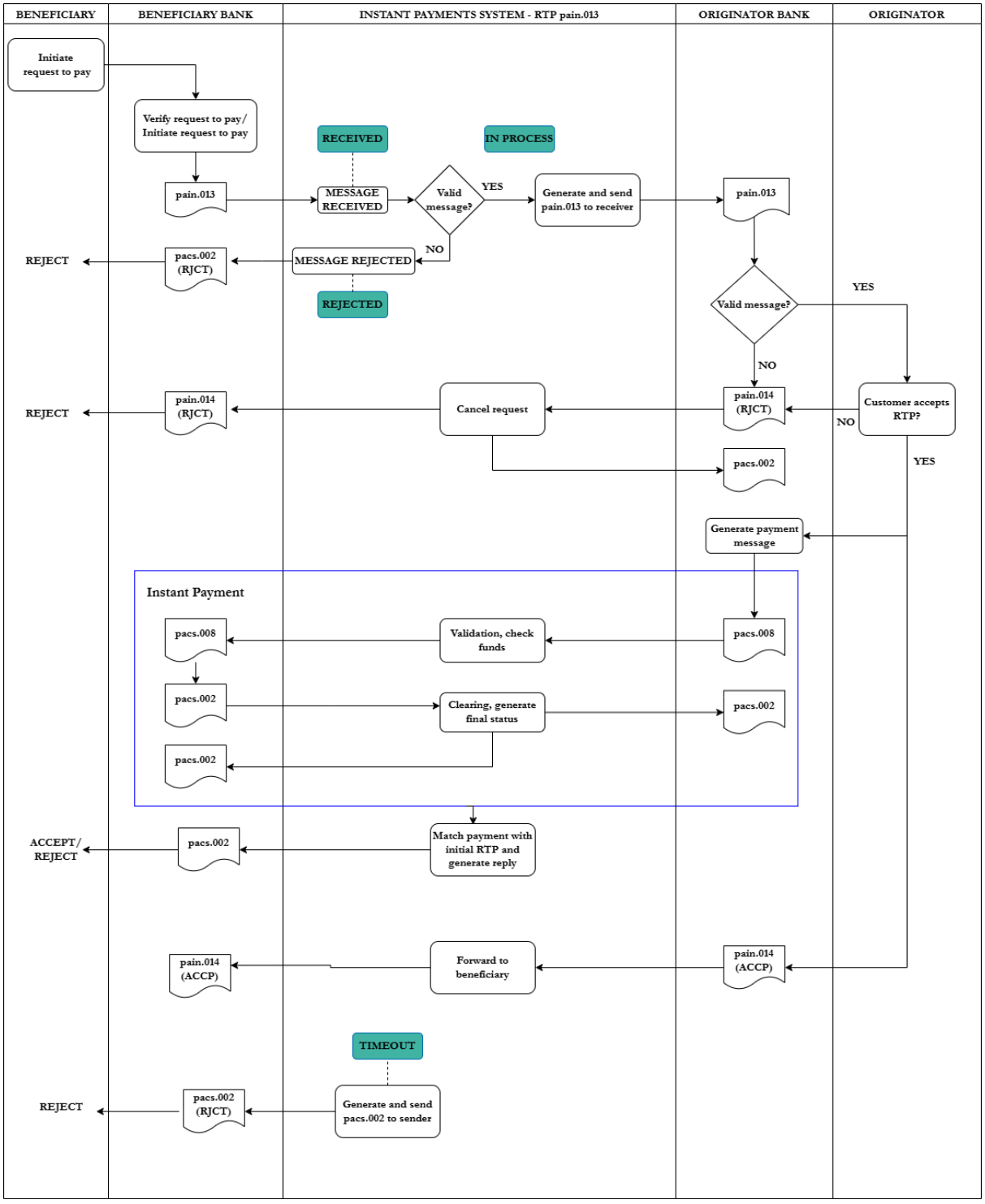


FIGURE 15. STATUS TRANSITION FLOW FOR RTP FAST FLOW

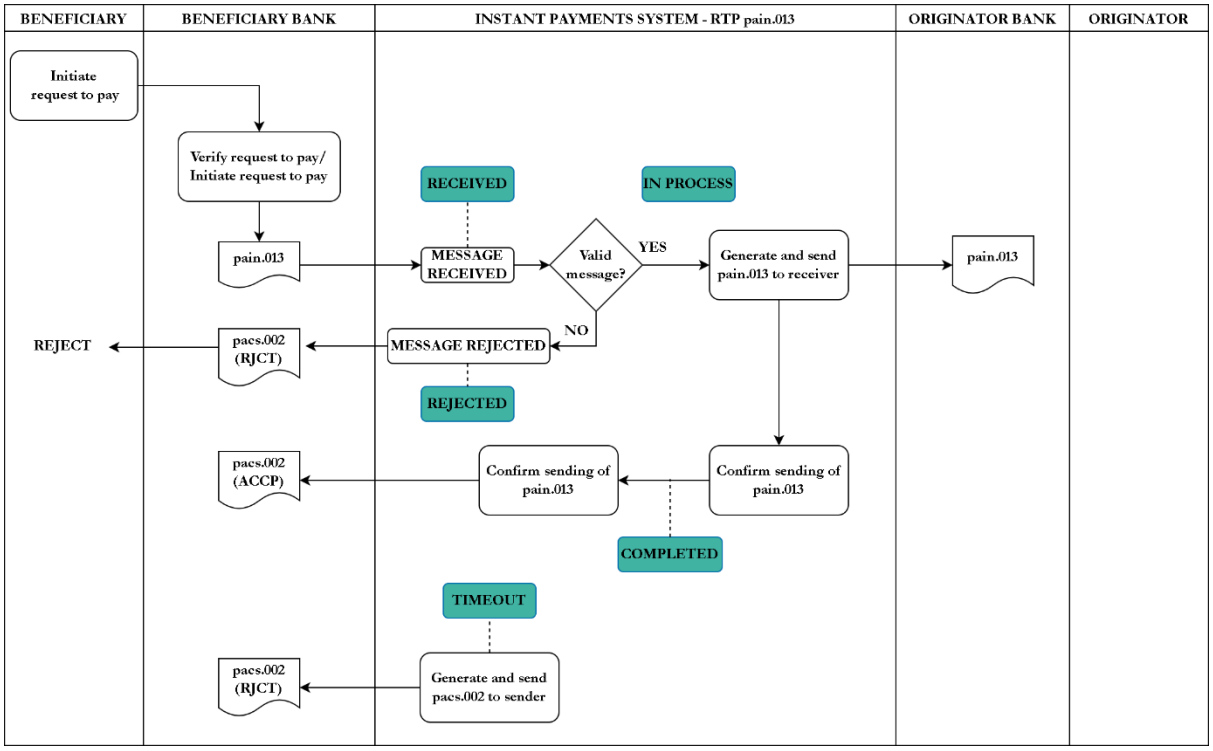


FIGURE 16. STATUS TRANSITION FLOW FOR RTP SLOW FLOW

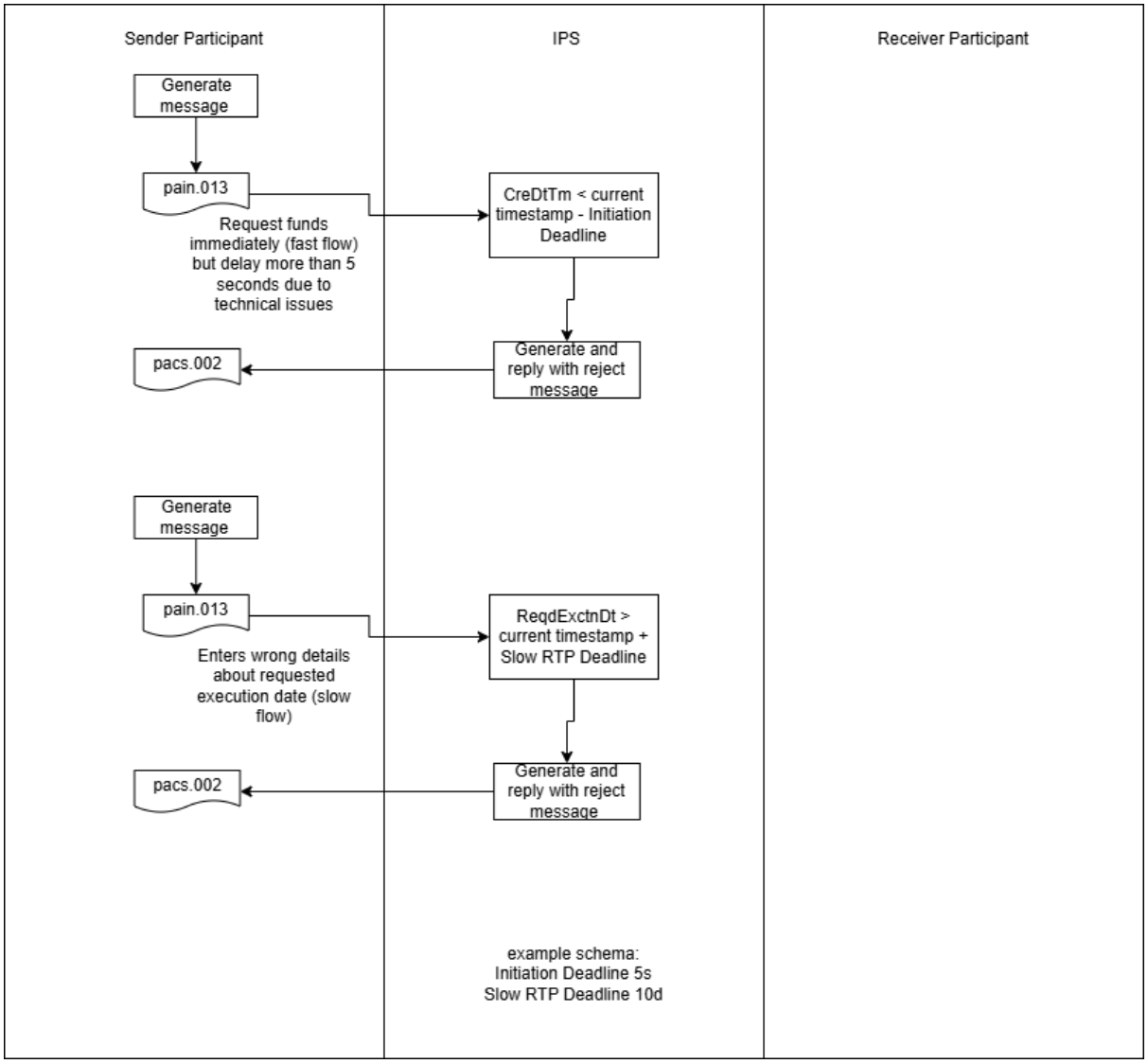


FIGURE 17. TIMEOUTS FOR PAIN.013 MESSAGE

3.2.8. Answer to Request to Pay Message Validation – pain.014.001.11

The IPS's validation process for the received pain.014 payment messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation.
4. Message business fields' validation:
    a. Static message fields: **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes**.
    b. **InitgPty** – BIC of sender Participant. It must identify an ACTIVE participant in the system. The BIC must identify the sender Participant detected at the sending channel.
    c. **OrgnlMsgId** (from OrgnlGrpInfAndSts) – message id of original request to pay.
    d. **OrgnlMsgNmId** (from OrgnlGrpInfAndSts) – fixed text "pain.013.001.11".
    e. **OrgnlCreDtTm** (from OrgnlGrpInfAndSts) – date of original request to pay.
    f. **TxSts –** reported status for the initial request to pay; use ACCP or RJCT. The information related to RTP reject is extracted from the combination of TxSts with "RJCT" value and the presence of TxInfSts - StsRsnInf - Rsn - Cd for the reason.

       In case of accept, for accept now / pay now the payer participant sends the pacs.008 directly followed by pain.014.

       In case of accept now / pay later the information is extracted from the TxSts with "ACCP" value and the payee can check the Acceptance Date Time (TxInfAndSts - AccptncDtTm) proposed by the payer.
    g. **Cd** (from TxInfSts > StsRsnInf) – use an error code if the TxSts is RJCT, as in the Error codes annex at the end of this document.
    h. **InstdAmt** - value equals to the ones in the original request to pay (fast flow).

       No validation is performed for this tag in the slow flow, besides XML schema.
    i. **ReqdExctnDt**:**either DtTm or Dt is allowed;**

       For the fast flow, value equals to the one in the original request to pay;

       No validation is performed for this tag in the **slow flow**, besides XML schema**.**
    j. **XpryDt either DtTm or Dt is allowed;**

For the fast flow, value equals to the one in the original request to pay.

No validation is performed for this tag in the **slow flow**, besides XML schema.

k. **Ustrd -** value equals to the ones in the original request to pay (**fast flow**).

No validation is performed for this tag in the **slow flow**, besides XML schema.

l. **DuePyblAmt** – value equals to the ones in the original request to pay (**fast flow**).

No validation is performed for this tag in the **slow flow**, besides XML schema.

m. **DbtrAgt** – BIC of debtor Participant (original). This must be equal to the **InitgPty** for direct connection participants or to one of the sender's indirect participants**CdtrAgt** – BIC of creditor Participant (original). This must identify an ACTIVE

n. Participant.

a. **Id** (Cdtr – Id – OrgId – Othr or Cdtr – Id – PrvtId - Othr) – creditor identification; combined with **Cd** (Cdtr – Id – OrgId – Othr – SchmeNm or Cdtr – Id – PrvtId – Othr - SchmeNm). IPS will interpret Id as MCC if Cd is set to: "BDID" (value of id is the Merchant Category Code). If Cd is not set or with a different value then no additional validation is performed for this tag.**DbtrAcct** and **CdtrAcct** – IBAN codes must be valid: structure and checksum (ISO 7064). Checksum validation is done only if System Parameter is set.

5. Duplicate message verification. For this purpose, the IPS system compares the item/message reference (field **MsgId**) with all references of messages that the system received from the same Participant (DebtorAgent) during the last 24 hours for Instant transactions.

6. Validation of digital signature.

During this validation process, the IPS reports only the first detected error by replying with a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

If any of the answers to a RTP is negative, the initial RTP is marked as REJECTED and all future Credit Transfers related to it will be rejected.

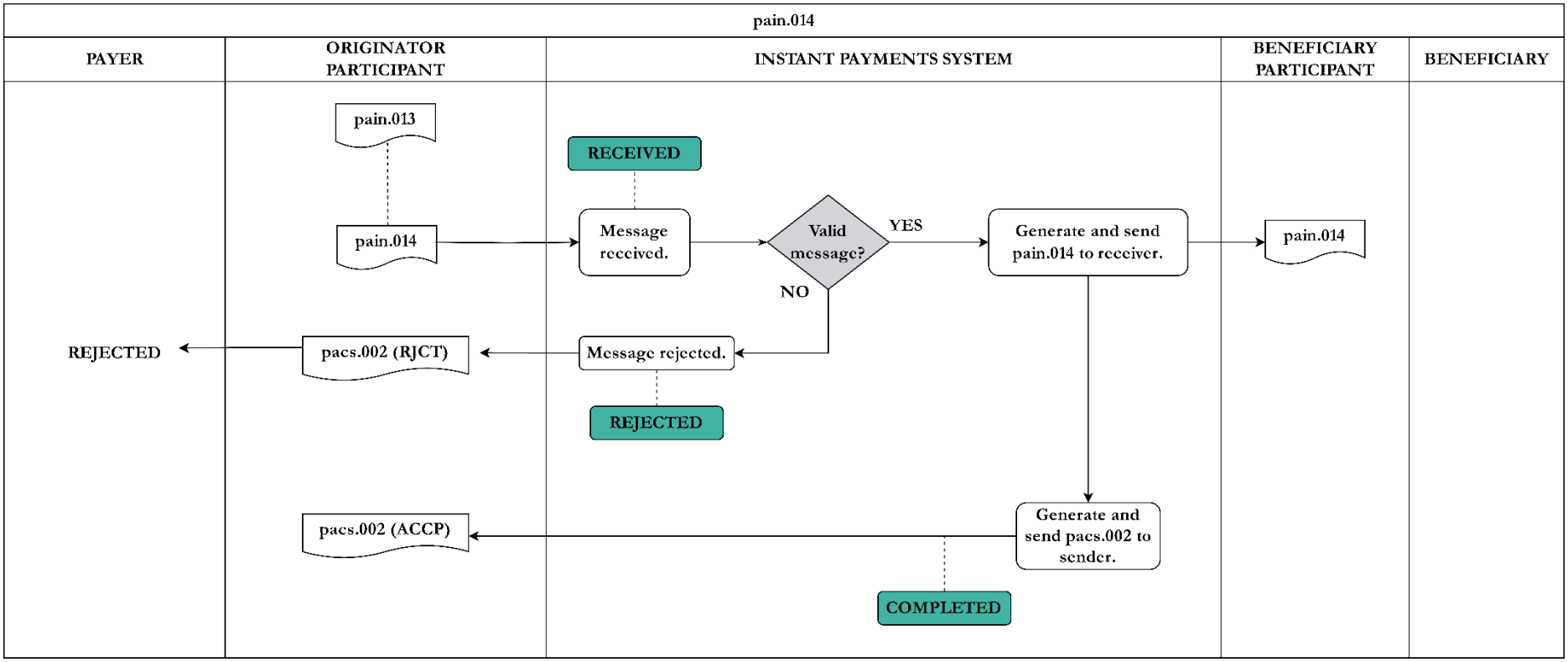


FIGURE 18. STATUS TRANSITION FLOW OF PAIN.014 MESSAGE

3.2.9. Investigation Message Validation – pacs.028.001.06

Investigation message can be used for Instant Credit Transfer, Recall and Request to Pay.

The IPS's validation process for the received pacs.028 payment messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation.
4. There are 3 main flows for this message, based on its target: pacs.008, camt.056 or pain.013. The participant asks the central system about an in-process transfer or it asks the original creditor bank why it has not returned the funds as requested in a camt.056 recall, or why it has not initiated a payment as requested in a pain.013 RTP.
5. For pacs.008: If the original transaction does not exist the investigation is rejected with error code AG09 (internal 1016). If the original transaction is still being processed then the investigation is rejected with error code AG09 (internal 1017). If timeout occurs in communication with main database (only needed for rejects), the investigation request is rejected with HTTPS error code 500. The investigation message should be sent from participant after the deadline for confirmation message receipt, of 9 seconds.
6. Message business fields' validation:
    a. Static message fields (PmtTpInf): **ServiceLevel, LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes.**
    b. **InstgAg**t – BIC of sender Participant. It must identify an ACTIVE participant in the system. This BIC must identify the sender Participant detected at the sending channel.
    c. **OrgnlMsgId** (from OrgnlGrpInfAndSts) – – when sent for a pacs.008, it must identify a pacs.008 message generated by Instructing Agent. The transaction (pacs.008) is based on this reference and it verifies its status. If the IPS does not find the corresponding transaction, then the message is rejected.

       When sent for a camt.056 or pain.013 the system will forward the query to the receiver party.
    d. **OrgnlMsgNmId** (from OrgnlGrpInfAndSts) –fixed text "pacs.008.001.12", "camt.056.001.11" or "pain.013.001.11".
    e. **Original Transaction ID** –must be equal with the original transaction reference.
    f. The BIC of the institution that generated the reply message is equal to **InstgAgt.**

g. **DbtrAgt** (from OrgnlTxRef) – BIC of debtor Participant (original). This must be equal to **InstgAgt** for direct connection participants or to one of the sender's indirect Participants.

h. **CdtrAgt** (from OrgnlTxRef) – BIC of creditorParticipant (original). This must identify an ACTIVE participant if sent for camt.056 or pain.013.

   This information is not validated for pacs.008 since the message is not forwarded to original creditor. The combination of sender, reference and time is enough to identify the original transaction and its status.

i. **InstrPrty (from PmtTpInf) –** must be present for pain.013 investigation to identify fast/slow flow.

7. Timestamp validation, expired message – when sent for a pacs.008, the system checks if the time in the field **Acceptance Date Time** (AT-50) is equal to the one in the original pacs.008 message. The system validates that the timestamp from the original pacs.008 is the same as the timestamp declared for the original payment in pacs.028 message. This helps prevent mismatch of transactions since transaction id uniqueness is enforced for a limited interval (last 24h).

8. Validation of digital signature.

9. Duplicate message verification. For this purpose, the IPS compares the message reference (field **MsgId**) with all references of same type messages that the system received from the same Participant (DebtorAgent) during the last 24 hours for Instant transactions. Also the item reference (field **PmtInfId**) is compared with all item references that the system received from the same Participant during the last 24 hours.

10. When sent for a pacs.008, IPS must have successfully received and processed within the last 24 hours the pacs.008 message (payment instruction) referred to in the pacs.028 message. If not, IPS will reply a pacs.002 message with code RJCT and error code AG09 (internal code 1016). If the related type is camt.056 or pain.013 the message will be forwarded to the CdtrAgt specified.

During this validation process, the IPS reports only the first detected error by replying a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

The flow below is based on the EPC Rulebook flow.

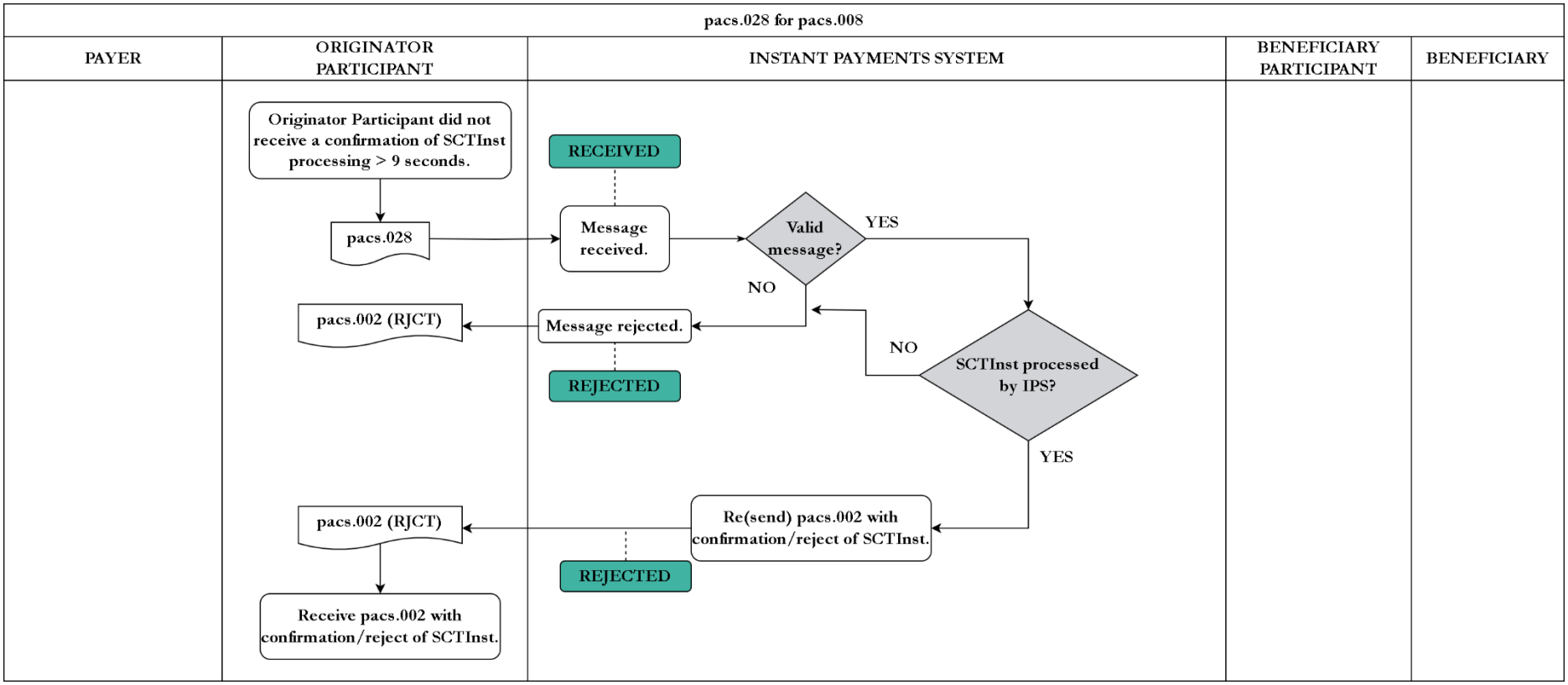


FIGURE 19. STATUS TRANSITION FLOW OF PACS.028 MESSAGE FOR PACS.008

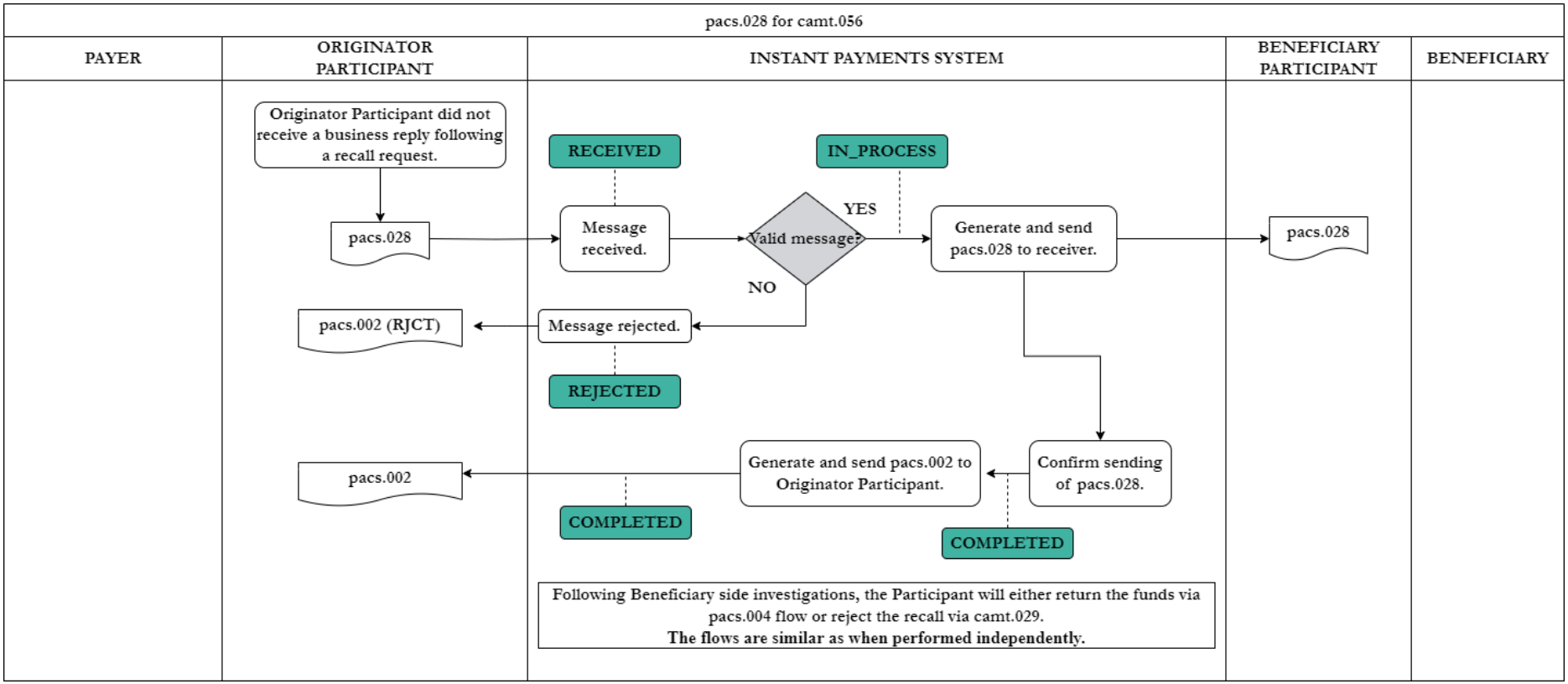


FIGURE 20. STATUS TRANSITION FLOW OF PACS.028 MESSAGE FOR CAMT.056

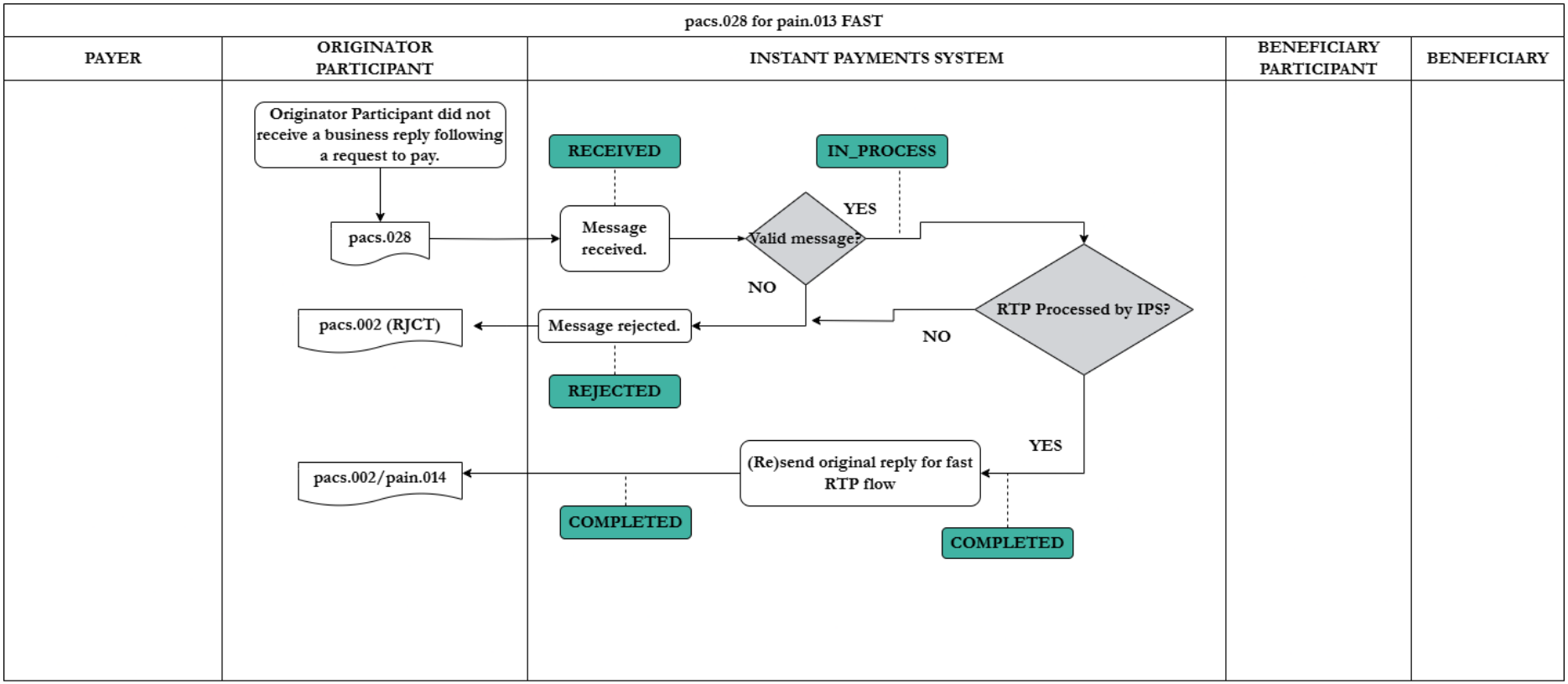


FIGURE 21. STATUS TRANSITION FLOW OF PACS.028 MESSAGE FOR FAST RTP

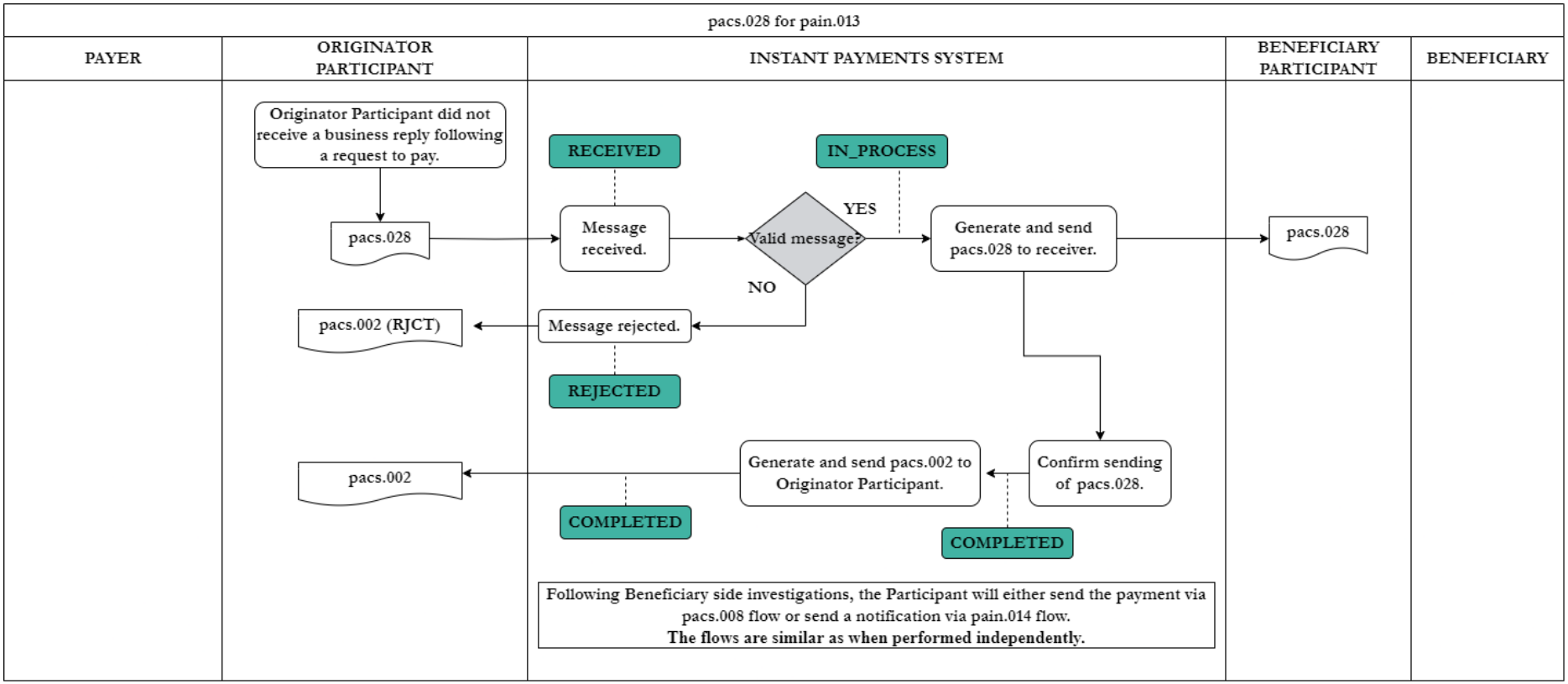


FIGURE 22. STATUS TRANSITION FLOW OF PACS.028MESSAGE FOR SLOW RTP

3.2.10. Payment Confirmation/Rejection Message – pacs.002.001.14

This section describes two scenarios:

A. The validation of pacs.002 messages received by IPS from Participants, which only applies to the status of an instant credit transfer (pacs.008 flow).

B. The generation of pacs.002 messages by IPS and sending these to the Participants.

A. The IPS's validation process for the received pacs.002 payment confirmation/rejection messages needed for the processing of Instant Credit Transfers (pacs.008) from Participants follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message (ReplyMessage), as described in part B of this section.
3. Message business fields' validation:
    a. **InstgAg**t – BIC of sender Participant. It must identify an ACTIVE Participant in the system. This BIC must identify the sender Participant detected at the sending channel.
    b. **OrgnlMsgId** (from OrgnlGrpInfAndSts) – – must identify a pacs.008 message generated by the system and sent to receiver Participant. The transaction processing (pacs.008) is based on this reference (OrgnlGrpInfAndSts - OrgnlMsgId) and it verifies its status. If the IPS does not find the corresponding transaction, then the message is rejected.The reference is the message id (GrpHdr - MsgId) of the original pacs.008 message and it is generated and tracked by the IPS system.
    c. **OrgnlMsgNmId** (from OrgnlGrpInfAndSts) – fixed text "pacs.008.001.12".
    d. **Original Transaction Reference**– validation with the original transaction reference.
    e. Static message fields (PmtTpInf): **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes.**
    f. **DbtrAgt** (from OrgnlTxRef) – BIC of debtor Participant (original). This must be equal to **the one from the original pacs.008**.
    g. **IntrBkSttlmDt** – original payment date, must fall within the payment schema's paramaeters.
    h. The BIC of the instititution that generated the reply message is equal to **the original CdtrAgt.**
    i. Group Status and Tran Status – ACCP or RJCT.

j. Reason code – according to the ISO20022 schema, **will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes – Reject Reasons.**

4. Timestamp validation, expired message – when a pacs.002 is sent by a participant as a reply for pacs.008 , the system checks if the time in the field **Acceptance Date Time** (AT-50) is equal to the one in the original message.
5. Validation of digital signature.

During this validation process, the IPS reports only the first detected error by replying a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

This confirmation or rejection message (pacs.002) of a received pacs.008 payment instruction can be sent several times by the payment receiver Participant, in case the IPS's reply message for the message processing is not received or processed by the receiving Participant, as described in the breakdown below, step 5.

The processing of a pacs.002 ConfirmationMessage received by the IPS from a Participant for a pacs.008 follows the steps:

1. Message validation, including the authentication of the referred transaction.
2. If the referred instruction (pacs.008) has WAIT_RECEIVER status, the system processes the transaction according to the reply received from the receiver bank (ACCP or RJCT).
3. The IPS generates and sends a pacs.002 ReplyMessage to the receiver bank, which entails the transaction status:
    a. ACCP for a completed transaction, or
    b. RJCT for a cancelled transaction (including because of timeout cause, e.g., if the pacs.002 ConfirmationMessage is received after the expiration of the timeout parameter).
    c. Error code if it is the case.
4. The system generates the pacs.002 ReplyMessage to the sender Participant at the moment of transaction completion (COMPLETE or CANCELLED).
5. In case the receiver Participant does not receive the IPS generated message from step 3, it can send pacs.002 ConfirmationMessage again, in which case the IPS will process the message executing only steps 1 and 3, 2 and 4 being executed after the system received the initial pacs.002 message.

B. IPS generates and replies with pacs.002 messages for the following flows:

- Pacs.008 – either a validation error or the final status of the transaction (details forwarded from Beneficiary Participant message if they replied)
- Pacs.004 – either a validation error or the technical acceptance
- Pacs.009 - either a validation error or the technical acceptance
- Camt.056 - either a validation error or the technical acceptance
- Camt.055 - either a validation error or the technical acceptance
- Camt.029 - either a validation error or the technical acceptance
- Pain.013 slow flow – either a validation error or the technical acceptance
- Pain.013 fast flow – either a validation error or the final status of the transaction
- Pain.002 – either a validation error or the technical acceptance
- Pain.014 – either a validation error or the technical acceptance
- Pacs.002 – either a validation error or the final status of the transaction
- Pacs.028 for pacs.008 – either a validation error or the final status of the transaction
- Pacs.028 for camt.056 - either a validation error or the technical acceptance
- Pacs.028 for pain.013 - either a validation error or the technical acceptance
- Pain.001 – a validation error.

3.2.11. Payment Initiation – pain.001.001.012

A participant can be configured in MMC as a "Payment Initiator Service Provider" with a list of PISP Participants. That participant can send payment initiation messages (pain.001) instructing a participant from the PISP list to initiate a payment to another participant in the system. The PISP will receive synchronously a pain.002 with the status of the payment. If no payment or reply is made by the originator participant (the one who receives the initiation request) in the time period specified in the Payment Schema (Timeout Deadline), then the original pain.001 is marked as rejected by the IPS and a pain.002 notification is generated and sent to the PISP.

The IPS's validation process for the received pain.001 messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pain.002 message.
3. Business Application Header validation.
4. Message business fields' validation:
    a. **NbOfTxs** – value of this field should be 1
    b. Static message fields: **ServiceLevel**, **LocalInstrument, Payment Method, Charge Bearer – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes**.
    c. **InitgPty – BIC of sender Participant. It must identify an** ACTIVE PISP **Participant in the system. This BIC must identify the sender Participant detected at the sending channel.**
    d. **ReqdExctnDt** – requested execution date.
    e. **DbtrAgt** – BIC of debtor Participant. This must be equal to **a participant registered with the PISP**. The participant should be ACTIVE and connected to the system.
    f. **CdtrAgt**– BIC of creditor Participant. This must identify an ACTIVE Participant.
    g. **DbtrAcct** and **CdtrAcct** (from OrgnlTxRef) – IBAN codes must be valid: structure and checksum (ISO 7064). Checksum is validated according to System Parameter configured by Operator.
5. Duplicate message verification. For this purpose, the IPS compares the item/message reference (field **MsgId**) with all references of messages that the system received from the same Participant during the last 24 hours. Also the item reference (field **PmtInfId**) is compared with all item references that the system received from the same Participant during the last 24 hours.
6. Validation of digital signature.
7. Timestamp validation:

a. Late initiation message – the system checks if the time in the field **Creation Date Time** (AT-50) is not exceeded by the current processing time with more than the **Initiation Deadline** parameter configured in the payment schema. This check is done to allow enough time for the originator to initiate the payment within the SLA.

b. expired message – the system checks if the time in the field **Creation Date Time** (AT-50) is not exceeded by the current processing time with more than the **Timeout Deadline** parameter configured in the payment schema. After the initiation deadline validation, the application also runs a timer to check if the initiation is replied to before the timeout deadline and cancels it otherwise.

During this validation process, the IPS reports only the first detected error by replying a pain.002 message. The message is placed in REJECTED status and the processing is completed.

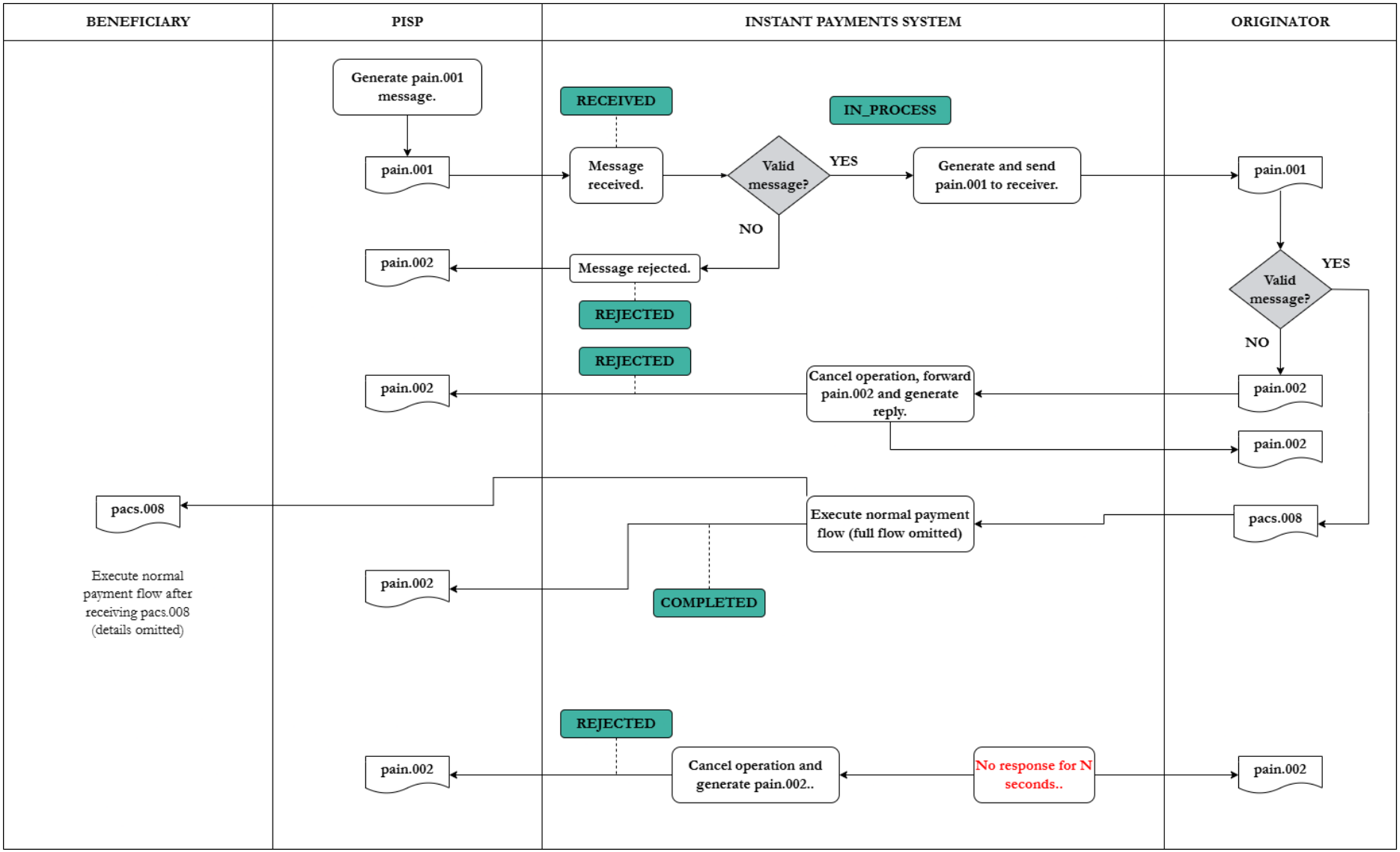
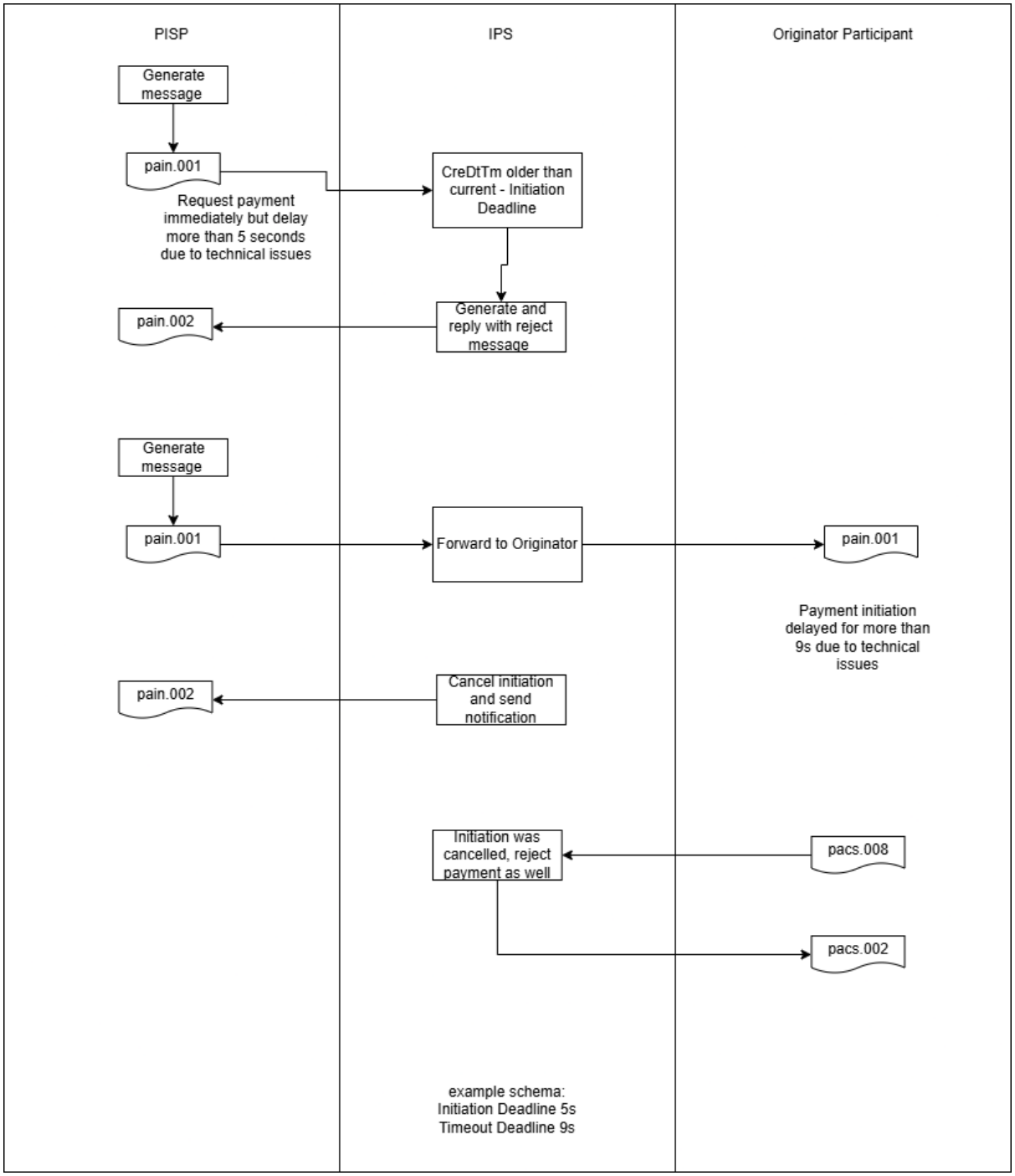


FIGURE 23. STATUS TRANSITION FLOW OF PAIN.001 MESSAGE


PISP
IPS
Originator Participant
Generate message
pain.001
Request payment immediately but delay more than 5 seconds due to technical issues
CreDtTm older than current - Initiation Deadline
Generate and reply with reject message
pain.002
Generate message
pain.001
Forward to Originator
pain.001
Payment initiation delayed for more than 9s due to technical issues
pain.002
Cancel initiation and send notification
Initiation was cancelled, reject payment as well
pacs.008
pacs.002
example schema:
Initiation Deadline 5s
Timeout Deadline 9s

3.2.12. Payment Initiation Status Report – pain.002.001.10

The IPS's validation process for the received pain.002 messages follows the steps:

1. Validation of HTTPS request header.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pain.002 message.
3. Business Application Header validation.
4. Message business fields' validation:
    a. Static message fields: **ServiceLevel**, **LocalInstrument – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes**.
    b. **OrgnlMsgId** (from OrgnlGrpInfAndSts) – message id of original payment initiation
    c. **OrgnlMsgNmId** (from OrgnlGrpInfAndSts) – fixed text "pain.001.001.12".
5. Duplicate message verification. For this purpose, the IPS system compares the item/message reference (field **MsgId**) with all references of messages that the system received from the same Participant (InitgPty) during the last 24 hours.
6. If the referred instruction (pain.001) already has a reply generated, the system will reject the pain.002 and send reply to the Originator Participant a pain.002 message with status code AG09 (internal error code 1017).
7. Validation of digital signature.

During this validation process, the IPS system reports only the first detected error by replying with a pain.002 message. The message is placed in REJECTED status and the processing is completed.

3.2.13. Customer Payment Cancellation Request – camt.055.001.012

The message is used for either a request for cancellation (RfC) or for request for status update of a RfC of pain.013 or pain.001. The camt.055.001.012 message with the field for reason containing RFSU or RFC indicates that the message applies to a Request for Status Update on a request for cancellation.

The IPS's validation process for the received camt.055 messages follows the steps:

1. Validate https request header. Each HTTPS request to the system must have the X-MONTRAN-IPS-Channel request header which indicates the Participant's communication channel. If this header is missing or incorrect then the PM https reply will have **error code 401 Unauthorized**.
2. Parsing and validation of XML message according to the XSD schema – if this step is not successfully completed, IPS replies a pacs.002 message.
3. Business Application Header validation.
4. Message business fields' validation:
    a. Static message fields: **ServiceLevel**, **LocalInstrument**. (from PmtTpInf) - – will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External Codes.
    b. **Assigner** – BIC of sender Participant. It must identify an ACTIVE Participant in the system. This BIC must identify the sender Participant detected at the sending channel.
    c. **Assignee** – IPS's BIC.
    d. **DbtrAgt** – BIC of debtor Participant (original). This must identify an ACTIVE Participant.
    e. **CdtrAgt** – BIC of creditor Participant (original). This must identify an ACTIVE Participant. This must be equal to Assigner for direct clearing participants or to one of the sender's indirect clearing participants.
    f. **OrgnlMsgNmId** (from OrgnlGrpInfAndSts) **–** fixed text 'pain.013.001.11' or 'pain.001.001.012' or 'camt.055.001.08'
5. **Rsn** (Undrlyg - OrgnlPmtInfAndCxl - TxInf - CxlRsnInf); will be valided according to the values listed in the system and presented in the Inception report, section 3.5.6 External CodesDuplicate message verification. For this purpose, the IPS compares the item/message reference (field **Id**) with all references of messages that the system received from the same Participant during the last 24 hours.
6. Validation of digital signature.

7. During this validation process, the IPS reports only the first detected error by replying a pacs.002 message. The message is placed in REJECTED status and the processing is completed.

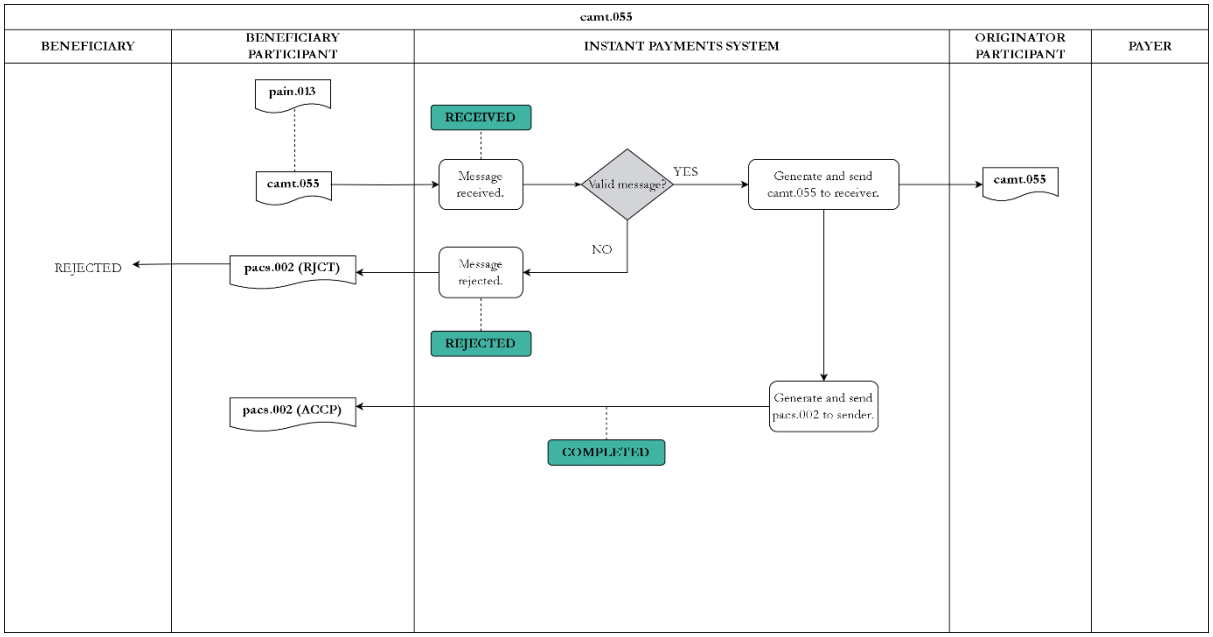


FIGURE 24. STATUS TRANSITION FLOW FOR CAMT.055 FOR PAIN.013

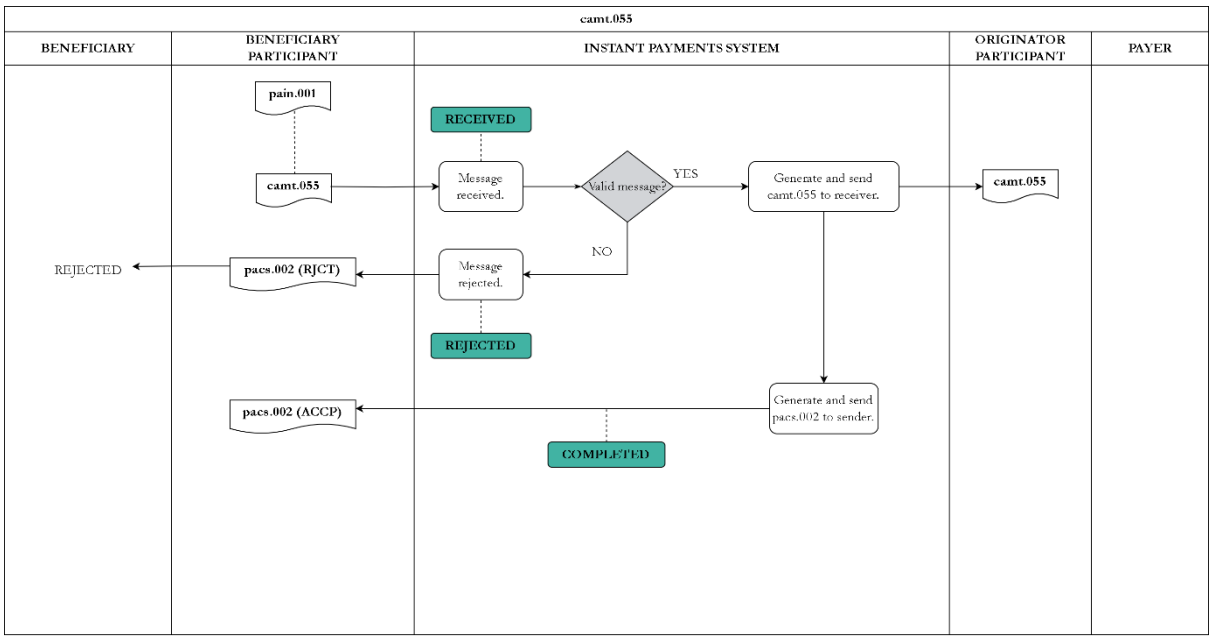


FIGURE 25. STATUS TRANSITION FLOW FOR CAMT.055 FOR PAIN.001

3.2.14. Time and Date Information

The XML messages used by the IPS system include fields that contain information about date and time. For a correct processing, please take into consideration the following details:

- Field **CreDt** from **AppHdr** must contain the date and hour in UTC format, indicated by the presence of 'Z' as suffix. The format of this field is essential because it is validated according to the XML schema, but the content (actual value of the field) is not validated by the IPS.
- Field **CredDtTm** from the messages must contain the correct time zone information, in the allowed format of type:

  xs:dateTime: YYYY-MM-DDTHH:mm:ss[{+/-}HH:mm].

Although the time zone information from the two fields mentioned above is optional for XML standards, the IPS system uses these, in order to eliminate ambiguities that might occur due to the summer/winter time change. Thus, IPS uses this information if the XML messages contain it. If not, IPS uses the system's existing time zone information at the moment of validation, even though it might be different from the time zone at the moment of payment generation by the Originator.

Please see an example below:

MOMENT	XML TIMESTAMP VALUE WITHOUT TIME ZONE INFORMATION	XML TIMESTAMP VALUE WITH TIME ZONE INFORMATION
On 2018-03-25 at 02:30:00, the Originator generates and sends an XML message	XML information: 2018-03-25T02:30:00	XML information: 2018-03-25T02:30:00+02:00
At 02:30:01, IPS receives the message and interprets the XML values this way:	IPS Interpretation: Date: 2018-03-25 Local hour: 02:30:00 UTC hour: 00:30:00 The system's existing time zone at the moment of validation is used.	IPS Interpretation: Date: 2018-03-25 Local hour: 02:30:00 UTC hour: 00:30:00 The time zone indicated in the XML value is used.
In this case, the difference between the system's UTC time and the message's UTC time is of 1 second, regardless of the presence of time zone in the XML message.		

In the case of messages processed at the moment of summer time change (**03:00:00 becomes 04:00:00**):

MOMENT	XML TIMESTAMP VALUE WITHOUT TIME ZONE INFORMATION	XML TIMESTAMP VALUE WITH TIME ZONE INFORMATION

Originator generates and sends an XML message at 02:59:55, local time or 00:59:55 UTC time	XML information**:** 2018-03-25T02:59:55	XML information**:** 2018-03-25T02:59:55**+02:00**
03:00:00 becomes 04:00:00 The sent message (see above cell) is received by IPS at 04:00:01, local time or 01:00:01, UTC time (after 6 seconds) and it interprets the XML value this way:	**IPS Interpretation:** Date and UTC hour: 2018-03-24 23:59:55 (previous day) Date and local hour: 2018-03-25 02:59:55 The system's existing time zone at the moment of validation is used to obtain the UTC value, to which the new system's time zone is added.	**IPS Interpretation:** Date and UTC hour: 2018-03-25 00:59:55 Date and local hour: 2018-03-25 03:59:55 The time zone information indicated in the XML file is used to obtain the UTC time, to which the local system's time zone is added.
	The time difference between the file time value and the validation moment is 1 hour and 6 seconds.	The time difference between the file time value and validation moment is 6 seconds.

3.2.15. Time Synchronization

Time synchronization of IPS is performed following the Network Time Protocol (NTP). The protocol uses a hierarchical semi-layered system of time sources. Each layer of the hierarchy is starting with a zero at the top. The higher the layer the closer the server is located to a reference clock.

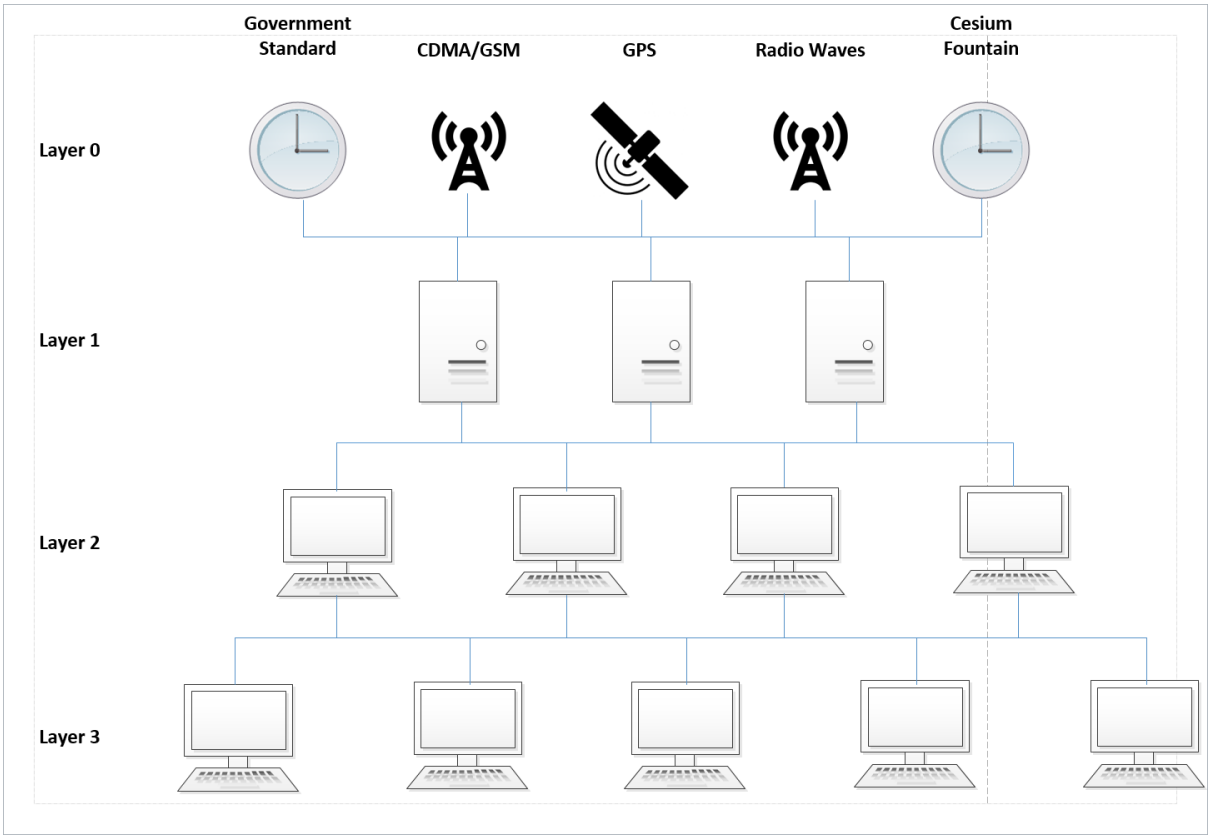


FIGURE 26. NETWORK TIME SYNCHRONIZATION

The IPS synchronizes its internal clock with a Layer 1 time source. Institutions that are connected to IPS should synchronize the clocks of their systems with a Layer 1 time source closest to the location of these systems.

4. Security

The security mechanisms used by the IPS guarantees confidentiality, integrity and authenticity of the data transferred between the systems. Technically, the IPS has two security levels:

1. SSL[6] technology for the encryption of the communication channel between the Customer application of Participants and the central IPS system.
2. Digital signature of the ISO20022 payment messages schema.

Each level of security requires a different digital certificate. The digital certificate must be uploaded into the central IPS system so that the Participants' STP application can use it. The private key of each digital certificate must be kept only at the Participant, being used by applications for securing the communication.

4.1. Communication Channel Encryption

The encryption of the communication channel is made using the SSL (TLS 1.2) protocol. This ensures the confidentiality, integrity and authenticity of the systems. The mutual authentication of the systems is carried out as described below.

The **authentication of the IPS system by the Participant STP application** is made by verifying some elements of the IPS's public certificate:

1. IPS's Certificate must be issued by a trusted Certification Authority (configured in truststore). NBG's B-Trust CA will be used for issuing of certificates
2. Certificate must not be expired.
3. Certificate must not be revoked

The **authentication of the Participant STP application to the IPS system** is made through:

1. Verifying the certificate's presence in the certificate list uploaded in IPS for communication authentication purpose.
2. Certificate validation in terms of expiration and revocation.

This second authentication allows IPS to precisely identify the Participant that initiates the connection.

Within the use of the IPS system, both systems require their own digital certificate:

1. TLS server certificate issued for IPS.
2. Client TLS server certificate for Participant's STP application.

[6] In fact, the TLS 1.2 standard is employed, a newer version of the SSL protocol. SSL (3.0) was considered vulnerable and deprecated since 2015.

4.2. Digital Signature

All ISO20022 schema payment messages are digitally signed, by the sending bank or by the sending central IPS system. The XML messages contain a **Timestamp** field that is validated by the central system. Thus, the digital signature must be executed in real time, before sending the message.

The standard for XML Signature type digital signature is described at the URL https://www.w3.org/TR/xmldsig-core1/ and it is configured with the following parameters:

- Content encoding: http://www.w3.org/TR/2001/REC-xml-c14n-20010315
- ENVELOPED Transformation: http://www.w3.org/2000/09/xmldsig#enveloped-signature
- Signature encoding: http://www.w3.org/2006/12/xml-c14n11
- Digest: http://www.w3.org/2001/04/xmlenc#sha256
- Signature: http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256

The Participant's STP application uses a private key to apply the digital signature. The digital certificate that contains the public key associated to the private key must be issued by a certificate authority approved by the Customer and uploaded into the central IPS system so that it can be used to validate signatures.

When receiving messages, the Participant's STP application validates the messages' digital signature applied by the central IPS system. Upon validation, the application will have access to the IPS digital certificate either in the form of a keystore or imported into the operating system.

5. Straight-Through-Processing Application and IPS Client Library

The Participants' IPS consists of the following elements:

1. The internal IPS application – payment messages generation/processing solution that interfaces with the STP application.
2. The STP application – module that implements the message transmission/reception functions by implementing the HTTPS protocol (described in chapter above) or through the IPS client library (developed in Java).

The Customer STP application initiates permanent[7] requests to the STP interface and awaits a response from it. The Customer STP application must wait the IPS response longer than the timeout parameter set by the payment schema - `Timeout Deadline`.[8] This response period can be configured by Participants through the IPS client library.

Resending a message by the Customer STP application without receiving a reply from the STP interface must be executed explicitly by the solution that implements the IPS client library, without being included in the transmission protocol.

In order for the IPS system to send messages, the Customer STP application developed through the implementation of the IPS client library must use the receive message function **GetMessage**. The receive message function is implemented according to the HTTPS Long-Polling method, through which the Customer application initiates a receive request from the server system. If there is an available message in the central IPS application, this will be immediately delivered and the STP application initiates a new receive request for the next message in the shortest time period. If there is no available message in the STP interface, the central IPS system delays the zero-value reply to the requesting Participant for maximum 5 seconds.

5.1. IPS Client Library Configuration

The configuration of the client library can be done in two ways:

1. Using a configuration file named **client-config.properties**. this is uploaded by the IPS client library when a library class if first used.
2. Dynamically, through the field change of the **ClientConfig** class of the library.

The configurable parameters are presented in the table below:

[7] This is a necessity for detecting the online status of the receiver Participant.
[8] For now, the parameter is 20 seconds. This value can be adjusted depending on the timeout parameter established by the SCT Inst schema.

NAME	VALUE EXAMPLE	DESCRIPTION
BASE_URL	BASE_URL=https://rtp.cluster/pe	URL address of IPS's STP interface.
MY_DNSxxx	MY_DNSrtp.cluster=10.33.1.50, 10.33.1.52	Local translation of the IP address (in the library).
RTP_BIC	RTP_BIC=NETCMNUB	BIC of the central IPS system.
HTTP_CONNECTION_TIMEOUT	HTTP_CONNECTION_TIMEOUT=2	Maximum allowed time (seconds) for establishing a connection to the central IPS system.
HTTP_SEND_MESSAGE_TIMEOUT	HTTP_SEND_MESSAGE_TIMEOUT=25	Maximum allowed time (seconds) for sending a message. It must be larger than the maximum allowed time according to the payment schema.
HTTP_RECEIVE_MESSAGE_TIMEOUT	HTTP_RECEIVE_MESSAGE_TIMEOUT=10	Maximum allowed time (seconds) for receiving a message from the central system.

At the first reference of the **ClientConfig** class, the class reads the configured values from the configuration file. Later, these values can be modified directly within the class. The values become concrete for connections (**EngineConnenction** instances) obtained later from **ConnectionFactory.**

The configuration of keystore files and of certificates used by the Customer application is made through setting some properties in the configuration file **security.properties**. Similar to **client-config.properties**, this must be present in the application's classpath. Its reload is made through the Java class loading mechanism. Properties to be configured in this file are:

1. **keyPass** – password for all configured keystore files.
2. **SSLkeyFile** – path to the keystore that holds the own SSL type certificate (client) for the authentication to the central IPS system. The client library will use the private key certificate from the keystore certificate suggested by the sslKeyAlias parameter when a connection was created.
3. **SSLTruststore** – path to the keystore that holds public certificates of servers and of server certificate issuer entities to which the IPS system connects. It is used by the Customer application to authenticate the central IPS system. If missing, the value of the SSLkeyFile will be used.

4. **DSkeyFile** – path to the keystore that holds the own Digital Signature certificate used for the signature of messages sent to the IPS. The certificate used by the application is indicated by the keyAlias parameter.
5. **DSTruststore** – path to the keystore that holds the servers' public certificate or certificates of server certificate issuer entitites to which the IPS application connects. It is used by the Customer application for the verification of the digital signature of messages sent by the central IPS system. If missing, the value of the DSTruststore will be used.
6. **keyAlias** – private key alias used for the digital signature.

5.2. Certificates Configuration Procedure

Each participant will receive the following digital certificates from the Certification Authority:

- Public certificates of the certificate issuer entities: **InterBanksCA.cert.jks** / **InterBanksCA.cer** and **IssuingCA.cert.jks** / **IssuingCA.cer**. Load these certificates as trusted entries into the SSLTruststore and DSTruststore.
- Public certificates of the IPS server: **NETCMNUB.cer**. Load this certificate as trusted entry into the SSLTruststore and DSTruststore.
- Private key certificate for SSL, named **NNNNNNNN-SSL.p12** and public key exported separately **NNNNNNNN-SSL.cer**. Load the private certificate into SSLkeyfile. Upload the public certificate into the IPS MMC Web Interface, with *TLS Client Authentication* usage type, from function *MAINTENANCE > Security > Digital Certificate > Create*, and then *MAINTENANCE > Security > Digital Certificate > Approve* to approve the upload.
- Private key certificate for digital signing, named **NNNNNNNN-DS.p12** and public key exported separately **NNNNNNNN-DS.cer**. Load the private certificate into DSkeyfile. Upload the public certificate into the IPS MMC Web Interface, with *Digital Signature* usage type, from function *MAINTENANCE > Security > Digital Certificate > Create*, and then *MAINTENANCE > Security > Digital Certificate > Approve* to approve the upload.

A procedure to create and load the keystores uses the following commands (you will need to have Java installed). If you want to simplify the procedure, use the same file for SSLkeyFile and SSLTruststore; also, use same file for DSkeyFile and DSTruststore.

SSLkeyFile:

keytool -importkeystore -srckeypass *SRCPASS* -srcstorepass *SRCPASS* -srcalias *nnnnnnnn-ssl* -destkeystore SSLkeyFile -destkeypass *DESTPASS* -deststorepass *DESTPASS* -destalias *KEYALIAS* -srckeystore *NNNNNNNN-SSL.p12*

where:

- SRCPASS – the password for the .p12 file

- DESTPASS – the password for the keystore, as set in the *security.properties* file, property *keyPass*
- NNNNNNNN-SSL.p12 – the name of the digital certificate file you received
- nnnnnnnn-ssl – the name of the digital certificate you received, written in lowercase

```
keytool -import -trustcacerts -alias netcmnub -file netcmnub.cer -storepass SRCPASS -keystore SSLkeyFile
```

where:

- STOREPASS – the password for the keystore, as set in the *security.properties* file, property *keyPass*

SSLTruststore:

```
keytool -import -trustcacerts -alias interbanksca -file interbanksca.cer -storepass SRCPASS -keystore SSLTruststore
```

where:

- STOREPASS – the password for the keystore, as set in the *security.properties* file, property *keyPass*

```
keytool -import -trustcacerts -alias server -file issuingca.cer -storepass SRCPASS -keystore SSLTruststore
```

where:

- STOREPASS – the password for the keystore, as set in the *security.properties* file, property *keyPass*

DSkeyFile:

```
keytool -importkeystore -srckeypass SRCPASS -srcstorepass SRCPASS -srcalias nnnnnnnn-ds -destkeystore SSLkeyFile -destkeypass DESTPASS -deststorepass DESTPASS -destalias KEYALIAS -srckeystore NNNNNNNN-DS.p12
```

where:

- SRCPASS – the password for the .p12 file
- DESTPASS – the password for the keystore, as set in the *security.properties* file, property *keyPass*
- NNNNNNNN-DS.p12 – the name of the digital certificate file you received
- nnnnnnnn-ds – the name of the digital certificate you received, written in lowercase

```
keytool -import -trustcacerts -alias netcmnub -file netcmnub.cer -storepass SRCPASS -keystore DSkeyFile
```

where:

- STOREPASS – the password for the keystore, as set in the *security.properties* file, property *keyPass*

DSTruststore:

```
keytool -import -trustcacerts -alias interbanksca -file interbanksca.cer -storepass SRCPASS -keystore DSTruststore
```

where:

- STOREPASS – the password for the keystore, as set in the *security.properties* file, property *keyPass*

```
keytool -import -trustcacerts -alias server -file issuingca.cer -storepass SRCPASS -keystore DSTruststore
```

where:

- STOREPASS – the password for the keystore, as set in the *security.properties* file, property *keyPass*

5.3. IPS Message Class

The IPS Message Class contains the following fields:

- **Type**: String – it represents the type of reply message that the central IPS sends. Its possible values are: camt.029, camt.056, pacs.008, pacs.009, pacs.004, pacs.002, pacs.028, camt.055, pain.001, pain.002, pain.013, pain.014
- **Sequence**: long – sequence of the message received by Participant from the central IPS system. This sequence is assigned by the system when messages are generated.
- **Content**: String – XML content of the received/sent message from/to the central IPS system.
- **ErrorCode**: integer – the internal error code reported by the system for the sent message. Please see details in section 7.2.
- **ReportedStatus**: String – ACCP or RJCT code for a pacs.002 type message received from the central system.
- **ProcessingDuration**: long – total processing time of a message send to the central system, expressed in nanoseconds.

5.4. EngineConnection Interface

SendNewMessage

Description: The method is used for sending a new message to the central IPS system. The supported message types are the ones belonging to the SCT Inst schema (see Table 1. IPS Reception – Accepted Messages FOR ISO20022), except message type pacs.002, which is sent using a specific method.

Method signature:

```
public IPSMessage sendNewMessage(IPSMessage message) throws
IOException;
```

Input parameters: pacs.002 message to be sent, enclosed into an object of type IPSMessage.

Configuration parameters:

- HTTP_SEND_MESSAGE_TIMEOUT – the maximum allowed time (seconds) for receiving a reply from the central IPS system. If this time is exceeded, an exception of type **org.apache.http.NoHttpResponseException** is raised.

Result: pacs.002 reply message, received from the central IPS system, if sending was successfully executed.

Exceptions: In case of communication errors with the central IPS system, the client library will raise an exception type java.io.**IOException**.

ReplyToPayment

Description: The method is used by receiver Participant to reply positively or negatively to a payment message received from the central IPS system.

Method signature:

```
public IPSMessage replyToPayment(IPSMessage responseMessage) throws
IOException;
```

Input parameters: pacs.002 message to be sent, enclosed into an object of type IPSMessage.

Configuration parameters:

- HTTP_SEND_MESSAGE_TIMEOUT – the maximum allowed time (seconds) for receiving a reply from the central IPS system. If this time is exceeded, an exception of type **org.apache.http.NoHttpResponseException** is raised.

Result: pacs.002 reply message, received from the central IPS system, if sending was successfully executed.

Exceptions: In case of communication errors with the central IPS system, the client library will raise an exception type **IOException**.

GetMessage

Description: The method is used by a Participant for receiving a message from the central IPS system. If there is no available message for the Participant, the method replies the value **null**. In both cases, if calling this function returns a message or not, the **Participant must initiate a new call immediately** (within maxim 5 seconds[9]), because this function is used by the central IPS system to check the ONLINE status of Participants (check availability of pacs.008 messages).

Method signature:

```
public IPSMessage getMessage() throws IOException;
```

Input parameters: none.

Configuration parameters:

- HTTP_RECEIVE_MESSAGE_TIMEOUT – the maximum allowed time (seconds) for receiving a reply from the central IPS system. If this time is exceeded, an exception of type **org.apache.http.NoHttpResponseException** is raised.

Result: message received from the central IPS system or **null** if there is no available message.

Exceptions: In case of communication errors with the central IPS system, the client library will raise an exception type **IOException**.

ConfirmMessage

Description: The method is used by a Participant to confirm receiving a message. A message received from the central IPS system must be confirmed explicitly by the Participant by using this method. Contrary, or if the confirmation is executed after a period of time larger than IPS's Output Redelivery Time, the system will automatically resend the unconfirmed messages by placing them in the message queue processed by the function GetMessage.

Method signature:

```
public void confirmMessage(long sequence) throws IOException;
```

[9] This parameter is defined by the IPS central system and controlled by the operator exclusively. It should rarely be changed; a yearly review is typical. The value is communicated to the participants to use in the STP application configuration.

Input parameters: sequence of received message. This is to be found in the object of IPSMessage received as the result of **GetMessage** function's execution.

Configuration parameters:

- HTTP_SEND_MESSAGE_TIMEOUT – the maximum allowed time (seconds) for receiving a reply from the central IPS system. If this time is exceeded, an exception of type **org.apache.http.NoHttpResponseException** is raised.

Result: none.

Exceptions: In case of communication errors with the central IPS system, the client library will raise an exception type **IOException**.

GetPositions

Description: The method is used by a Participant to get the position of the technical account and its available amount. **Method signature**:

```
public String getPositions() throws IOException;
```

Input parameters: missing.

Result: An XML message that contains the current values of technical accounts' balances at the time of the call.

Exceptions: In case of communication errors with the central IPS system, the client library will raise an exception type **IOException.**

Exception handling

In the case of IOException it means that it was a communication issue and the client does not know whether the operation succeeded or failed. Therefore, the flow should be retried to account for transient faults. If the issue persists then it requires manual intervention, and an alert could be triggered.

- **SendNewMessage**
  - pacs.008 – to find the final status of the payment the investigation flow should be used (pacs.028). This can be done before retrying to check if the payment went through (and retry if IPS reports that the payment was not processed), or after a retry for which IPS reported a duplicate (the original payment was sent before the IOException).
  - For other messages (since they are not covered by the investigation mechanism) – during retry the following HTTP Header can be included in the request "X-MONTRAN-RTP-PossibleDuplicate" with value "true". If IPS identifies this header on

a request and the original message was already processed, then it will reply with the status of the original message instead of replying with a duplicate error code.

- **ReplyToPayment** can be retried with no side effects; if this reply is sent multiple times IPS will reply with the final status of the payment each time
- **GetMessage** – can be retried with no side effects; this is the method used for polling and if it fails continuously due to network issues/misconfiguration then IPS will mark the participant as offline
- **ConfirmMessage** – can be retried with no side effects. If this operation is not succesful then IPS will re-send unconfirmed messages periodically.
- **GetPositions** – can be retried with no side effects.

5.5. ConnectionFactory Class

The **ConnectionFactory** class offers a set of static methods that allow getting concrete instances that implement the **EngineConnection** interface.

GetEngineConnection Method

Description: The method is used for obtaining an object that implements the EngineConnect interface and that can be used later to access the central IPS system's functions.

Method signature:

```
public     static     EngineConnection
getEngineConnection(String channelName, String sslKeyAlias);
```

Input parameters:

1. Communication channel's identifier that must be the Participant's BIC.
2. Name (alias) of the SSL private key used by the Participant to authenticate the central IPS system. The public certificate associated to this key must be uploaded into the central IPS system.

Configuration parameters:

- HTTP_CONNECTION_TIMEOUT – the maximum allowed time (seconds) for establishing a connection to the central IPS system. If the client library cannot establish the TCP connection for any call of a function of the central IPS system interface, then an exception of type **java.net.ConnectException** is raised.

Result: instance that implements the EngineConnection interface.

Exceptions: In case of library configuration or integration error, the method will raise an exception of type **RuntimeException**.

5.6. Digital Signature Application and Verification Functions

The IPS library also provides Participants with a set of functions for applying and verifying the digital signature of messages exchanged with the central IPS system. These functions are offered by the **XMLSignatureUtils** class and are described in the next sections.

GenerateSignature Method

Description: The method is used for applying the digital signature to an XML message before it is sent to the central IPS system. The alias of the private key used for the signature is configurated in **security.properties**.

Method signature:

```
public String generateSignature(String xmlContent) throws
SignatureException;
```

Input parameters:

- XML message in String format. The message structure must be according to the montran.message.01 schema, which contains a **head:BusinessApplicationHeader** structure defined by ISO 20022, where the digital signature is to be inserted.

Result: digitally signed XML message, String format.

Exceptions: In case of library configuration or signature entry error, the method will raise an exception of type **SignatureException.**

ValidateSignature Method

Description: The method is used for applying the digital signature to an XML message, represented as a DOM document, before it is sent to the central IPS system. The alias of the private key used for the signature is configurated in **security.properties**.

Method signature:

```
public String generateSignature(Document xmlContent) throws
SignatureException;
```

Input parameters:

- XML message in org.w3c.dom.Document format. The message structure must be according to the montran.message.01 schema, which contains a **head:BusinessApplicationHeader** structure defined by ISO 20022, where the digital signature is to be inserted.

Result: digitally signed XML message, String format.

Exceptions: In case of library configuration or signature entry error, the method will raise an exception of type **SignatureException.**

5.7. Use Cases

Please find below some basic examples for the use of the IPS client library for sending and receiving messages. The purpose of these examples is to present the initial use and it does not entail a complete and sufficient solution for connecting to the central IPS system. The examples below do not handle all operation exceptions or communication errors with the central system that could occur.

Example of Send Message

```
String participantBIC="TESAROBU";
EngineConnection conn =
ConnectionFactory.getEngineConnection(participantBIC);

String xmlContent = "<?xml …";       // IPS Message
String signedMessage = XMLSignatureUtils.generateSignature(xmlContent,
"signer");
IPSMessage message = new IPSMessage(signedMessage);
// send message
IPSMessage replyFromIPS = conn.sendNewMessage(message);
String replyContent = replyFromIPS.getContent();
// validate DS try
{
      XMLSignatureUtils.validateSignature(replyContent);
} catch (SignatureValidationException sve) {
      // handle Exception, DS validation failed
}
// handle reply either based on content or use replyFromIPS.getErrorCode()
```

Example of Receive Message

```
String participantBIC="TESAROBU";
EngineConnection conn =
ConnectionFactory.getEngineConnection(participantBIC);

while (alive) {
       IPSMessage receivedMessage = conn.getMessage();
      String replyContent = receivedMessage.getContent();
      // validate DS
      try {
            XMLSignatureUtils.validateSignature(replyContent);
```

```
        } catch (SignatureValidationException sve) {
              // handle Exception, DS validation failed
        }

        // handle receivedMessage, persist
        // then either reply by sending a pacs.002 for a pacs.008
        // or use conn.confirmMessage(receivedMessage.getSequence());
}
```

6. HTTPS Communication Protocol Description

Invoking the operations offered by the IPS system is done by sending requests (GET, POST) from specific secure URLs. The details of these URLs and the methods are described below:

OPERATION	URL	HTTP METHOD
Send message	<BASE_URL>/Message	POST
Receive message	<BASE_URL>/Message	GET
Confirm received message	<BASE_URL>/MessageAck	POST
Position query	<BASE_URL>/Positions	GET

BASE_URL is the main IPS URL and its form is: <PROTOCOL>://<HOSTNAME>[<PORT>]/<APP>, where:

- PROTOCOL is HTTPS.
- HOSTNAME is the name of the domain where the IPS system is installed.
- PORT is the TCP port, including 443. This field may be missing if there is a default value.
- APP is the path to the application.

Complete BASE_URL examples are: https://ipsURL:8443/pe for Instant Mode. Common Elements of Messages Exchange with IPS.

6.1. HTTP Header Attributes of Messages sent to IPS

All requests sent by the Customer application to the central IPS system must contain the following attributes in the HTTP header:

- **X-MONTRAN-IPS-Channel** – BIC of sender Participant.
- **X-MONTRAN-IPS-Version** – protocol version, this is 1 for now.

6.2. HTTP Answer Codes

- **200 (HTTP OK)** – if the request was successfully processed. This does not imply that a message was accepted or that a payment was completed, it only implies that no technical errors occurred during the processing.

- **400 (HTTP Bad Request)** – error occurred for sending an incorrect receive confirmation message, if the confirmation message is a pacs.008 one (see section 2.2 for explanation).
- **401 (HTTP Unauthorized)** – error occurred during Participant authentication (BIC present in X-MONTRAN-IPS-Channel cannot identify an ACTIVE Participant or the Participant's TLS certificate is not accepted by IPS).
- **500 (HTTP Internal Server Error)** – in case of a generic error during the processing of a message by IPS.
- **503 (HTTP Service Unavailable)** – in case the service is not available (node hot-standby).

6.3. Send Message to IPS

This method is used by both operations:

1. The generic send message.
2. The confirmation of received pacs.008 messages.

Service URL: <BASE_URL>/Message

Method: POST

Parameters: nothing.

Sent message HTTP Attribute Header:

- **X-MONTRAN-IPS-Channel** – BIC of sender Participant.
- **X-MONTRAN-IPS-Version** – **Protocol Version**.

Content: XML message in the format accepted by IPS.

Response Code:

- 200 (HTTP OK) – if IPS the received and processed the message.

Replied Content:

- If IPS successfully completed the message processing, then the response code will be 200 and the IPS system will send a reply pacs.002 message, according to the ISO20022 schema. The pacs.002 message indicates that the message was either accepted or rejected by the system.
- If the response code is different then 200, then the system will not send a pacs.002 reply message.

HTTP Attribute Header for reply:

- **X-MONTRAN-IPS-ReqSts** – Status of sent message:

  - ACCP – sent message was accepted and successfully processed.
  - RJCT/<ErrorCode> – sent message was rejected because of validation reasons or it was not successfully completed, e.g., payment was rejected by receiver or timeout. The error code is according to section 7.2.
- **X-MONTRAN-IPS-MessageSeq** – sequence of reply message.
- **X-MONTRAN-IPS-MessageType** – Type of reply message. Possible values are pacs.002, pain.002, pain.014.
- **X-MONTRAN-IPS-Version** – Protocol version.

6.4. Receive Message from IPS

Service URL: <BASE_URL>/Message

Method: GET

Parameters: nothing.

HTTP Attribute Header:

- **X-MONTRAN-IPS-Channel** – BIC of sender Participant.
- **X-MONTRAN-IPS-Version** – **Protocol Version**.
- **Accept-Encoding: gzip** – optional, if responses can be received zipped.

Content: nothing.

Response Code:

- 200 (HTTP OK) – if IPS successfully processed the message.

Replied Content:

- XML message if the request was successfully processed (response code HTTP 200) and there is an available receive message for Participant.
- Nothing, if there is no available receive message for the Participant that makes the call. In this case, the HTTP reply message will entail **X-MONTRAN-RTP-ReqSts** in the attribute header with value EMPTY.

HTTP Attribute Header for reply:

- **X-MONTRAN-IPS-ReqSts** – Value EMPTY, if there is no available message.
- **X-MONTRAN-IPS-PossibleDuplicate** – if this attribute is present, its value is true and it indicates that the message was delivered to the Participant at least once. This can happen if a message received earlier was not confirmed by IPS.
- **X-MONTRAN-IPS-MessageSeq** – sequence of received message. This is generated by IPS and it is used to confirm that the message was received.

- **X-MONTRAN-IPS-MessageType** – Type of reply message. Possible values are: pacs.008, pacs.009, pacs.004, pacs.028, camt.056, camt.029, camt.053, pacs.002, pain.001, pain.002, camt.055, pain.013, pain.014.
- **X-MONTRAN-IPS-Version** – Protocol version.

6.5. Received Message Confirmation

Service URL: <BASE_URL>/MessageAck

Method: POST

Parameters: nothing.

HTTP Attribute Header:

- **X-MONTRAN-IPS-Channel** – BIC of sender Participant.
- **X-MONTRAN-IPS-MessageSeq** – sequence of message that needs to be confirmed.
- **X-MONTRAN-IPS-Version** – **Protocol Version**.

Content: nothing.

Response Code:

- 200 (HTTP OK) – if IPS successfully processed the request.
- Other codes, according to 7.1.2.

Replied Content: nothing.

HTTP Attribute Header for reply:

- **X-MONTRAN-IPS-Version** – Protocol version.

Content: "Stored" message in case of success or "NotFound", if the message referred to in the sequence sent is not found. In both cases, the HTTP reply is 200.

6.6. Own Positions Queries

Service URL: <BASE_URL>/Positions

Method: GET

Parameters: nothing.

HTTP Attribute Header:

- **X-MONTRAN-IPS-Channel** – BIC of sender Participant.
- **X-MONTRAN-IPS-Version** – **Protocol Version**.

Content: nothing.

Response Code:

- 200 (HTTP OK) – if IPS successfully processed the request.
- Other codes, according to 7.1.2.

Reply: XML message according to 8.1.13.

HTTP Attribute Header for received reply:

- **X-MONTRAN-IPS-Version** – Protocol version.

7. Annexes

7.1. Annex 1 – XML Format Description

1. The ISO payment scheme messages, as defined in the as defined in ISO20022 documentation:
    a. pacs.008.001.12 – FI to FI Customer Credit Transfer
    b. pacs.009.001.011 – Financial Institution Credit Transfer
    c. pacs.002.001.14 – Positive and Negative Confirmation Message
    d. camt.056.001.11 – Recall of an CT
    e. camt.029.001.13 – Negative Response to a Recall of an CT
    f. pacs.004.001.13 – Positive Response to a Recall of an CT
    g. pacs.028.001.06 –Transaction Status Investigation
    h. pain.013.001.11 – Request to pay, supporting debit transaction flow, purely informational, passed through the system to the debtor party, to be followed by a pacs.008 or pain.014
    i. pain.014.001.11 - Request to pay response, used when the debit requested via a previous pain.013 is refused.
    j. camt.055.001.012 – Request for Cancellation of a RTP, or Request for Status update of a RfC
    k. pain.001.001.012 – Payment Inititiation
    l. pain.002.001.014 – Status Report

    camt.053.001.12 – Reconciliation message

    m. head.001.001.03 – Header message
2. Messages supported by the IPS solution that are not part of the ISO20022 message standard:
    a. positions.001 - The IPS response message to the participant with information on the balance of technical accounts.
    b. Participants.001 – The IPS list of participants.

7.1.1. Message Header (App Hdr) – head.001.001.03.xsd

The format of this message is described in ISO20022, but the IPS solution uses a specific set of fields that is described below:

ELEMENT	TYPE	DESCRIPTION
Fr > FIId > FinInstnId > BICFI	BICFIIdentifier	Sender BIC
To > FIId > FinInstnId > BICFI	BICFIIdentifier	Receiver BIC
BizMsgIdr	Max35Text	Message identifier
MsgDefIdr	Max35Text	Message type
CreDt	ISONormalisedDateTime	Moment of message creation
Sgntr		Element entailing the digital signature.

Example of message with header that contains pacs.008 business message:

```
<env:Message xmlns:env="urn:montran:message.01">
    <env:AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.03">
        <Fr>
            <FIId>
                <FinInstnId>
                    <BICFI>PALSPS22</BICFI>
                </FinInstnId>
            </FIId>
        </Fr>
        <To>
            <FIId>
                <FinInstnId>
                    <BICFI>IFTSUS33</BICFI>
                </FinInstnId>
            </FIId>
        </To>
        <BizMsgIdr>MREF7a8c6ff5e4c0a</BizMsgIdr>
        <MsgDefIdr>pacs.008.001.12</MsgDefIdr>
        <BizSvc>RTP</BizSvc>
        <CreDt>2023-05-10T09:39:36Z</CreDt>
        <Sgntr>                 .....
       </Sgntr>
      </hdr:AppHdr>
      <env:FIToFICstmrCdtTrf
xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.008.001.12">
             <GrpHdr>
.....
</GrpHdr>
<CdtTrfTxInf>
.....
</CdtTrfTxInf>
      </env:FIToFICstmrCdtTrf>
</env:Message>
```

7.1.2. Instant Credit Transfer – pacs.008.001.12

The format uses the standard ISO schemas in the following structure. A restriction of a single instant credit is enforced.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<FIToFICstmrCdtTrf>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Credit Transfer Transaction Information	<CdtTrfTxInf>	[1..1]

Group Header

INDEX	MESSAGE ITEM			XML TAG	MULTIPLICITY	TYPE
1.0	Group Header			<GrpHdr>	[1..1]	
1.1		Message Identification		<MsgId>	[1..1]	Max35Text
1.2		Creation Date Time		<CreDtTm>	[1..1]	ISODateTime The exact time at which the PSP (direct participant in the system) technically receives the order from customer or indirect participant
1.3		Number Of Transactions		<NbOfTxs>	[1..1]	1
1.4		Total Interbank Settlement Amount		<TtlIntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
1.5		Interbank Settlement Date		<IntrBkSttlmDt>	[1..1]	ISODate
1.6		Settlement Information		<SttlmInf>	[1..1]	
1.7			Settlement Method	<SttlmMtd>	[1..1]	Only "CLRG is allowed. CLRG: ClearingSystem

						Settlement is done through a payment clearing system
1.8			Clearing System	<ClrSys>	[0..1]	Fixed text “IPS”
1.9				Code	<Cd>	[1..1]	
1.10		Payment Type Information		<PmtTpInf>	[1..1]	
1.11			Instruction Priority	<InstrPrty>	[0..1]	Allowed values “HIGH”/ ”NORM” to indicate payments for RTP fast/slow flows.
1.12			Service Level	<SvcLvl>	[1..1]	
1.13				Code	<Cd>	[1..1]	
1.14			Local Instrument	<LclInstrm>	[1..1]	
1.15				Code	<Cd>	[1..1]	
1.16			Category Purpose	<CtgyPurp>	[0..1]	Has child element either Cd or Prtry but not both
1.17				Code	<Cd>	[1..1]	ExternalCategoryPurpose1Code
1.18		Instructing Agent		<InstgAgt>	[0..1]	

1.19			Financial Institution Identification		<FinInstnId>	[1..1]	
1.20				BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.21				Name	<Nm>	[0..1]	Max140Text

Item Details

INDEX	MESSAGE ITEM				XML TAG	MULTIPLICITY	TYPE
2.1	Credit Transfer Transaction Information				<CdtTrfTxInf>	[1..1]	
2.2		Payment Identification			<PmtId>	[1..1]	
2.3			Instruction Identification		<InstrId>	[1..1]	Max35Text
2.4			End To End Identification		<EndToEndId>	[1..1]	Max35Text For RTP initiated messages it must contain the text "RTP-" followed by original RTP reference (PmtInfId)
2.5			Transaction Identification		<TxId>	[1..1]	Max35Text
2.6		Interbank Settlement Amount			<IntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
2.7		Acceptance Date and time			<AccptncDtTm>	[1..1]	ISODateTime
2.8		Charge Bearer			<ChrgBr>	[1..1]	Fixed text:"SLEV"
2.9		Ultimate Debtor			<UltmtDbtr>	[0..1]	
2.10			Name		<Nm>	[0..1]	Max70Text
2.11			Id		<Id>	[0..1]	
2.12				Organisation Identification	<OrgId>	[0..1]	

2.13					Other		<Othr>	[0..1]	
2.14						Id	<Id>	[1..1]	Third party ordering organization id
2.15				Private Identification			<PrvtId>		
2.16					Other		<Othr>	[0..1]	
2.17						Id	<Id>	[1..1]	Third party ordering person id
2.18		Debtor					<Dbtr>	[1..1]	
2.19			Name				<Nm>	[1..1]	Max70Text
2.20			Postal Address				<PstlAdr>	[0..1]	
2.21			Id				<Id>	[0..1]	
2.22				Organisation Identification			<OrgId>	[0..1]	
2.23					Other		<Othr>	[1..n]	
2.24						Id	<Id>	[1..1]	Max256Text Service user identifier for bill payments - If no code is set, value is Ordering organization id
2.25						Scheme Name	<SchmeNm>	[1..1]	
2.26						Code	<Cd>	[1..1]	Fixed text “BILL”
2.27				Private Identification			<PrvtId>	[0..1]	
2.28					Date and Place of Birth		<DtAndPlcOfBirth>	[0..1]	

2.29					Other			<Othr>	[1..n]	
2.30						Id		<Id>	[1..1]	Max256Text - Service user identifier for bill payments - If no code is set, value is Personal Id
2.31						Scheme Name		<SchmeNm>	[1..1]	
2.32							Code	<Cd>	[1..1]	Fixed text “BILL”
2.33		Debtor Account						<DbtrAcct>	[1..1]	
2.34			Identification					<Id>	[1..1]	
2.35				IBAN				<IBAN>	[0..1]	
2.36				Other				<Othr>	[0..1]	
2.37					Identification			<Id>	[1..1]	Treasury Code
2.38		Debtor Agent						<DbtrAgt>	[1..1]	
2.39			Financial Institution Identification					<FinInstnId>	[1..1]	
2.40				BICIdentifier				<BICFI>	[1..1]	BICIdentifier
2.41				Name				<Nm>	[0..1]	Max140Text
2.42		Creditor Agent						<CdtrAgt>	[1..1]	
2.43			Financial Institution Identification					<FinInstnId>	[1..1]	
2.44				BICIdentifier				<BICFI>	[1..1]	BICIdentifier
2.45				Name				<Nm>	[0..1]	Max140Text

2.46		Creditor							<Cdtr>	[1..1]	
2.47			Name						<Nm>	[1..1]	Max70Text
2.48			Postal Address						<PstlAdr>	[0..1]	
2.49			Id						<Id>	[0..1]	
2.50				Organisation Identification					<OrgId>	[0..1]	
2.51					Other				<Othr>	[1..1]	
2.52						Id			<Id>	[1..1]	Max256Text Beneficiary organization id
2.53				Private Identification					<PrvtId>	[0..1]	
2.54					Date and Place of Birth				<DtAndPlcOfBirth>	[0..1]	
2.55					Other				<Othr>	[1..1]	
2.56						Id			<Id>	[1..1]	Beneficiary person id
2.57			Contact Details						<CtctDtls>	[0..1]	
2.58		Creditor Account							<CdtrAcct>	[1..1]	
2.59			Identification						<Id>	[1..1]	
2.60				IBAN					<IBAN>	[0..1]	
2.61				Other					<Othr>	[0..1]	
2.62					Identification				<Id>	[1..1]	Treasury Code
2.63		Ultimate Creditor							<UltmtCdtr>	[0..1]	
2.64			Name						<Nm>	[0..1]	Max70Text
2.65			Id						<Id>	[0..1]	
2.66				Organisation Identification					<OrgId>	[0..1]	

2.67					Other	<Othr>	[0..1]	
2.68					Id	<Id>	[1..1]	Third party beneficiary organization id
2.69				Private Identification				
2.70					Other	<Othr>	[0..1]	
2.71					Id	<Id>	[1..1]	Third party beneficiary person id
2.72		Purpose				<Purp>	[0..1]	
2.73		Related Remittance Information				<RltdRmtInf>	[0..n]	
2.74			Remittance Identification			<RmtId>	[0..1]	Max35Text Channel and Instrument codes separated by colon in format: XXXX:XXXX.
2.75			Remittance Location Details			<RmtLctnDtls>	[0..1]	
2.76				Electronic Address		<ElctrncAdr>	[0..1]	Max2048Text The coordinates of the POS/device which was used for the payment
2.77		Remittance Information				<RmtInf>	[0..1]	
2.78			Unstructured			<Ustrd>	[0..n]	Max140Text
2.79			Structured			<Strd>	[0..n]	
2.80				Creditor Reference Information		<CdtrRefInf>	[0..1]	
2.81					Creditor Reference Type	<Tp>	[1..1]	
2.82					Code or Proprietary	<CdOrPrtry>	[1..1]	

2.83							Proprietary	<Prtry>	[1..1]	If value is set to “MCC” then <Ref> is interpreted as an MCC code. If value is set to “SERV”, then <Ref> is interpreted as a Service identifier code.
2.84						Issuer		<Issr>	[0..1]	Max35Text
2.85					Reference			<Ref>	[1..1]	Max35Text MCC or Service Identifier Codes depending on Cd value
2.86				Additional Remittance Information				<AddtlRmtInf>	[0..1]	Additional purpose of payment

7.1.3. Financial Institution Credit Transfer – pacs.009.001.011

The format uses the standard ISO schemas in the following structure. A restriction of a single credit is enforced.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<FIToFICstmrCdtTrf>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Credit Transfer Transaction Information	<CdtTrfTxInf>	[1..1]

Group Header

INDEX	MESSAGE ITEM				XML TAG	MULTIPLICITY	TYPE
1.0	Group Header				<GrpHdr>	[1..1]	
1.1		Message Identification			<MsgId>	[1..1]	Max35Text
1.2		Creation Date Time			<CreDtTm>	[1..1]	ISODateTime
1.3		Number Of Transactions			<NbOfTxs>	[1..1]	1
1.4		Total Interbank Settlement Amount			<TtlIntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
1.5		Interbank Settlement Date			<IntrBkSttlmDt>	[1..1]	ISODate
1.6		Settlement Information			<SttlmInf>	[1..1]	
1.7			Settlement Method		<SttlmMtd>	[1..1]	
1.8			Clearing System		<ClrSys>	[0..1]	
1.9				Code	<Cd>	[1..1]	
1.10		Payment Type Information			<PmtTpInf>	[0..1]	
1.11			Service Level		<SvcLvl>	[0..1]	
1.12				Code	<Cd>	[1..1]	
1.13			Local Instrument		<LclInstrm>	[0..1]	
1.14				Code	<Cd>	[1..1]	
1.15			Category Purpose		<CtgyPurp>	[0..1]	Has child element Cd
1.16				Code	<Cd>	[1..1]	ExternalCategoryPurpose1Code

1.17		Instructing Agent			<InstgAgt>	[0..1]	
1.18			Financial Institution Identification		<FinInstnId>	[1..1]	
1.19				BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.20				Name	<Nm>	[0..1]	Max140Text

Item Details

INDEX	MESSAGE ITEM				XML TAG	MULTIPLICITY	TYPE
2.1	Credit Transfer Transaction Information				<CdtTrfTxInf>	[1..1]	
2.2		Payment Identification			<PmtId>	[1..1]	
2.3			Instruction Identification		<InstrId>	[1..1]	Max35Text
2.4			End To End Identification		<EndToEndId>	[1..1]	Max35Text
2.5			Transaction Identification		<TxId>	[1..1]	Max35Text
2.6		Interbank Settlement Amount			<IntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
2.7		Interbank Settlement Date			<IntrBkSttlmDt>	[1..1]	ISODate
2.8		Debtor			<Dbtr>	[1..1]	
2.9			Financial Institution Identification		<FinInstnId>	[1..1]	
2.10				BICIdentifier	<BICFI>	[1..1]	
2.11		Debtor Account			<DbtrAcct>	[0..1]	
2.12			Identification		<Id>	[0..1]	
2.13				IBAN	<IBAN>	[0..1]	

2.14		Debtor Agent			<DbtrAgt>	[1..1]	
2.15			Financial Institution Identification		<FinInstnId>	[1..1]	
2.16				BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.17				Name	<Nm>	[0..1]	Max140Text
2.18		Creditor Agent			<CdtrAgt>	[1..1]	
2.19			Financial Institution Identification		<FinInstnId>	[1..1]	
2.20				BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.21				Name	<Nm>	[0..1]	Max140Text
2.22		Creditor			<Cdtr>	[1..1]	
2.23			Financial Institution Identification		<FinInstnId>	[1..1]	
2.24				BICIdentifier	<BICFI>	[1..1]	
2.25		Creditor Account			<CdtrAcct>	[0..1]	
2.26			Identification		<Id>	[0..1]	
2.27				IBAN	<IBAN>	[0..1]	
2.28		Purpose			<Purp>	[0..1]	Rulebook AT-44 The purpose of the ISO20022 Instruction.
2.29		Remittance Information			<RmtInf>	[0..1]	
2.30			Unstructured		<Ustrd>	[0..1]	Max140Text

7.1.4. Credit Transfer Return – pacs.004.001.13

The format uses the standard ISO schemas.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<PmtRtr>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Transaction Information	<TxInf>	[1..1]

Group Header

INDEX	MESSAGE ITEM				XML TAG	MULTIPLICITY	TYPE
1.0	Group Header				<GrpHdr>	[1..1]	
1.1		Message Identification			<MsgId>	[1..1]	Max35Text
1.2		Creation Date Time			<CreDtTm>	[1..1]	ISODateTime
1.3		Number Of Transactions			<NbOfTxs>	[1..1]	1
1.4		Total Returned Interbank Settlement Amount			<TtlRtrdIntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
1.5		Interbank Settlement Date			<IntrBkSttlmDt>	[1..1]	ISODate
1.6		Settlement Information			<SttlmInf>	[1..1]	
1.7			Settlement Method		<SttlmMtd>	[1..1]	Fixed text: ”CLRG”
1.8			Clearing System		<ClrSys>	[1..1]	
1.9				Code	<Cd>	[1..1]	
1.10		Instructing Agent			<InstgAgt>	[0..1]	
1.11			Financial Institution Identification		<FinInstnId>	[1..1]	
1.12				BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.13				Name	<Nm>	[0..1]	Max140Text
1.14		Instructed Agent			<InstdAgt>	[0..1]	
1.15			Financial Institution Identification		<FinInstnId>	[1..1]	
1.16				BICIdentifier	<BICFI>	[1..1]	BICIdentifier

Item Details

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
2.1	Transaction Information	<TxInf>	[1..1]	
2.2	Return Identification	<RtrId>	[1..1]	Max35Text
2.3	Original Group Information	<OrgnlGrpInf>	[0..1]	
2.4	Original Message Identification	<OrgnlMsgId>	[1..1]	Max35Text
2.5	Original Message Name Identification	<OrgnlMsgNmId>	[1..1]	Max35Text
2.6	Original End to End Identification	<OrgnlEndToEndId>	[1..1]	Max35Text
2.7	Original Transaction Identification	<OrgnlTxId>	[1..1]	Max35Text
2.8	Interbank Settlement Amount	<IntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
2.9	Original Interbank Settlement Amount	<OrgnlIntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
2.10	Returned Interbank Settlement Amount	<RtrdIntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
2.11	Charge Bearer	<ChrgBr>	[1..1]	Fixed text:"SLEV"
2.12	Return Reason Information	<RtrRsnInf>	[1..1]	
2.13	Originator	<Orgtr>	[1..1]	
2.14	Identification	<Id>	[1..1]	
2.15	Organization Id	<OrgId>	[1..1]	
2.16	BIC or BEI	<BICOrBEI>	[1..1]	AnyBICIdentifier

2.17			Reason		<Rsn>	[1..1]	
2.18				Code	<Cd>	[1..1]	
2.19		Original Transaction Reference			<OrgnlTxRef>	[1..1]	
2.20			Interbank Settlement Date		<IntrBkSttlmDt>	[1..1]	ISODate
2.21			Payment Type Information		<PmtTpInf>	[0..1]	
2.22				Service Level	<SvcLvl>	[0..1]	
2.23				Code	<Cd>	[1..1]	
2.24				Local Instrument	<LclInstrm>	[1..1]	
2.25				Code	<Cd>	[1..1]	
2.26				Category Purpose	<CtgyPurp>	[0..1]	Has child element Cd
2.27				Code	<Cd>	[1..1]	ExternalCategoryPurpose1Code
2.28			Remittance Information		<RmtInf>	[0..1]	
2.29				Unstructured	<Ustrd>	[0..1]	Max140Text
2.30				Structured	<Strd>	[0..1]	Only one occurrence of 'Structured' is allowed. 'Structured' can be used, provided the tags and the data within the 'Structured' element (i.e., excluding <Strd> and </Strd>) do not exceed 140 characters in length.

2.31					Creditor Reference Information			<CdtrRefInf>	[0..1]	
2.32						Code or Proprietary		<CdOrPrtry>	[1..1]	
2.33							Code	<Cd>	[1..1]	Fixed text “SCOR”
2.34						Issuer		<Issr>	[0..1]	Max35Text
2.35					Reference			<Ref>	[1..1]	Max35Text
2.36			Ultimate Debtor					<UltmtDbtr>	[0..1]	
2.37				Party Identification				<Pty>	[0..1]	
2.38					Name			<Nm>	[1..1]	Max70Text
2.39					Identification			<Id>	[0..1]	Rulebook AT-09 The identification code of the Originator Reference Party.
2.40			Debtor					<Dbtr>	[1..1]	
2.41				Party Identification				<Pty>	[0..1]	
2.42					Name			<Nm>	[1..1]	Max70Text
2.43					Postal Address			<PstlAdr>	[0..1]	Rulebook AT-03 The address of the Originator.
2.44					Id			<Id>	[0..1]	Rulebook AT-10 The Originator identification code.
2.45			Debtor Account					<DbtrAcct>	[1..1]	
2.46				Identification				<Id>	[1..1]	
2.47					IBAN			<IBAN>	[1..1]	

2.48			Debtor Agent			<DbtrAgt>	[1..1]	
2.49				Financial Institution Identification		<FinInstnId>	[1..1]	
2.50					BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.51					Name	<Nm>	[0..1]	Max140Text
2.52			Creditor Agent			<CdtrAgt>	[1..1]	
2.53				Financial Institution Id		<FinInstId>	[1..1]	
2.54					BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.55					Name	<Nm>	[0..1]	Max140Text
2.56			Creditor			<Cdtr>	[1..1]	
2.57				Party Identification		<Pty>	[0..1]	
2.58				Name		<Nm>	[1..1]	Max70Text
2.59				Postal Address		<PstlAdr>	[0..1]	Rulebook AT-22 The address of the Beneficiary.
2.60				Id		<Id>	[0..1]	Rulebook AT-24 The Beneficiary identification code.
2.61			Creditor Account			<CdtrAcct>	[1..1]	
2.62				Identification		<Id>	[1..1]	
2.63					IBAN	<IBAN>	[1..1]	
2.64			Ultimate Creditor			<UltmtCdtr>	[0..1]	
2.65				Party Identification		<Pty>	[0..1]	
2.66				Name		<Nm>	[1..1]	Max70Text

2.67					Id	<Id>	[0..1]	Rulebook AT-29 Identification code of the Beneficiary Reference Party.

7.1.5. Recall Message – camt.056.001.11

The format uses the standard ISO schemas in the following structure..

INDEX		MESSAGE ITEM		XML TAG	MULTIPLICITY
1	Message Root			<FIToFIPmtCxlReq>	[1..1]
2		Group Header		<Assgnmt>	[1..1]
3		Transaction Batch Information		<Undrlyg>	[1..1]
4			Transaction Information	<TxInf>	[1..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<Assgnmt>	[1..1]	
1.1	Message Identification	<Id>	[1..1]	Max35Text
1.2	Instructing Agent	<Assgnr>	[0..1]	
1.3	Agent	<Agt>	[1..1]	
1.4	Financial Institution Identification	<FinInstnId>	[1..1]	
1.5	BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.6	Instructed Agent	<Assgne>	[0..1]	
1.7	Agent	<Agt>	[1..1]	
1.8	Financial Institution Identification	<FinInstnId>	[1..1]	
1.9	BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.10	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime

Item Details

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
2.1	Transaction Information	<TxInf>	[1..1]	
2.2	Recall Identification	<CxlId>	[1..1]	Max35Text
2.3	Original Group Information	<OrgnlGrpInf>	[0..1]	
2.4	Original Message Identification	<OrgnlMsgId>	[1..1]	Max35Text

2.5			Original Message Name Identification	<OrgnlMsgNmId>	[1..1]	Max35Text
2.6		Original End To End Identification		<OrgnlEndToEndId>	[1..1]	Max35Text
2.7		Original Transaction Identification		<OrgnlTxId>	[1..1]	Max35Text
2.8		Original Interbank Settlement Amount		<OrgnlIntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
2.9		Original Interbank Settlement Date		<OrgnlIntrBkSttlmDt>	[1..1]	ISODate
2.10		Cancellation Reason Information		<CxlRsnInf>	[1..1]	
2.11			Originator	<Orgtr>	[1..1]	
2.12			Identification	<Id>	[1..1]	
2.13			Organization Id	<OrgId>	[1..1]	
2.14			BIC or BEI	<BICOrBEI>	[1..1]	
2.15			Reason	<Rsn>	[1..1]	
2.16			Code	<Cd>	[1..1]	
2.17		Original Transaction Reference		<OrgnlTxRef>	[1..1]	
2.18			Interbank Settlement Date	<IntrBkSttlmDt>	[1..1]	ISODate
2.19			Settlement Instruction	<SttlmInf>	[0..1]	
2.20			Clearing System	<ClrSys>	[0..1]	
2.21			Code	<Cd>	[0..1]	
2.22			Payment Type Information	<PmtTpInf>	[0..1]	
2.23			Service Level	<SvcLvl>	[0..1]	
2.24			Code	<Cd>	[0..1]	
2.25			Local Instrument	<LclInstrm>	[1..1]	

2.26					Code	<Cd>	[0..1]	
2.27			Remittance Information			<RmtInf>	[0..1]	
2.28				Unstructured		<Ustrd>	[0..1]	Max140Text
2.29				Structured		<Strd>	[0..1]	Only one occurrence of 'Structured' is allowed. 'Structured' can be used, provided the tags and the data within the 'Structured' element (i.e. excluding <Strd> and </Strd>) do not exceed 140 characters in length.
2.30					Creditor Reference Information	<CdtrRefInf>	[0..1]	
2.31					Creditor Reference Type	<Tp>	[1..1]	
2.32					Code or Proprietary	<CdOrPrtry>	[1..1]	
2.33					Code	<Cd>	[1..1]	Fixed text "SCOR"
2.34					Issuer	<Issr>	[0..1]	Max35Text
2.35					Reference	<Ref>	[1..1]	Max35Text
2.36			Ultimate Debtor			<UltmtDbtr>	[0..1]	
2.37				Party Identification		<Pty>	[0..1]	
2.38				Name		<Nm>	[1..1]	Max70Text
2.39				Id		<Id>	[0..1]	Rulebook AT-09 The identification code of the Originator Reference Party.

2.40			Debtor	<Dbtr>	[1..1]	
2.41			Party Identification	<Pty>	[0..1]	
2.42			Name	<Nm>	[1..1]	Max70Text
2.43			Postal Address	<PstlAdr>	[0..1]	Rulebook AT-03 The address of the Originator.
2.44			Id	<Id>	[0..1]	Rulebook AT-10 The Originator's identification code.
2.45			Debtor Account	<DbtrAcct>	[1..1]	
2.46			Identification	<Id>	[1..1]	
2.47			IBAN	<IBAN>	[1..1]	
2.48			Debtor Agent	<DbtrAgt>	[1..1]	
2.49			Financial Institution Identification	<FinInstnId>	[1..1]	
2.50			BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.51			Name	<Nm>	[0..1]	Max140Text
2.52			Creditor Agent	<CdtrAgt>	[1..1]	
2.53			Financial Institution Id	<FinInstId>	[1..1]	
2.54			BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.55			Name	<Nm>	[0..1]	Max140Text
2.56			Creditor	<Cdtr>	[1..1]	
2.57			Party Identification	<Pty>	[0..1]	
2.58			Name	<Nm>	[1..1]	Max70Text

2.59						Postal Address	<PstlAdr>	[0..1]	Rulebook AT-22 The address of the Originator.
2.60						Id	<Id>	[0..1]	Rulebook AT-24 The Originator's identification code.
2.61			Creditor Account				<CdtrAcct>	[1..1]	
2.62				Identification			<Id>	[1..1]	
2.63					IBAN		<IBAN>	[1..1]	
2.64			Ultimate Creditor				<UltmtCdtr>	[0..1]	
2.65				Party Identification			<Pty>	[0..1]	
2.66						Name	<Nm>	[1..1]	Max70Text
2.67						Id	<Id>	[0..1]	Rulebook AT-29 The Originator's identification code.

7.1.6. Negative Answer to Recall – camt.029.001.13

The format uses the standard ISO schemas in the following structure.

INDEX		MESSAGE ITEM		XML TAG	MULTIPLICITY
1	Message Root			<RsltnOfInvstgtn>	[1..1]
2		Group Header		<Assgnmt>	[1..1]
3		Status		<Sts>	[1..1]
4			Conf	<Conf>	[1..1] RJCR
5		Transaction Batch Information		<CxlDtls>	[1..1]
6			Transaction Information	<TxInfAndSts>	[1..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<Assgnmt>	[1..1]	
1.1	Message Identification	<Id>	[1..1]	Max35Text
1.2	Instructing Agent	<Assgnr>	[0..1]	
1.3	Agent	<Agt>	[1..1]	
1.4	Financial Institution Identification	<FinInstnId>	[1..1]	
1.5	BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.6	Instructed Agent	<Assgne>	[0..1]	
1.7	Agent	<Agt>	[1..1]	
1.8	Financial Institution Identification	<FinInstnId>	[1..1]	
1.9	BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.10	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime

Item Details

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
2.1	Transaction Information	<TxInfAndSts>	[1..1]	
2.2	Recall NAK Identification	<CxlStsId>	[1..1]	Max35Text
2.3	Original Group Information	<OrgnlGrpInf>	[0..1]	

2.4			Original Message Identification							<OrgnlMsgId>	[1..1]	Max35Text
2.5			Original Message Name Identification							<OrgnlMsgNmId>	[1..1]	Max35Text
2.6		Original End To End Identification								<OrgnlEndToEndId>	[1..1]	Max35Text
2.7		Original Transaction Identification								<OrgnlTxId>	[1..1]	Max35Text
2.8		Cancellation status								<TxCxlSts>	[1..1]	RJCR
2.9		Cancellation Status Reason Information								<CxlStsRsnInf >	[1..1]	
2.10			Originator							<Orgtr>	[1..1]	
2.11				Identification						<Id>	[1..1]	
2.12					Organization Id					<OrgId>	[1..1]	
2.13						BIC or BEI				<BICOrBEI>	[1..1]	
2.14			Reason							<Rsn>	[1..1]	
2.15				Code						<Cd>	[1..1]	
2.16		Original Transaction Reference								<OrgnlTxRef>	[1..1]	
2.17			Interbank Settlement Amount							<IntrBkSttlmAmt>	[1..1]	ActiveCurrencyAndAmount
2.18			Interbank Settlement Date							<IntrBkSttlmDt>	[1..1]	ISODate
2.19			Settlement Information							<SttlmInf>	[1..1]	
2.20				Settlement Method						<SttlmMtd>	[1..1]	Fixed text:”CLRG”
2.21				Clearing System						<ClrSys>	[1..1]	
2.22					Cd					<Cd>	[1..1]	
2.23			Payment Type Information							<PmtTpInf>	[0..1]	
2.24				Service Level						<SvcLvl>	[0..1]	

2.25					Code			<Cd>	[1..1]	
2.26				Local Instrument				<LclInstrm>	[1..1]	
2.27					Code			<Cd>	[1..1]	
2.28			Remittance Information					<RmtInf>	[0..1]	
2.29				Unstructured				<Ustrd>	[0..1]	Max140Text
2.30				Structured				<Strd>	[0..1]	Only one occurrence of 'Structured' is allowed. 'Structured' can be used, provided the tags and the data within the 'Structured' element (i.e. excluding <Strd> and </Strd>) do not exceed 140 characters in length.
2.31					Creditor Reference Information			<CdtrRefInf>	[0..1]	
2.32						Creditor Reference Type		<Tp>	[1..1]	
2.33							Code or Proprietary	<CdOrPrtry>	[1..1]	
2.34								Code	<Cd>	[1..1]	Fixed text "SCOR"
2.35							Issuer	<Issr>	[0..1]	Max35Text
2.36						Reference		<Ref>	[1..1]	Max35Text
2.37			Ultimate Debtor					<UltmtDbtr>	[0..1]	
2.38				Party Identification				<Pty>	[0..1]	
2.39					Name			<Nm>	[1..1]	Max70Text
2.40					Id			<Id>	[0..1]	Rulebook AT-09 The Identification Code of the

								Originator Reference Party.
2.41			Debtor			<Dbtr>	[1..1]	
2.42				Party Identification		<Pty>	[0..1]	
2.43					Name	<Nm>	[1..1]	Max70Text
2.44					Postal Address	<PstlAdr>	[0..1]	Rulebook AT-03 The address of the Originator
2.45					Id	<Id>	[0..1]	Rulebook AT-10 The Originator identification Code.
2.46			Debtor Account			<DbtrAcct>	[1..1]	
2.47				Identification		<Id>	[1..1]	
2.48					IBAN	<IBAN>	[1..1]	
2.49			Debtor Agent			<DbtrAgt>	[1..1]	
2.50				Financial Institution Identification		<FinInstnId>	[1..1]	
2.51					BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.52					Name	<Nm>	[0..1]	Max140Text
2.53			Creditor Agent			<CdtrAgt>	[1..1]	
2.54				Financial Institution Id		<FinInstId>	[1..1]	
2.55					BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.56					Name	<Nm>	[0..1]	Max140Text
2.57			Creditor			<Cdtr>	[1..1]	
2.58				Party Identification		<Pty>	[0..1]	

2.59					Name	<Nm>	[1..1]	Max70Text
2.60					Postal Address	<PstlAdr>	[0..1]	Rulebook AT-22 The address of the Beneficiary.
2.61					Id	<Id>	[0..1]	Rulebook AT-24 The Beneficiary identification code.
2.62			Creditor Account			<CdtrAcct>	[1..1]	
2.63				Identification		<Id>	[1..1]	
2.64					IBAN	<IBAN>	[1..1]	
2.65			Ultimate Creditor			<UltmtCdtr>	[0..1]	
2.66				Party Identification		<Pty>	[0..1]	
2.67					Name	<Nm>	[1..1]	Max70Text
2.68					Id	<Id>	[0..1]	Rulebook AT-29 The identification code of the Beneficiary Reference Party.

7.1.7. Investigation – pacs.028.001.06

The format uses the standard ISO schemas in the following structure. A restriction of a single investigation is enforced.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<FIToFIPmtStsReq>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Transaction Information	<TxInf>	[1..1]

Group Header

INDEX	MESSAGE ITEM				XML TAG	MULTIPLICITY	TYPE
1.0	Group Header				<GrpHdr>	[1..1]	
1.1		Message Identification			<MsgId>	[1..1]	Max35Text
1.2		Creation Date Time			<CreDtTm>	[1..1]	ISODateTime
1.3		Instructing Agent			<InstgAgt>	[1..1]	
1.4			Financial Institution Identification		<FinInstnId>	[1..1]	
1.5				BICFIIdentifier	<BICFI>	[1..1]	BICFIIdentifier
1.6				Name	<Nm>	[0..1]	Max140Text

Original Group Information

INDEX	MESSAGE ITEM		XML TAG	MULTIPLICITY	TYPE
2.1	Original Group Information		<OrgnlGrpInf>	[0..1]	
2.2		Original Message Identification	<OrgnlMsgId>	[1..1]	Max35Text
2.3		Original Message Name Identification	<OrgnlMsgNmId>	[1..1]	Max35Text

Item Details

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE

3.1	Transaction Information					<TxInf>	[1..1]	
3.2		Request Identification				<StsReqId>	[1..1]	Max35Text
3.3		Original End To End Identification				<OrgnlEndToEndId>	[1..1]	Max35Text
3.4		Original Transaction Identification				<OrgnlTxId>	[1..1]	Max35Text
3.5		Acceptance Date Time				<AccptncDtTm>	[1..1]	ISODateTime
3.6		Original Transaction Reference				<OrgnlTxRef>	[1..1]	
3.7			Payment Type Information			<PmtTpInf>	[0..1]	
3.8				Service Level		<SvcLvl>	[0..1]	
3.9					Code	<Cd>	[1..1]	
3.10				Local Instrument		<LclInstrm>	[1..1]	
3.11					Code	<Cd>	[1..1]	
3.12			Debtor Agent			<DbtrAgt>	[1..1]	
3.14				Financial Institution Id		<FinInstId>	[1..1]	
3.15					BICFIIdentifier	<BICFI>	[1..1]	BICFIIdentifier
3.16					Name	<Nm>	[0..1]	Max140Text
3.17			Creditor Agent			<CdtrAgt>	[0..1]	
3.18				Financial Institution Id		<FinInstId>	[1..1]	
3.19					BICFIIdentifier	<BICFI>	[1..1]	BICFIIdentifier
3.20					Name	<Nm>	[0..1]	Max140Text

7.1.8. Payment Confirmation/Rejection Message – pacs.002.001.014

The format uses the standard ISO schemas in the following structure.

When the original message (pacs.008) is rejected due to xsd schema validation, participants can opt to receive additional information in the pacs.002 message. In this case, the AddtlInf field is added containing an xpath pointing to the element in which the issue was identified. For example: <AddtlInf>1000-01-01 below the supported minimum Mon Jan 01 00:00:00 EET 1753 at env:Message>env:FIToFICstmrCdtTrf></AddtlInf>.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<FIToFIPmtStsRpt>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Original Group Info and Status	<OrgnlGrpInfAndSts>	[1..1]
4		Original Payment Info and Status	<TxInfAndSts>	[0..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<GrpHdr>	[1..1]	
1.1	Message Identification	<MsgId>	[1..1]	Max35Text
1.2	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime
1.3	Instructing Agent	<InstgAgt>	[0..1]	
1.4	Financial Institution Identification	<FinInstnId>	[1..1]	
1.5	BIC	<BICFI>	[0..1]	AnyBICIdentifier
1.6	Name	<Nm>	[0..1]	Max140Text

Original Group Info and Status

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
2.1	Original Group Info and Status	<OrgnlGrpInfAndSts>	[1..1]	
2.2	Original Message Identification	<OrgnlMsgId>	[1..1]	Max35Text
2.3	Original Message Name Identification	<OrgnlMsgNmId>	[1..1]	Max35Text
2.4	Group Status	<GrpSts>	[0..1]	Fixed text:"ACCP","RJCT"
2.5	Status Reason Information	<StsRsnInf>	[0..1]	
2.6	Reason	<Rsn>	[0..1]	
2.7	Code	<Cd>	[1..1]	Reason code
2.8	Additional Information	<AddtlInf>	[0..1]	Max105Text

Original Payment Info and Status

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
3.1	Original Payment Info and Status	<TxInfAndSts>	[0..1]	
3.2	Status Identification	<StsId>	[1..1]	Max35Text
3.3	Original End to End Identification	<OrgnlEndToEndId>	[1..1]	Max35Text
3.4	Original Transaction Identification	<OrgnlTxId>	[1..1]	Max35Text
3.5	Payment Information Status	<TxSts>	[0..1]	RJCT, only if GrpSts is not set
3.6	Status Reason Information	<StsRsnInf>	[0..1]	
3.7	Originator	<Orgtr>	[1..1]	
3.8	Name	<Nm>	[0..1]	Max70Text
3.9	Identification	<Id>	[0..1]	
3.10	Organization Id	<OrgId>	[1..1]	
3.11	BIC or BEI	<BICOrBEI>	[1..1]	AnyBICIdentifier
3.12	Reason	<Rsn>	[0..1]	
3.13	Code	<Cd>	[1..1]	External Reason Code
3.14	Acceptance Date and time	<AccptncDtTm>	[1..1]	ISODateTime
3.15	Original Transaction Information	<OrgnlTxRef>	[1..1]	

3.16			Payment type Information			<PmtTpInf>	[1..1]	
3.17				Service Level		<SvcLvl>	[1..1]	
3.18					Code	<Cd>	[1..1]	
3.19				Local Instrument		<LclInstrm>	[1..1]	
3.20					Code	<Cd>	[1..1]	INST
3.21				Category Purpose		<CtgyPurp>	[0..1]	Has child element Cd
3.22					Code	<Cd>	[1..1]	ExternalCategoryPurpose1 Code
3.23			Debtor Agent			<DbtrAgt>	[1..1]	
3.24				Financial Institution Identification		<FinInstnId>	[1..1]	
3.25					BIC	<BICFI>	[0..1]	AnyBICIdentifier
3.26					Name	<Nm>	[0..1]	Max140Text

7.1.9. Request To Pay – pain.013.001.11

The format uses the standard ISO schemas in the following structure.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<CdtrPmtActvtnReq>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Payment Information	<PmtInf>	[1..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<GrpHdr>	[1..1]	
1.1	Message Identification	<MsgId>	[1..1]	Max35Text
1.2	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime
1.3	Number of Transactions	<NbOfTxs>	[1..1]	1
1.4	Initiating Party	<InitgPty>	[1..1]	
1.5	Name	<Nm>	[0..1]	
1.6	Identification	<Id>	[0..1]	
1.7	OrgId	<OrgId>	[1..1]	
1.8	Any BIC	<AnyBIC>	[0..1]	AnyBICIdentifier

Item Details

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
2.1	Payment Information	<PmtInf>	[1..1]	
2.2	Payment Information Identification	<PmtInfId>	[1..1]	Max35Text
2.3	Payment Method	<PmtMtd>	[1..1]	Fixed text:"TRF"
2.4	Payment Type Information	<PmtTpInf>	[0..1]	
2.5	Instruction Priority	<InstrPrty>	[0..1]	Allowed values "HIGH"/"NORM" to indicate payments for RTP fast/slow flows.

2.6			Service Level	<SvcLvl>	[0..1]	
2.7			Code	<Cd>	[1..1]	external service level code
2.8			Local Instrument	<LclInstrm>	[0..1]	
2.9			Code	<Cd>	[1..1]	
2.10			Category Purpose	<CtgyPurp>	[0..1]	Has child element Cd
2.11			Code	<Cd>	[1..1]	ExternalCategoryPurpose1Code
2.12		Requested Execution Date		<ReqdExctnDt>	[1..1]	
2.13			Date	<Dt>	[0..1]	ISODate
2.14			Date Time	<DtTm>	[0..1]	
2.15			Expiration Date	<XpryDt>	[1..1]	
2.16			Date	<Dt>	[0..1]	ISODate
2.17			Date Time	<DtTm>	[0..1]	
2.18		Debtor		<Dbtr>	[1..1]	
2.19			Name	<Nm>	[0..1]	Max140Text
2.20			Identification	<Id>	[0..1]	
2.21			Organization Identification	<OrdId>	[1..1]	
2.22			Any BIC	<AnyBIC>	[0..1]	AnyBICIdentifier
2.23		Debtor Account		<DbtrAcct>	[1..1]	
2.24			Identification	<Id>	[1..1]	
2.25			IBAN	<IBAN>	[1..1]	IBAN2007Identifier
2.26		Debtor Agent		<DbtrAgt>	[1..1]	

2.27			Financial Institution Identification	<FinInstnId>	[1..1]	
2.28			BICFI Identifier	<BICFI>	[1..1]	BICFIDec2014Identifier
2.29			Name	<Nm>	[0..1]	Max140Text
2.30		Ultimate Debtor		<UltmtDbtr>	[0..1]	
2.31			Name	<Nm>	[0..1]	Max140Text
2.32		Credit Transfer Transaction		<CdtTrfTx>	[1..1]	
2.33			Payment Identification	<PmtId>	[1..1]	
2.34			Instruction Identification	<InstrId>	[0..1]	Max35Text
2.35			End to End Id	<EndToEndI>	[1..1]	Max35Text
2.36			Amount	<Amt>		
2.37			Instructed Amount	<InstdAmt>	[1..1]	ActiveOrHistoric CurrencyAndAmount
2.38			Charge Bearer	<ChrgBr>	[1..1]	Fixed text “SLEV”
2.39			Creditor Agent	<CdtrAgt>	[0..1]	
2.40			Financial Institution Identification	<FinInstnId>	[1..1]	
2.41			BICFI Identifier	<BICFI>	[0..1]	BICFIDec2014Identifier
2.42			Name	<Nm>	[0..1]	Max140Text
2.43			Creditor	<Cdtr>	[0..1]	
2.44			Name	<Nm>	[0..1]	Max140Text
2.45			Identification	<Id>	[0..1]	

2.46					Organization Identification						<OrgId>	[0..1]	
2.47						AnyBIC					<AnyBIC>	[0..1]	AnyBICIdentifier
2.48						Other					<Othr>	[0..n]	
2.49							Id				<Id>	[1..1]	MCC code
2.50							Scheme Name				<SchmNm>	[0..1]	
2.51								Code			<Cd>	[1..1]	Fixed text “BDID”
2.52					Private Identification						<PrvtId>	[0..1]	
2.53						Other					<Othr>	[0..n]	
2.54							Id				<Id>	[1..1]	
2.55			Creditor Account								<CdtrAcct>	[0..1]	
2.56				Identification							<Id>	[1..1]	
2.57					IBAN						<IBAN>	[1..1]	IBAN2007Identifier
2.58			Ultimate Creditor								<UltmtCdtr>	[0..1]	
2.59				Name							<Nm>	[0..1]	Max140Text
2.60				Purpose							<Purp>	[1..1]	
2.61					Code						<Cd>	[1..1]	
2.62			Related Remittance Information								<RltdRmtInf>	[0..1]	
2.63				Remittance Identification							<RmtId>	[0..1]	Max140Text
2.64				Remittance Location Details							<RmtLctnDtls>	[0..n]	

2.65					Method			<Mtd>	[1..1]	Fixed text: “FAXI”, “EDIC”, “URID”, “EMAL”, “POST”, “SMSM”
2.66					Electronic Address			<ElctrncAdr>	[0..1]	Max2048Text
2.67			Remittance Information					<RmtInf>	[0..1]	
2.68				Unstructured				<Ustrd>	[1..1]	Max140Text
2.69				Structured				<Strd>	[0..1]	Only one occurrence of ‘Structured’ is allowed. ‘Structured’ can be used, provided the tags and the data within the ‘Structured’ element (i.e. excluding <Strd> and </Strd>) do not exceed 140 characters in length.
2.70					Creditor Reference Information			<CdtrRefInf>	[0..1]	
2.71						Creditor Reference Type		<Tp>	[1..1]	
2.72							Code or Proprietary	<CdOrPrtry>	[1..1]	
2.73								Code	<Cd>	[1..1]	Fixed text “SCOR”
2.74							Issuer	<Issr>	[0..1]	Max35Text
2.75						Reference		<Ref>	[1..1]	Max35Text

7.1.10. Request to Pay Response – pain.014.001.11

The format uses the standard ISO schemas in the following structure.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<CdtrPmtActvtnReqStsRpt>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Original Group Info and Status	<OrgnlGrpInfAndSts>	[1..1]
4		Original Payment Info and Status	<OrgnlPmtInfAndSts>	[1..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<Assgnmt>	[1..1]	
1.1	Message Identification	<MsgId>	[1..1]	Max35Text
1.2	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime
1.3	Initiating Party	<InitgPty>	[0..1]	
1.4	Identification	<Id>	[0..1]	
1.5	Organization Identification	<OrgId>	[1..1]	
1.6	Any BIC	<AnyBIC>	[0..1]	AnyBICIdentifier

Original Group Info and Status

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
2.1	Original Group Info and Status	<OrgnlGrpInfAndSts>	[1..1]	
2.2	Original Message Identification	<OrgnlMsgId>	[1..1]	Max35Text
2.3	Original Message Name Identification	<OrgnlMsgNmId>	[1..1]	Max35Text
2.4	Original Creation Date Time	<OrgnlCreDtTm>	[0..1]	ISODateTime
2.5	Original Number of Transactions	<OrgnlNbOfTxs>	[0..1]	Max15NumericText
2.6	Group Status	<GrpSts>	[0..1]	External payment status code
2.7	Status Reason Information	<StsRsnInf>	[0..1]	
2.8	Reason	<Rsn>	[0..1]	

2.9				Code	<Cd>	[1..1]	External reason code

Original Payment Info and Status

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
3.1	Original Payment Info and Status	<OrgnlPmtInfAndSts>	[0..1]	
3.2	Original Payment Information Identification	<OrgnlPmtInfId>	[1..1]	Max35Text
3.3	Payment Information Status	<PmtInfSts>	[0..1]	
3.4	Transaction Information and Status	<TxInfAndSts>	[0..1]	
3.5	Transaction Status	<TxSts>	[0..1]	External status code
3.6	Status Reason Information	<StsRsnInf>	[0..1]	
3.7	Reason	<Rsn>	[0..1]	
3.8	Code	<Cd>	[1..1]	External reason code
3.9	Original Transaction Reference	<OrgnlTxRef>	[0..1]	
3.10	Amount	<Amt>	[0..1]	
3.11	Instructed Amount	<InstdAmt>	[1..1]	ActiveOrHistoricCurrencyAndAmount
3.12	Requested Execution Date	<ReqdExctnDt>	[0..1]	
3.13	Date	<Dt>	[0..1]	ISODate
3.14	Date Time	<DtTm>	[0..1]	
3.15	Payment Type Info	<PmtTpInf>	[0..1]	
3.16	Service Level	<SvcLvl>	[0..1]	
3.17	Code	<Cd>	[1..1]	External service code

3.18					Local Instrument						<LclInstrm>	[0..1]	
3.19						Code					<Cd>	[1..1]	
3.20				Remittance Information							<RmtInf>	[0..1]	
3.21					Unstructured						<Ustrd>	[0..1]	Max140Text
3.22					Structured						<Strd>	[0..1]	Only one occurrence of 'Structured' is allowed. 'Structured' can be used, provided the tags and the data within the 'Structured' element (i.e. excluding <Strd> and </Strd>) do not exceed 140 characters in length.
3.23						Creditor Reference Information					<CdtrRefInf>	[0..1]	
3.24							Creditor Reference Type				<Tp>	[1..1]	
3.25								Code or Proprietary			<CdOrPrtry>	[1..1]	
3.26									Code		<Cd>	[1..1]	Fixed text "SCOR"
3.27								Issuer			<Issr>	[0..1]	Max35Text
3.28							Reference				<Ref>	[1..1]	Max35Text
3.29				Debtor							<Dbtr>	[0..1]	
3.30					Name						<Nm>	[0..1]	Max140Text
3.31				Debtor Account							<DbtrAcct>	[0..1]	
3.32					Identification						<Id>	[1..1]	
3.33						IBAN					<IBAN>	[1..1]	IBAN2007Identifier

3.34				Debtor Agent				<DbtrAgt>	[0..1]	
3.35					Financial Institution Identification			<FinInstnId>	[1..1]	
3.36						BICFI Identifier		<BICFI>	[0..1]	BICFIDec2014Identifier
3.37						Name		<Nm>	[0..1]	Max140Text
3.38				Creditor Agent				<CdtrAgt>	[1..1]	
3.39					Financial Institution Identification			<FinInstnId>	[1..1]	
3.40						BICFI Identifier		<BICFI>	[0..1]	BICFIDec2014Identifier
3.41						Name		<Nm>	[0..1]	Max140Text
3.42				Creditor				<Cdtr>	[1..1]	
3.43					Name			<Nm>	[0..1]	Max140Text
3.44					Id			<Id>		
3.45						Other		<Othr>	[0..n]	
3.46							Id	<Id>	[1..1]	MCC code
3.47							Scheme Name	<SchmNm>	[0..1]	
3.48								Code	<Cd>	[1..1]	Fixed text “BDID”
3.49				Creditor Account				<CdtrAcct>	[0..1]	
3.50					Identification			<Id>	[1..1]	
3.51						IBAN		<IBAN>	[1..1]	IBAN2007Identifier

7.1.11. Payment Initiation – pain.001.001.012

The format uses the standard ISO schemas in the following structure. A restriction of a single payment information is enforced.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<CstmrCdtTrfInitn>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Payment Information	<PmtInf>	[1..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<GrpHdr>	[1..1]	
1.1	Message Identification	<MsgId>	[1..1]	Max35Text
1.2	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime
1.3	Number of Transactions	<NbOfTxs>	[1..1]	1
1.4	Control Sum	<CtrlSum>	[1..1]	DecimalNumber
1.5	Initiating Party	<InitgPty>	[1..1]	
1.7	Name	<Nm>	[0..1]	
1.8	Identification	<Id>	[0..1]	
1.9	OrgId	<OrgId>	[1..1]	
1.10	BIC or BEI	<BICOrBEI>	[0..1]	AnyBICIdentifier

Item Details

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
2.1	Payment Information	<PmtInf>	[1..1]	
2.2	Payment Information Identification	<PmtInfId>	[1..1]	Max35Text
2.3	Payment Method	<PmtMtd>	[1..1]	Fixed text:"TRF"
2.4	Payment Type Information	<PmtTpInf>	[0..1]	
2.5	Service Level	<SvcLvl>	[0..1]	

2.6				Code	<Cd>	[1..1]	external service level code
2.7			Local Instrument		<LclInstrm>	[0..1]	
2.8				Code	<Cd>	[1..1]	
2.9			Category Purpose		<CtgyPurp>	[0..1]	Has child element Cd
2.10				Code	<Cd>	[1..1]	ExternalCategoryPurpose1Code
2.11		Requested Execution Date			<ReqdExctnDt>	[1..1]	ISODate
2.12		Debtor			<Dbtr>	[1..1]	
2.13			Name		<Nm>	[1..1]	Max70Text
2.14			Postal Address		<PstlAdr>	[0..1]	Rulebook AT-03 The address of the Originator
2.15			Identification		<Id>	[0..1]	Rulebook AT-10 The Originator identification code
2.16		Debtor Account			<DbtrAcct>	[1..1]	
2.17			Identification		<Id>	[1..1]	
2.18				IBAN	<IBAN>	[1..1]	IBAN2007Identifier
2.19		Debtor Agent			<DbtrAgt>	[1..1]	
2.20			Financial Institution Identification		<FinInstnId>	[1..1]	
2.21				BIC Identifier	<BICFI>	[1..1]	AnyBICIdentifier
2.22				Name	<Nm>	[0..1]	Max140Text

2.23		Ultimate Debtor			<UltmtDbtr>	[0..1]	
2.24			Name		<Nm>	[0..1]	Max70Text
2.25			Id		<Id>	[0..1]	Rulebook AT-09 The identification code of the Originator Reference Party
2.26		Charge Bearer			<ChrgBr>	[0..1]	Fixed text:"SLEV"
2.27		Credit Transfer Transaction Information			<CdtTrfTxinf>	[1..1]	
2.28			Payment Identification		<PmtId>	[1..1]	
2.29				Instruction Identification	<InstrId>	[0..1]	Max35Text
2.30				End to End Id	<EndToEndI>	[1..1]	Max35Text
2.31			Amount		<Amt>		
2.32				Instructed Amount	<InstdAmt>	[1..1]	ActiveOrHistoric CurrencyAndAmount
2.33			Creditor Agent		<CdtrAgt>	[0..1]	
2.34				Financial Institution Identification	<FinInstnId>	[1..1]	
2.35				BIC Identifier	<BICFI>	[0..1]	AnyBICIdentifier
2.36				Name	<Nm>	[0..1]	Max140Text
2.37			Creditor		<Cdtr>	[0..1]	
2.38				Name	<Nm>	[0..1]	Max70Text
2.39				Postal Address	<PstlAdr>	[0..1]	Rulebook AT-22 The address of the Beneficiary.

2.40				Identification	<Id>	[0..1]	Rulebook AT-24 The Beneficiary identification code.
2.41			Creditor Account		<CdtrAcct>	[0..1]	
2.42				Identification	<Id>	[1..1]	
2.43				IBAN	<IBAN>	[1..1]	IBAN2007Identifier
2.44			Ultimate Creditor		<UltmtCdtr>	[0..1]	
2.45				Name	<Nm>	[0..1]	Max70Text
2.46				Id	<Id>	[0..1]	Rulebook AT-29 The identification code of the Beneficiary Reference Party.
2.47			Purpose		<Purp>	[0..1]	Rulebook AT-44 The purpose of the ISO20022 Instruction.
2.48			Remittance Information		<RmtInf>	[0..1]	
2.49				Unstructured	<Ustrd>	[1..1]	Max140Text
2.50				Structured	<Strd>	[0..1]	Only one occurrence of 'Structured' is allowed. 'Structured' can be used, provided the tags and the data within the 'Structured' element (i.e. excluding <Strd> and </Strd>) do not

											exceed 140 characters in length.
2.51					Creditor Reference Information				<CdtrRefInf>	[0..1]	
2.52						Creditor Reference Type			<Tp>	[1..1]	
2.53							Code or Proprietary		<CdOrPrtry>	[1..1]	
2.54								Code	<Cd>	[1..1]	Fixed text “SCOR”
2.55							Issuer		<Issr>	[0..1]	Max35Text

7.1.12. Status Report – pain.002.001.14

The format uses the standard ISO schemas in the following structure. A restriction of a single payment information is enforced.

When the original message is rejected due to xsd schema validation, participants can opt to receive additional information in the pain.002 message. In this case, the AddtlInf field is added containing an xpath pointing to the element in which the issue was identified.

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root	<CstmrPmtStsRpt>	[1..1]
2	Group Header	<GrpHdr>	[1..1]
3	Original Group Info and Status	<OrgnlGrpInfAndSts>	[1..1]
4	Original Payment Info and Status	<OrgnlPmtInfAndSts>	[0..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<GrpHdr>	[1..1]	
1.1	Message Identification	<MsgId>	[1..1]	Max35Text
1.2	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime
1.3	Debtor Agent	<DbtrAgt>	[0..1]	
1.4	Financial Institution Identification	<FinInstnId>	[1..1]	
1.5	BIC	<BICFI>	[0..1]	AnyBICIdentifier
1.6	Name	<Nm>	[0..1]	Max140Text

Original Group Info and Status

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
2.1	Original Group Info and Status	<OrgnlGrpInfAndSts>	[1..1]	
2.2	Original Message Identification	<OrgnlMsgId>	[1..1]	Max35Text
2.3	Original Message Name Identification	<OrgnlMsgNmId>	[1..1]	Max35Text
2.4	Group Status	<GrpSts>	[0..1]	Fixed text:"ACTC","RJCT"
2.5	Status Reason Information	<StsRsnInf>	[0..1]	
2.6	Reason	<Rsn>	[0..1]	

2.7				Code	<Cd>	[1..1]	External reason code
2.8			Additional information		<AddtlInf>	[0..1]	Up to 105 characters description

Original Payment Info and Status

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
3.1	Original Payment Info and Status	<OrgnlPmtInfAndSts>	[0..1]	
3.2	Original Payment Information Identification	<OrgnlPmtInfId>	[1..1]	Max35Text
3.3	Payment Information Status	<PmtInfSts>	[0..1]	
3.4	Status Reason Information	<StsRsnInf>	[0..1]	
3.5	Originator	<Orgtr>	[1..1]	
3.6	Name	<Nm>	[0..1]	Max140Text
3.7	Reason	<Rsn>	[0..1]	
3.8	Code	<Cd>	[1..1]	External Reason Code
3.9	Additional information	<AddtlInf>	[0..1]	Up to 105 characters description

7.1.13. Customer Payment Cancellation Request – camt.055.001.012

The format uses the standard ISO schemas in the following structure.

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root	<CstmrPmtCxlReq>	[1..1]
2	Group Header	<Assgnmt>	[1..1]
3	Transaction Batch Information	<Undrlyg>	[1..1]
4	Transaction Information	<OrgnlPmtInfAndCxl>	[1..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<Assgnmt>	[1..1]	
1.1	Message Identification	<Id>	[1..1]	Max35Text
1.2	Instructing Agent	<Assgnr>	[0..1]	
1.3	Agent	<Agt>	[1..1]	
1.4	Financial Institution Identification	<FinInstnId>	[1..1]	
1.5	BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.6	Instructed Agent	<Assgne>	[0..1]	
1.7	Agent	<Agt>	[1..1]	
1.8	Financial Institution Identification	<FinInstnId>	[1..1]	
1.9	BICIdentifier	<BICFI>	[1..1]	BICIdentifier
1.10	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime

Item Details

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
2.1	Original Payment Information and Cancellation	<OrgnlPmtInfAndCxl>	[1..1]	
2.2	Payment Cancellation Identification	<PmtCxlId>	[1..1]	Max35Text
2.3	Original Payment Information Identification	<OrgnlPmtInfId>	[1..1]	Max35Text

2.4		Original Group Information	<OrgnlGrpInf>	[0..1]	
2.5		Original Message Identification	<OrgnlMsgId>	[1..1]	Max35Text
2.6		Original Message Name Identification	<OrgnlMsgNmId>	[1..1]	Max35Text
2.7		Original Creation Date Time	<OrgnlCreDtTm>	[1..1]	ISODateTime
2.8		Transaction Information	<TxInf>	[1..1]	
2.9		Cancellation Identification	<CxlId>	[1..1]	Max35Text
2.10		Original Instruction Identification	<OrgnlInstrId>	[1..1]	Max35Text
2.11		Original End To End Identification	<OrgnlEndToEndId>	[1..1]	
2.12		Cancellation Reason Information	<CxlRsnInf>	[1..1]	
2.13		Originator	<Orgtr>		
2.14		Name	<Nm>	[0..1]	Max140Text
2.15		Identification	<Id>	[1..1]	
2.16		Organisation Identification	<OrgId>	[1..1]	
2.17		Any BIC	<AnyBIC>	[0..1]	AnyBICDec2014Identifier
2.18		Reason	<Rsn>	[1..1]	
2.19		Code	<Cd>	[1..1]	SEPA Code Restrictions
2.20		Additional Information	<AddtlInf>	[1..1]	Max105Text
2.21		Original Transaction Reference	<OrgnlTxRef>	[1..1]	
2.22		Amount	<Amt>	[1..1]	
2.23		Requested Execution Date	<ReqdExctnDt>	[1..1]	DateAndDateTime2Choice
2.24		Payment Type Information	<PmtTpInf>	[1..1]	

2.25					Service Level		<SvcLvl>	[0..1]	
2.26						Code	<Cd>	[0..1]	
2.27					Local Instrument		<LclInstrm>	[1..1]	
2.28						Code	<Cd>	[1..1]	
2.29					Category Purpose		<CtgyPurp>	[1..1]	
2.30						Code	<Cd>	[1..1]	
2.31				Remittance Information			<RmtInf>	[0..1]	
2.32				Debtor Agent			<DbtrAgt>	[1..1]	
2.33					Financial Institution Identification		<FinInstnId>	[1..1]	
2.34						BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.35						Name	<Nm>	[0..1]	Max140Text
2.36				Creditor Agent			<CdtrAgt>	[1..1]	
2.37					Financial Institution Identification		<FinInstnId>	[1..1]	
2.38						BICIdentifier	<BICFI>	[1..1]	BICIdentifier
2.39						Name	<Nm>	[0..1]	Max140Text
2.40				Creditor					
2.41					Party Identification		<Pty>	[0..1]	
2.42						Name	<Nm>	[1..1]	Max70Text
2.43						Postal Address	<PstlAdr>	[0..1]	
2.44						Id	<Id>	[0..1]	
2.45				Creditor Account			<CdtrAcct>	[1..1]	

2.46					Identification		<Id>	[1..1]	
2.47						IBAN	<IBAN>	[1..1]	

7.1.14. Reconciliation Message – camt.053.001.12

This message is sent after during the cut-off at midnight and at scheduled times throughout the day and covers the period between the last message and the current moment. IPS automatically sends the reconciliation messages to each Participant. This format uses the standard ISO schemas in the following structure.

INDEX		MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root		<BkToCstmrStmt>	[1..1]
2		Group Header	<GrpHdr>	[1..1]
3		Statement	<Stmt>	[1..1]

Group Header

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY	TYPE
1.0	Group Header	<Assgnmt>	[1..1]	
1.1	Message Identification	<MsgId>	[1..1]	Max35Text
1.2	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime
1.3	Message Recipient	<MsgRcpt>	[0..1]	
1.4	Identification	<Id>	[0..1]	
1.5	Organization Identification	<OrgId>	[1..1]	
1.6	BIC or BEI	<BICOrBEI>	[0..1]	AnyBICIdentifier

Item Details

INDEX	MESSAGE ITEM	XML TAG	MULTI.	TYPE
2.1	Statement	<Stmt>	[1..1]	
2.2	Identification	<CxlId>	[1..1]	Max35Text
2.3	Creation Date Time	<CreDtTm>	[1..1]	ISODateTime
2.4	Date Time Period	<FrToDt>	[1..1]	
2.5	From Date Time	<FrDtTm>	[1..1]	ISODateTime
2.6	To Date Time	<ToDtTm>	[1..1]	ISODateTime
2.7	Account	<Acct>	[1..1]	

2.8			Identification			<Id>	[1..1]	
2.9				Other		<Othr>	[1..1]	
2.10					Id	<Id>	[1..1]	Max34Text
2.11		Balance				<Bal>	[1..n]	
2.12			Type			<Tp>		
2.13				Code or Properitary		<CdOrPrtry	[1..1]	
2.14					Proprietary	<Prtry>	[0..1]	Max35Text
2.15			Amount			<Amt>	[1..1]	ActiveOrHistoricCurrencyAndAmount
2.16			Credit Debit Code			<CdtDbtInd>	[1..1]	Fixed text “CRDT” or “DBIT”
2.17			Date and DateTime Choice			<Dt>	[1..1]	
2.18				Date		<Dt>	[0..1]	ISODate
2.19				DateTime		<DtTm>	[0..1]	ISODateTime
2.20		Transactions Summary				<TxsSummry>	[0..1]	
2.21			Total Entries			<TtlNtries>	[0..1]	
2.22				Number of Entries		<NbOfNtries>	[0..1]	Max15NumericText
2.23				Sum		<Sum>	[0..1]	DecimalNumber
2.24				Total Net Entry Amount		<TtlNetNtryAmt>	[0..1]	DecimalNumber
2.25				Credit Debit Indicator		<CdtDbtInd>	[0..1]	Fixed text “CRDT” or “DBIT”
2.26			Total Credit Entries			<TtlCdtNtries>	[0..1]	
2.27				Number of Entries		<NbOfNtries>	[0..1]	Max15NumericText
2.28				Sum		<Sum>	[0..1]	DecimalNumber

2.29			Total Debit Entries							<TtlDbtNtries>	[0..1]	
2.30				Number of Entries						<NbOfNtries	[0..1]	Max15NumericText
2.31				Sum						<Sum>	[0..1]	DecimalNumber
2.32			Total Entries Per Bank Transaction Code							<TtlNtriesPerBkTxCd	[0..n]	
2.33				Number of Entries						<NbOfNtries>	[0..1]	Max15NumericText
2.34				Sum						<Sum>	[0..1]	DecimalNumber
2.35				Total Net Entry Amount						<TtlNetNtryAmt>	[0..1]	DecimalNumber
2.36				Credit Debit Indicator						<CdtDbtInd>	[0..1]	Fixed text “CRDT” or “DBIT”
2.37				Bank Transaction Code						<BkTxCd>	[1..1]	
2.38					Proprietary					<Prtry>	[0..1]	
2.39						Code				<Cd>	[1..1]	Fixed text: pacs.008, pacs.004, pacs.008fee or pacs.004fee
2.40		Transaction detail								<Ntry>	[0..n]	
2.41			Transaction reference							<NtryRef>	[1..1]	The unique reference of the tran
2.42			Transaction amount							<Amt>	[1..1]	ActiveOrHistoricCurrencyAndAmount
2.43			Credit Debit Indicator							<CdtDbtInd>	[1..1]	Fixed text “CRDT” or “DBIT”
2.44			Status							<Sts>	[1..1]	Fixed text “BOOK”
2.45			Transaction type							<BkTxCd>	[1..1]	
2.46				Proprietary						<Prtry>	[1..1]	pacs.008 or pacs.004
2.47			Charges							<Chrgs>	[0..1]	
2.48				Charge Amount						<Amt>	[1..1]	

2.49				Credit Debit Indicator	<CdtDbtInd>	[0..1]	Fixed text “CRDT” or “DBIT”

Gross totals of the value transactions are included in **TtlNtries** (completed pacs.008 and pacs.004). Breakdown in terms of credits (**TtlCdtNtries**) and debits (**TtlDbtNtries**) to the participant, accompanied by a further by type section (**TtlNtriesPerBkTxCd**) are also present to assist the reconciliation process.

7.1.15. Net Position Information Message – positions.001.xsd

The message that contains information about a Participant's positions has the following schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Montran Corporation 2017 - RP -->
<xs:schema xmlns="urn:montran:positions.001"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
	targetNamespace="urn:montran:positions.001">
	<xs:element name="positions">
		<xs:complexType>
			<xs:sequence>
				<xs:element name="snapshot" type="SnapshotInfo" />
			</xs:sequence>
		</xs:complexType>
	</xs:element>

	<xs:complexType name="SnapshotInfo">
		<xs:sequence>
			<xs:element name="conditions" type="ConditionsList"
maxOccurs="unbounded"/>
		</xs:sequence>
		<xs:attribute name="instgAgtBIC" type="BICIdentifier"
use="required"/>
		<xs:attribute name="lastTranSeq" type="xs:long"
use="required"/>
		<xs:attribute name="timestamp" type="xs:dateTime"
use="required"/>
	</xs:complexType>

	<xs:complexType name="ConditionsList">
		<xs:sequence>
			<xs:element name="condition" type="ConditionInfo"
maxOccurs="unbounded"/>
		</xs:sequence>
		<xs:attribute name="agtBIC" type="BICIdentifier" use="required"
/>
	</xs:complexType>

	<xs:complexType name="ConditionInfo">
		<xs:attribute name="accountCode" type="Max15Text"
use="required"/>
		<xs:attribute name="ccy" type="ActiveCurrencyCode"
use="required"/>
		<xs:attribute name="condType" type="ConditionType" />
		<xs:attribute name="balance" type="BalanceAmount_SimpleType" />
		<xs:attribute name="overdraft" type="Amount_SimpleType" />
		<xs:attribute name="debitAmount" type="Amount_SimpleType" />
		<xs:attribute name="debitCount" type="xs:integer" />
		<xs:attribute name="creditAmount" type="Amount_SimpleType" />
		<xs:attribute name="creditCount" type="xs:integer" />
	</xs:complexType>
```

```
	<!-- Supporting simple Types -->
	<xs:simpleType name="Amount_SimpleType">
		<xs:restriction base="xs:decimal">
			<xs:minInclusive value="0.00" />
			<xs:fractionDigits value="2" />
			<xs:totalDigits value="17" />
			<xs:maxInclusive value="999999999999999.99" />
			<xs:pattern value="[0-9]{0,15}([\.]([0-9]{0,2})){0,1}" />
		</xs:restriction>
	</xs:simpleType>

	<xs:simpleType name="BalanceAmount_SimpleType">
		<xs:restriction base="xs:decimal">
			<xs:minInclusive value="-999999999999999.99" />
			<xs:fractionDigits value="2" />
			<xs:totalDigits value="17" />
			<xs:maxInclusive value="999999999999999.99" />
			<xs:pattern value="[\-]{0,1}[0-9]{0,15}([\.]([0-
9]{0,2})){0,1}" />
		</xs:restriction>
	</xs:simpleType>

	<xs:simpleType name="ActiveCurrencyCode">
		<xs:restriction base="xs:string">
			<xs:pattern value="[A-Z]{3,3}" />
		</xs:restriction>
	</xs:simpleType>

	<xs:simpleType name="BICIdentifier">
		<xs:restriction base="xs:string">
			<xs:pattern value="[A-Z]{6,6}[A-Z2-9][A-NP-Z0-9]([A-Z0-
9]{3,3}){0,1}" />
		</xs:restriction>
	</xs:simpleType>

	<xs:simpleType name="ConditionType">
		<xs:restriction base="xs:string">
			<xs:enumeration value="COMPLETE" />
			<xs:enumeration value="HOLD" />
		</xs:restriction>
	</xs:simpleType>

	<xs:simpleType name="Max15Text">
		<xs:restriction base="xs:string">
			<xs:minLength value="1" />
			<xs:maxLength value="15" />
		</xs:restriction>
	</xs:simpleType>
</xs:schema>
```

Example of own net positions message:

```
<?xml version="1.0" encoding="UTF-8"?>
<positions xmlns="urn:montran:positions.001">
	<snapshot instgAgtBIC="TESABGSF" lastTranSeq="10104" timestamp="2020-06-
06T19:22:38+03:00" >
```

```
            <conditions conditions agtBIC="TESABGSF">
                  <condition accountCode='TESABGSF-EUR' ccy='EUR'
condType='COMPLETE' balance='-318.89' debitAmount='11025.20'
debitCount='1997' creditAmount='10706.31' creditCount='1972'/>
                  <condition accountCode='TESABGSF-EUR' ccy='EUR'
condType='HOLD' balance='0' debitAmount='0' debitCount='0' creditAmount='0'
creditCount='0'/>
            </conditions>
      </snapshot>
</positions>
```

The information reported in this message is divided into two conditions: COMPLETE and HOLD. The positions in the COMPLETE condition are information related to the transactions completed by the system, while the values from the HOLD condition are information related to transactions that are still being processed by the system.

The balance attribute is the net position of completed transactions (COMPLETE status) and is the arithmetic amount of the attributes: debitAmount and creditAmount.

DebitAmount and Creditamount are the total amounts of initial transactions received by the Participant that requested the information.

DebitCount and CreditCount is the number of initial transactions received by the Participant that requested the information.

The available balance for the initiation of a payment by a Participant does not have a specific field in the message, but it can be calculated with the following formula:

available credit limit = balance (COMPLETE) – DebitAmount (HOLD)

In other words, the available clearing limit is equal to the net amount of completed transactions, and from this amount the amount of initiated transactions still being processed is decreased.

7.1.16. Participant List Table – participants.001.xsd

The participant list will be delivered by the system when requested, on a schedule or when changes happen.

The participants will be able to use an API request to retrieve the information at any time.

At cutoff time, typically midnight, a file will be sent to all participants.

The Montran built-in format for the participant list message is shown below. Due to the more concise nature, it can be delivered as the full listing at all times. On top of the registration status, the online status is also captured.

INDEX	MESSAGE ITEM	XML TAG	MULTIPLICITY
1	Message Root	<participants>	[1..1]
1.1	Time attribute	timestamp	[1..1]
2	Participant node	<participant>	[1..n]
2.1	BIC attribute	bic	[1..1]
2.2	Type attribute	type	[1..1]
2.3	Valid from	validFrom	[0..1]
2.4	Valid to	validTo	[0..1]
3	Status	<status>	[1..1]
4	Dynamic status	<online>	[1..1]
5	Connection agent	<directAgent>	[0..1]

The type attribute reflects the participant mode:

- INST – Inst mode

The Connection agent is used for indirect clearing participants to link to its direct clearing participant:

```
<?xml version="1.0" encoding="UTF-8"?>
<participants timestamp=”2017-04-05T10:00:40”>
 <participant bic="CCPBIC33" type=”INST”>
       <status>ACTIVE</status>
       <online>false</online>
 </participant>
 <participant bic="STSABGSF" type=”INST”>
       <status>ACTIVE</status>
       <online>true</online>
 </participant>
 <participant bic="TCZBBGSF" type=”INST” validFrom=”2020-04-05”>
       <status>ACTIVE</status>
       <online>true</online>
 </participant>
 <participant bic="UBBSBGSF" type=”INST”>
```

```
            <status>ACTIVE</status>
            <online>true</online>
      </participant>
      <participant bic="INDIBGSF" type=”INST”>
            <status>ACTIVE</status>
            <online>true</online>
            <directAgent>UBBSBGSF</directAgent>
      </participant>
      <participant bic="FINVBGSF" type=”INST” validTo=”2021-09-01”>
            <status>ACTIVE</status>
            <online>true</online>
      </participant>
</participants>
```

7.2. Annex 2 – Error Codes

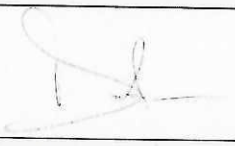
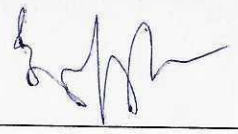
After processing the messages and transactions, the IPS system assigns to each message an internal error code, described in the table below. These codes are displayed in the graphical user interface (MMC) for user investigations.

When pacs.002 reply messages are generated, the error code generated by the IPS system is mapped to an error code according to the ISO20022 schema.

Internal Code	pacs.002 mapping	Description
000		No error.
100	MS03	Internal processing error.
101		Message Identification.
500	AB05	Timeout error.
501	MS02	Payment declined by the beneficiary Participant.
502	AB08	The recipient Participant is disconnected.
1000	MS03	Generic error.
1001	MS03	Generic validation error.
1002	FF01	The currency is invalid.
1003	FF01	Amount is invalid (less than or equal to zero).
1004	DNOR	The value in the DbtrAgt field is invalid: - No ACTIVE Participant with this BIC found. - The value is different from InstgAgt. - The value is different from the ordering detected Participant at channel transmission level.
1005	CNOR	The value in the CdtrAgt field is invalid: - No ACTIVE Participant with this BIC found.
1006	RC01	The value in the InstgAgt field is invalid: - No ACTIVE Participant with this BIC found. - The value is different from the ordering detected Participant at channel transmission level.
1007	RC01	Unused.
1008	AC01	The IBAN code of the debtor is invalid.
1009	AC01	The creditor IBAN code is invalid.
1010	AM05	A payment with the same reference is currently processed.
1011	AM05	A payment with the same reference was already processed.

INTERNAL CODE	PACS.002 MAPPING	DESCRIPTION
1012	FF01	The settlement date is invalid (IntrBkSttlmDt).
1013	FF01	Invalid XML format.
1014		Unused.
1015	TM01	Invalid Time – Value in the Acceptance `DataTime` field is older than the current time with the value of the timeout parameter configured in the payment schema.
1016	AG09	Invalid original reference – No transaction with the original reference was found when processing a pacs.002 message.
1017	AG09	Invalid status of the original transaction – When processing a pacs.002 message, the referenced transaction is not in the proper status (message: WAIT_RECEIVER, transaction: HOLD).
1018	RC01	Invalid sender – Sender Participant is not ACTIVE.
1019	RR04	The payment schema is not defined for the currency specified by the message.
1020	AM02	The amount is too high compared to the parameter defined in the payment schema.
1021	AG10	Sender is blocked (temporarily disabled).
1022	RR04	Payment schema not mapped (either for debtor or creditor)
1026	FF01	Invalid XML field (groups various XML validations not part of default xsd, i.e. specific codes like SvcLvl, CtgyPurp)
1027	RC01	Invalid receiver (receiver is not the system BIC for messages sent by participants)
1028	FF01	Invalid original settlement date (recalls that point to an original date from the future)
1029	RC01	Invalid on us (intra-bank payments sent to IPS)
1030	RC01	Invalid originator (originator BIC missing or invalid)
1033	AB05	Past requested execution day (for RTP flow)
1040	AB05	Missing requested execution day (from RTP message)
1041	MS03	RTP flow is not enabled in payment schema
1042	AB05	Requested execution date is after the max allowed in payment schema
1043	MS03	PmtInfId from RTP is invalid

Internal Code	pacs.002 mapping	Description
1044	MS03	Invalid date in PmtInfId from RTP (the id must start with the current date)
1045	MS03	PmtTpInf field present in both group and item description
2000	AM23	Insufficient funds to clear the transaction.
3000	FF01	The Participant does not have any active certificate of DS type for validating messages.
3001	FF01	The XML message does not contain the digital signature in the specified format.
3002	FF01	Digital signature does not protect the entire XML message.
3003	FF01	Digital signature is invalid.
3004	FF01	The certificate used for signing has expired or has been revoked.

PROJECT: *GE_IPS_DELIVERY_PROJECT*			
Date	2025-06-13	Deliverable Management Module	
Deliverable ID	01		
Deliverable Name	Annex D – IPS-Participant Interface		
Deliverable Code	GE_IPS_Inception_Report_Annex_D_IPS-Participant_Interface_v.1.00		
Deliverable Type	DOCUMENT		
Version	1.00		
Description	IPS-Participant Interface		
Montran QA	QA Team		
Deliverable Review and Approval			
Delivered by:	Nucu Dumitrascu Project Manager Montran	**Signature:**	
Approved by:	Beka Dotchviri Executive Director National Bank of Georgia	**Signature:**	
Expected review date:	2025-06-13	**Actual review date:**	2025-06-23