Central liquidity management

User detailed functional specifications

Author	4CB
Version	0.2
Date	06 June 2018

Table of contents

List of figures

List of tables

1 Overview CLM service

2 Parties, accounts and currencies

2.1 General information on reference data

2.1.1 Concept of parties and participants

2.1.2 Hierarchical party/participant model

2.1.3 Configuration of parties/participants

2.1.4 Party/participant identification

2.1.5 Reference data for parties/participants

2.2 CLM related reference data

2.2.1 Participation types

2.2.1.1 Direct participation in CLM

2.2.1.2 Multi-addressee access

2.2.1.3 Access as correspondent BIC ("addressable BIC")

2.2.2 Accounts structure and organization

2.2.2.1 Categories of accounts

2.2.2.2 Main cash accounts

3 Access to CLM

3.1 Connectivity (A2A/U2A)

3.2 Authentication and authorisation

3.2.1 Authentication and authorisation concepts

3.2.2 Instructing scenarios

3.3 User roles and access rights

3.4 Message subscription

3.5 Graphical user interface

3.6 Security

4 Business day

5 Operations and support

5.1 Business application configuration

5.2 Calendar management

5.3 Business day management

5.4 Business and operations monitoring

5.5 Archiving management

5.6 Trouble management

6 Application processes description

6.1 Settlement of payments linked to central bank operations

6.1.1 Overview

A central bank system can send a payment order (pacs.009) or a direct debit (pacs.010) linked to a central bank operation or cash withdrawal to a CLM participant that holds a MCA in CLM. In Case this can also be a connected payment, ie payments, that trigger a change in the credit line of the CLM participant and an immediate debit/credit of its account to compensate the change in this credit line. Payment orders and direct debits can be sent throughout the whole business day with the exception of the end of day processing (with the exception of the marginal lending facility) and the maintenance window. The processing of connected payments shall not be possible between the CB general cut-off for the use of standing facilities (ie 18:40) and the start of the provisioning of liquidity for the new business day (ie 19:00), as well as during the maintenance window. Central banks have the possibility to send payments with an “earliest debit time indicator” (FROM-Time) and with a “latest debit time indicator” (TILL-Time). Furthermore it is possible, to submit payments up to 10 calendar days in advance. In this case, the payment message is warehoused until CLM opens for that date. All Payments have the same priority. There is no need to distinguish between urgent and normal payments. At the settlement date, the warehoused payment undergoes the business validation checks for a second time.

The initiation can be carried out A2A by the central bank system or U2A by the CB operator. There can be submitted the following payment types:

- credit transfers or
- direct debits used for the settlement of cash withdrawals, repayment of monetary policy operations and collections of fees

6.1.2 Definition of execution time

CLM participants have also the possibility to determine the settlement time of their transactions. The following options are available:

- transactions with an “earliest debit time indicator”
- transactions with a “latest debit time indicator”

The following table describes payments with a set execution time.

	Earliest debit time indicator	Latest debit time indicator
Features	Transactions to be executed from a certain time (codeword: FROTIME)	▪ Transactions which should be executed up to certain time (only warning indicator) (codeword: /TILTIME/)
Effect	▪ Transaction is stored until the indicated time. ▪ At the earliest debit time, the transaction runs through the entry disposition.	▪ Setting the execution time only means a special identification via the U2A or A2A query. ▪ The transaction is treated like any other payment of this type.
Management	If the transaction cannot be settled at the earliest debit time, it will be queued till cut-off time for payment type is reached (or revoked).	If the transaction cannot be settled until the indicated debit time, the payment will remain in the queue.

In case a payment with a “latest debit time indicator” is not executed 15 minutes prior to the defined time, an automatic notification in the GUI will be triggered. The notification will be directly displayed on top of all screens of the participant whose account will be debited.

Note: In case the codeword /CLSTIME/ is used, the payment will be treated in the same way as a payment with a “latest debit time indicator”.

It is possible to combine the “earliest debit time indicator” with the “latest debit time indicator”. The transaction is meant to be executed during the indicated period.

The defined execution time of a payment can be changed if the payment is not executed yet. Effect of changing settlement time see chapter Amendment of payments [▸ 28].

Note: It is no longer possible to change the “earliest debit time indicator” of a payment which is queued due to the fact that the original “earliest debit time indicator” has been reached and it was already tried to settle this payment.

6.1.3 Warehouse functionality

Basics

It is possible to submit payments up to 10 calendar days in advance. In this case, the payment message is warehoused until RTGS service opens for that business date.

Note: In case a change in SWIFT standards or formats is performed warehoused payments with an execution time beyond this point in time cannot be stored in the RTGS service. This will be technically ensured by the RTGS service.

Rules

The validation of warehoused payments is a three layer approach:

- SWIFT format checks on the day of submission
- format checks by CLM service already on the day of submission
- content check (eg valid BICs) on the value day

No checks are made by SSP in the time between.

Processing on value day

On the value date with the start of the day trade phase (7.00) the warehoused payments are processed by CLM service (with entry timestamp 7.00) on top of the queue of incoming payments which have the same priority. They will be immediately settled if enough liquidity is available (normal processing of payments in the entry disposition, see chapter Entry disposition [▸ 32]. Otherwise they are queued until the settlement attempt is successful (see chapter Dissolution of the payment queue [▸ 32]).

Exception: Warehoused payments with an earliest debit time indicator are queued until the set execution time is reached.

Information and control functions

Warehoused payments benefit from the same functionality via U2A or A2A as queued payments:

- transparency about the status and other detailed information about the payment
- cancellation
- change of priority
- change of execution time (earliest and latest debit time indicator) if set in the warehoused payment

6.1.4 Flow of payments

6.1.4.1 Payments initiated by central bank

6.1.4.1.1 Credit transfer

Positive case

A central bank system can send a payment order linked to a central bank operation or cash withdrawal to a CLM participant that holds a MCA in CLM. Such a payment can be sent throughout the whole business day with the exception of the end of day processing (with the exception of the marginal lending facility) and the maintenance window. Central banks have the possibility to send payments with an “earliest debit time indicator” (FROM-Time) and with a “latest debit time indicator” (TILL-Time). Furthermore it is possible to submit payments up to 10 calendar days in advance (warehoused payments). In this case, the payment message is warehoused until CLM opens for that date. All payments have the same priority. There is no need to distinguish between urgent and normal payments.

Message flow

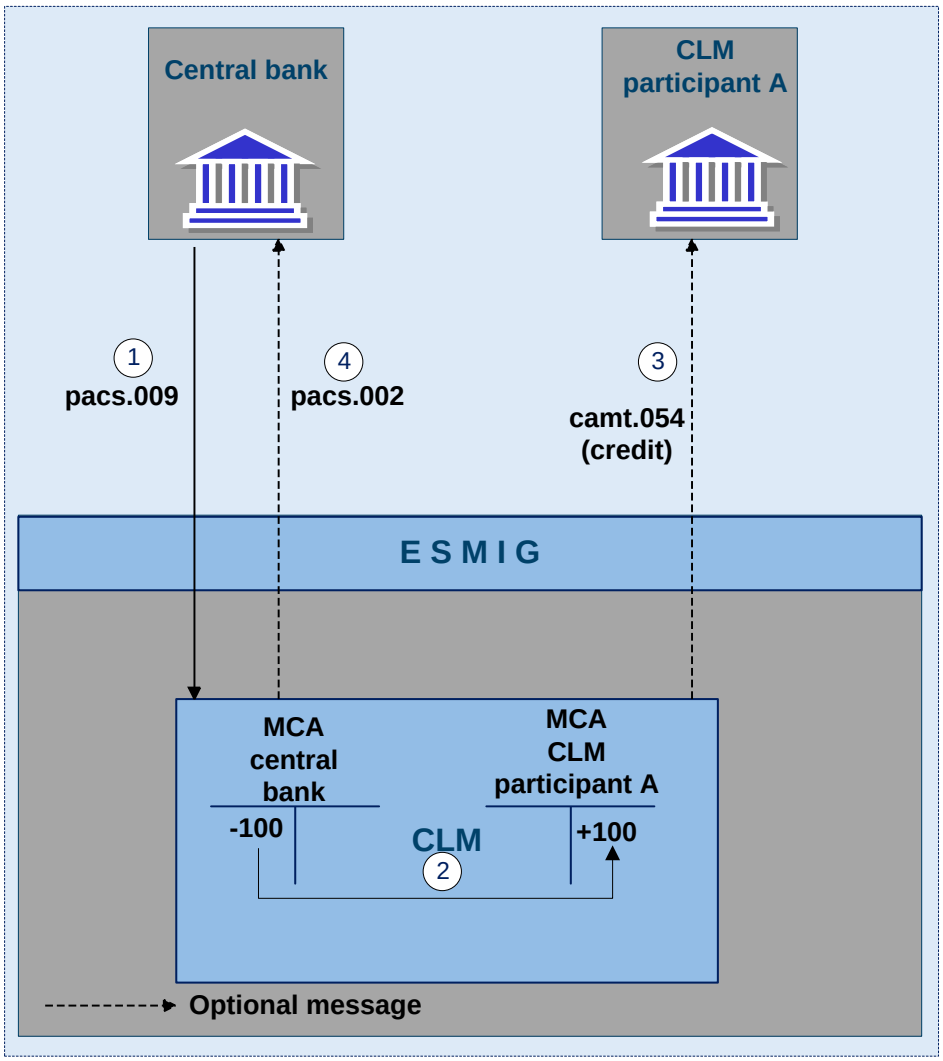


Figure 1 - pacs.009 CB operations

Process description

Step	Processing in/between	Description
1	Central bank via ESMIG to CLM	The central bank sends a pacs.009 via ESMIG to CLM
2	CLM	CLM message check and validation positive booking takes place in CLM
3	CLM via ESMIG to CLM participant	Creation and forwarding camt.054 (credit) (optional) by CLM via ESMIG to CLM participant A
4	CLM via ESMIG to central bank	Creation and forwarding of pacs.002 by CLM via ESMIG to central bank (optional)

Used messages

- pacs.009
- camt.054
- pacs.002

Technical validation failure

The service interface performs the following technical validations:

- type (including version) of delivered message is supported
- schema validation - syntax, format and structure of the message are compliant (eg all mandatory fields in the message received are populated)

If the technical validation fails the service interface rejects the message.

Message flow

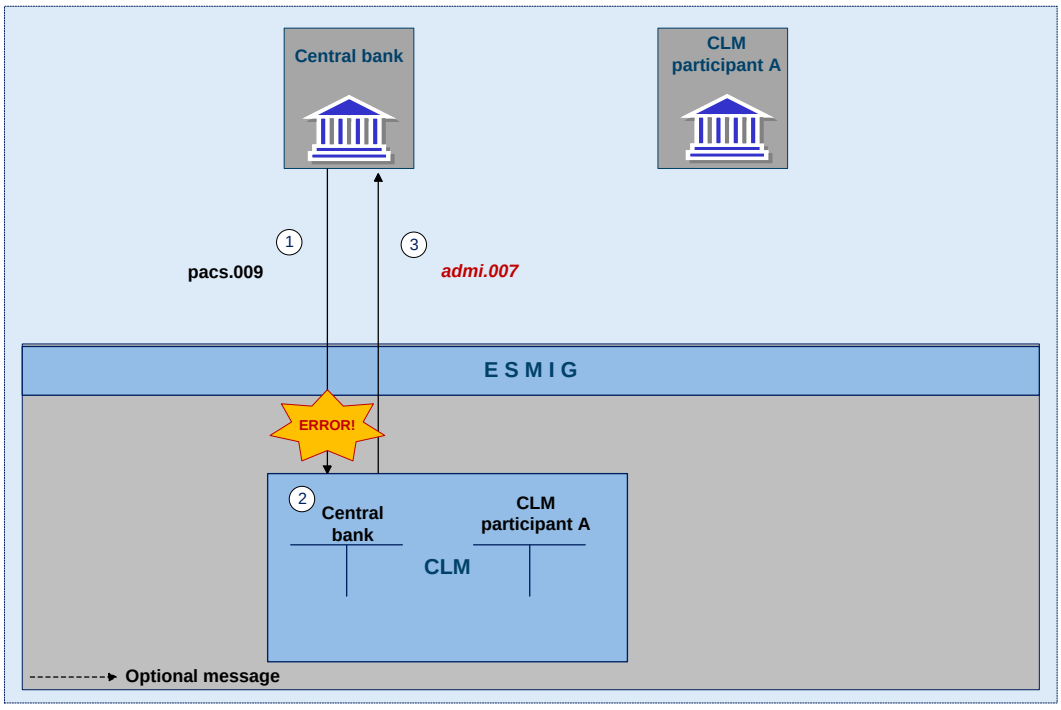


Figure 2 - pacs.009 CB operations technical validation failed

Process description

Step	Processing in/between	Description
1	Central bank via ESMIG to CLM	The central bank sends a pacs.009 via ESMIG to CLM
2	CLM	CLM technical validation failed
3	CLM via ESMIG to central bank	Creation and forwarding of admi.007 by CLM via ESMIG to central bank

Used messages

- pacs.009
- admi.007

Business failure

The service interface performs the following business validations:

- Duplicate submission control for incoming payments including the fields:
  - sender of the message
  - message Type
  - receiver
  - transaction Reference Number
  - related Reference
  - value Date and
  - amount
- The sender of the message is authorised to send payments linked to central bank operations or cash withdrawals. If the sender of the message is not the owner of the MCA, CLM shall check that it is authorised to send a payment order on behalf of the account owner.
- All provided values are valid according to predefined values or cross-field validations.
- The MCA and the central bank account mentioned in the payment order exist and are active for settlement in the relevant currency.
- The MCA owner is not blocked at account or party level.

If the business validation fails the interface rejects the message.

Message flow

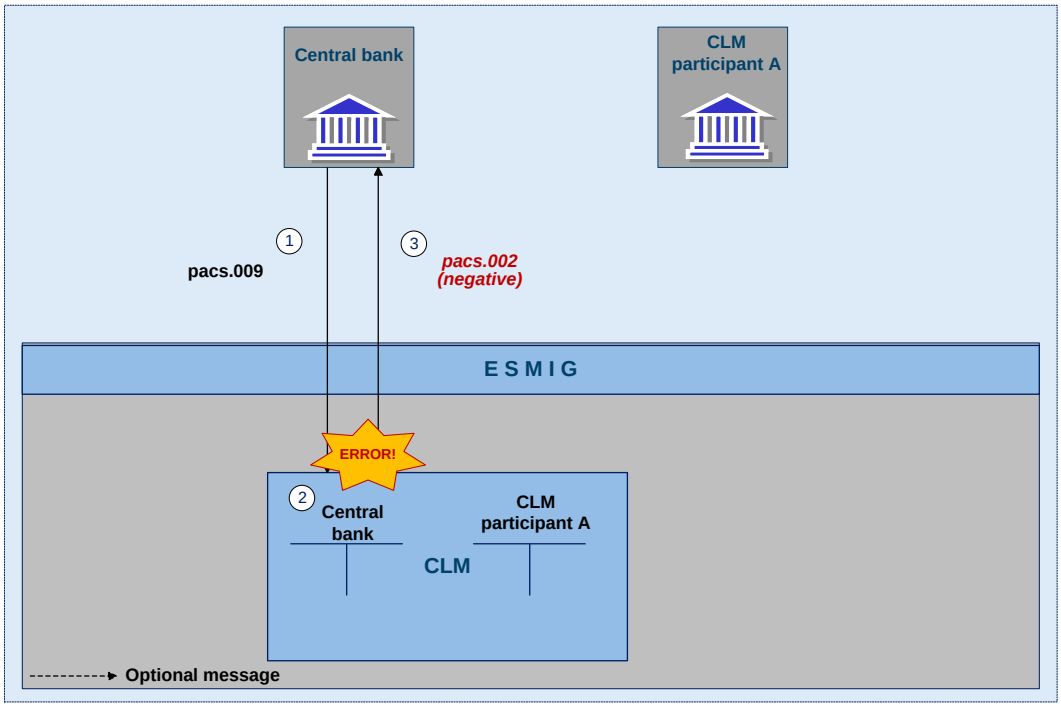


Figure 3 - pacs.009 CB operations business validation failed

Process description

Step	Processing in/between	Description
1	Central bank via ESMIG to CLM	The central bank sends a pacs.009 via ESMIG to CLM
2	CLM	CLM business validation failed
3	CLM via ESMIG to central bank	Creation and forwarding of a negative pacs.002 by CLM via ESMIG to central bank

Used messages

- pacs.009
- pacs.002

6.1.4.1.2 Direct debit

Positive case

A central bank system can send a direct debit linked to a central bank operation or cash withdrawal to a CLM participant that holds a MCA in CLM. Such a payment can be sent throughout the whole business day with the exception of the end of day processing (with the exception of the marginal lending facility) and the

maintenance window. Central banks have the possibility to send payments with an “earliest debit time indicator” (FROM-Time) and with a “latest debit time indicator” (TILL-Time). Furthermore it is possible to submit payments up to 10 calendar days in advance (warehoused payments). In this case, the payment message is warehoused until CLM opens for that date. All Payments have the same priority. There is no need to distinguish between urgent and normal payments.

Message flow

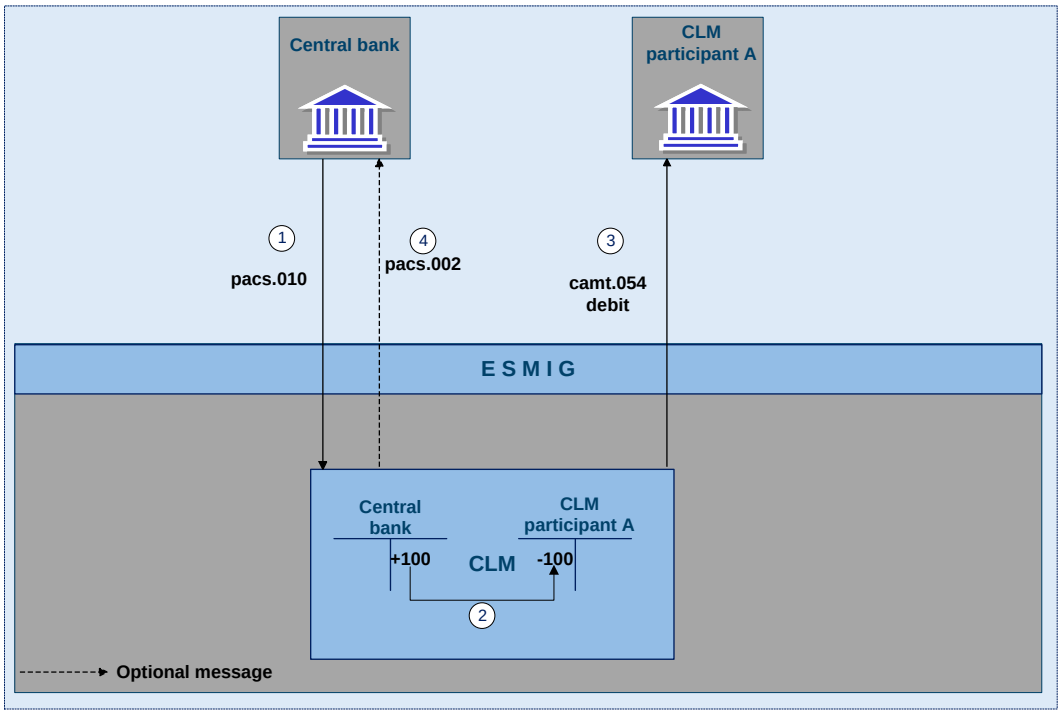


Figure 4 - pacs.010 CB operations

Process description

Step	Processing in/between	Description
1	Central bank via ESMIG to CLM	The central bank sends a pacs.010 via ESMIG to CLM
2	CLM	CLM message check and validation positive booking takes place in CLM
3	CLM via ESMIG to CLM participant	Creation and forwarding of camt.054 (debit) (optional)by CLM via ESMIG to CLM participant A
4	CLM via ESMIG to central bank	Creation and forwarding of pacs.002 by CLM via ESMIG to central bank(optional)

Used messages

- pacs.010

- camt.054
- pacs.002

Technical validation failure

The service interface performs the following technical validations:

- type (including version) of delivered message is supported
- schema validation - syntax, format and structure of the message are compliant (eg all mandatory fields in the message received are populated).

If the technical validation fails the service interface rejects the message.

Message flow

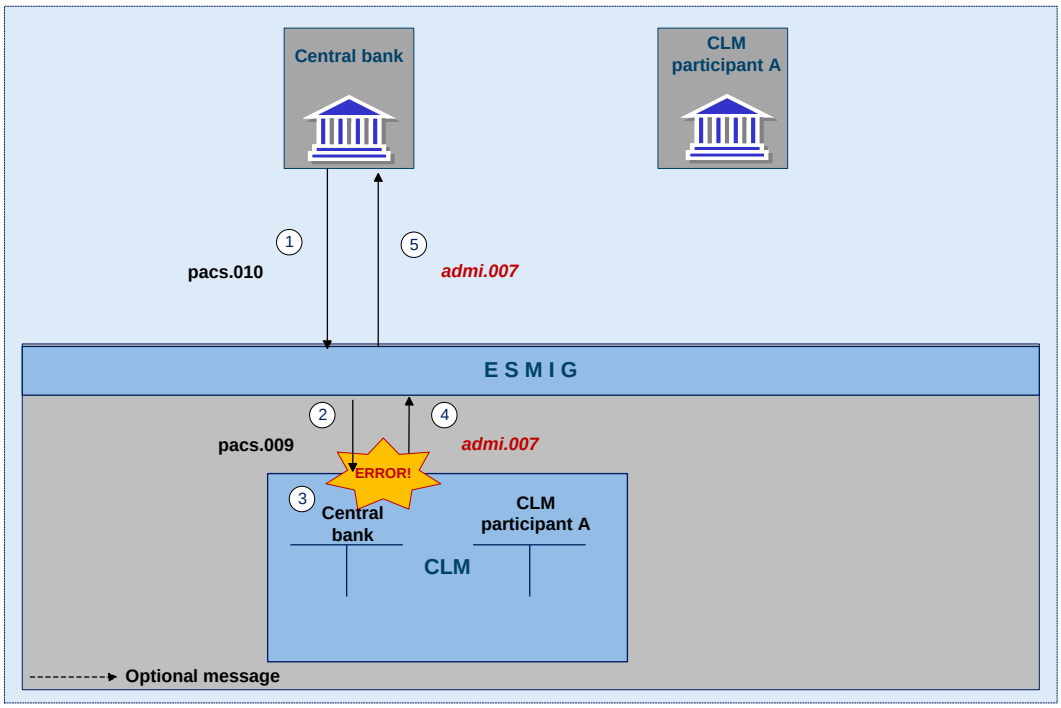


Figure 5 - pacs.010 CB operations technical validation failed

Process description

Step	Processing in/between	Description
1	Central bank via ESMIG to CLM	The central bank sends a pacs.010 via ESMIG to CLM
2	CLM	CLM technical validation failed
3	CLM via ESMIG to central bank	Creation and forwarding admi.007 by CLM via ESMIG to central bank

Used messages

- pacs.010
- admi.007

Business failure

The service interface performs the following business validations:

- Duplicate submission control for incoming payments including the fields
  - sender of the message
  - message Type
  - receiver
  - transaction reference number
  - related reference
  - value Date and
  - amount
- The sender of the message is authorised to send payments linked to central bank operations or cash withdrawals. If the sender of the message is not the owner of the MCA, CLM shall check that it is authorised to send a payment order on behalf of the account owner.
- All provided values are valid according to predefined values or cross-field validations
- The MCA and the central bank account mentioned in the payment order exist and are active for settlement in the relevant currency.
- The MCA owner is not blocked at account or party level.

If the business validation fails, the interface will reject the message.

Message flow

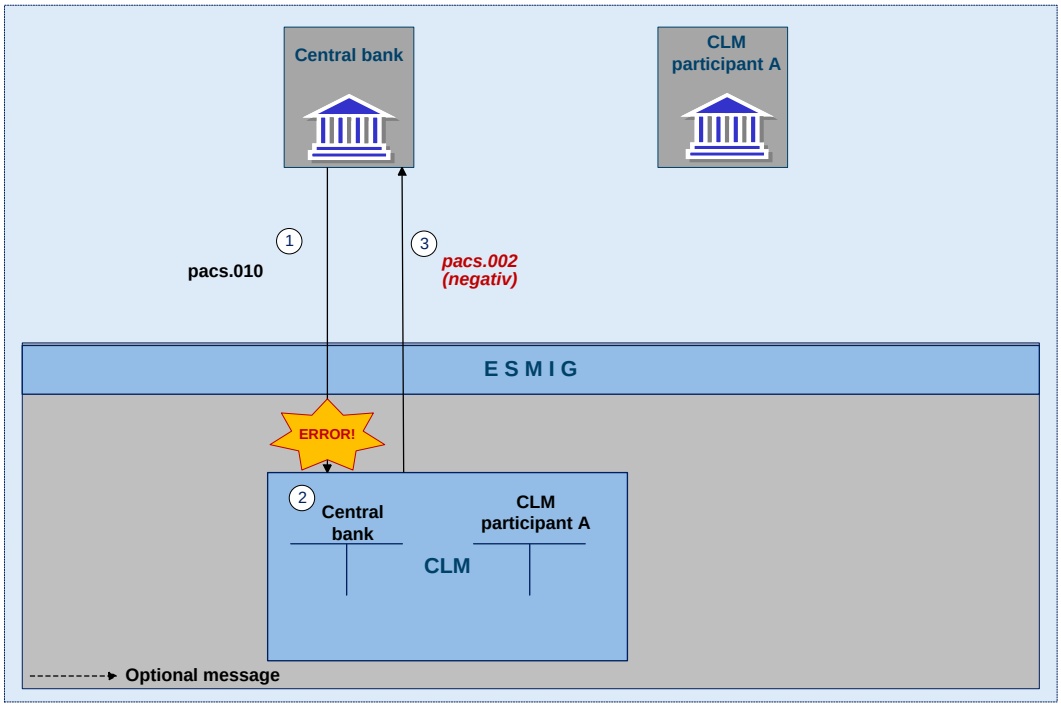


Figure 6 - pacs.010 CB operations business validation failed

Process description

Step	Processing in/between	Description
1	Central bank via ESMIG to CLM	The central bank sends a pacs.010 via ESMIG to CLM
2	CLM	CLM business validation failed
3	CLM via ESMIG to central bank	Creation and forwarding a negative pacs.002 by CLM via ESMIG to central bank

Used messages

- pacs.010
- pacs.002

6.1.5 Rejection of payments

For different reasons a payment can be rejected and returned to sender. If business validation in CLM interface fails the CLM service creates and forwards a pacs.002 (negative – payment status report) to the instructing party. This can be every CLM participant who initiates a payment. The pacs.002 refers to the origi-

nal instruction by means of references and a set of elements from the original instruction. Negative pacs.002 message is mandatory.

The following business validations are performed in CLM interface:

- check for duplicate payment order
- process specific authorisation checks:
  - Is the sender of the payment order the owner of the account to be debited?
  - In case of direct debit: is the sender of the payment order the owner of the account to be credited?
  - In case of mandated payments: is the sender of the payment order the neither the debtor nor the creditor and are there contractual agreements between the parties?
  - In case a central bank acts on behalf of a credit institution: does the credit institution belong to the acting central bank?
- check on value date for non-warehouse payments
- payment type specific checks
- field and reference data checks:
  - field value validation - codes are valid, domain values are within allowed range
  - cross-field validation - eg currency of the accounts involved same as amount currency etc.
  - database checks - eg existence of parties and accounts
- direct debit check
- check of backup payments
- mandated payment check
- account checks
- Error codes for possible rejections are listed in chapter Index of business rules and error codes [▸ 88].

If technical validation fails the payment is returned by admi.007.

6.1.5.1 Technical validations

6.1.5.2 Business validations

6.1.6 Amendment of payments

As long as a payment is not settled (including warehoused payments), an authorised system user has the ability to change the relevant parameters of this payment.

Three different control options are offered:

Action	Actor = authorised system user for the
Re-ordering (increase / decrease)	Debtor
Change of set execution time (if defined before sending to the RTGS service)	Business sender
Revocation (separate chapter Revocation of payments)	Business sender

Those features are necessary to enable CLM Actors to react on changed liquidity conditions during the day.

Note: Changing of priority is not possible as all payments have the same priority.

The following rules apply in principle:

- Interventions must be made via the business interface of the CLM service in U2A and A2A. A description of individual U2A processes can be found in the user handbook.
- Individual or several payment orders together can be modified at the same time.
- The business interface shows receipt and execution or non-execution of a modified order.

In case of intervention at transaction level, processes are started to resolve the queues.

Message flow

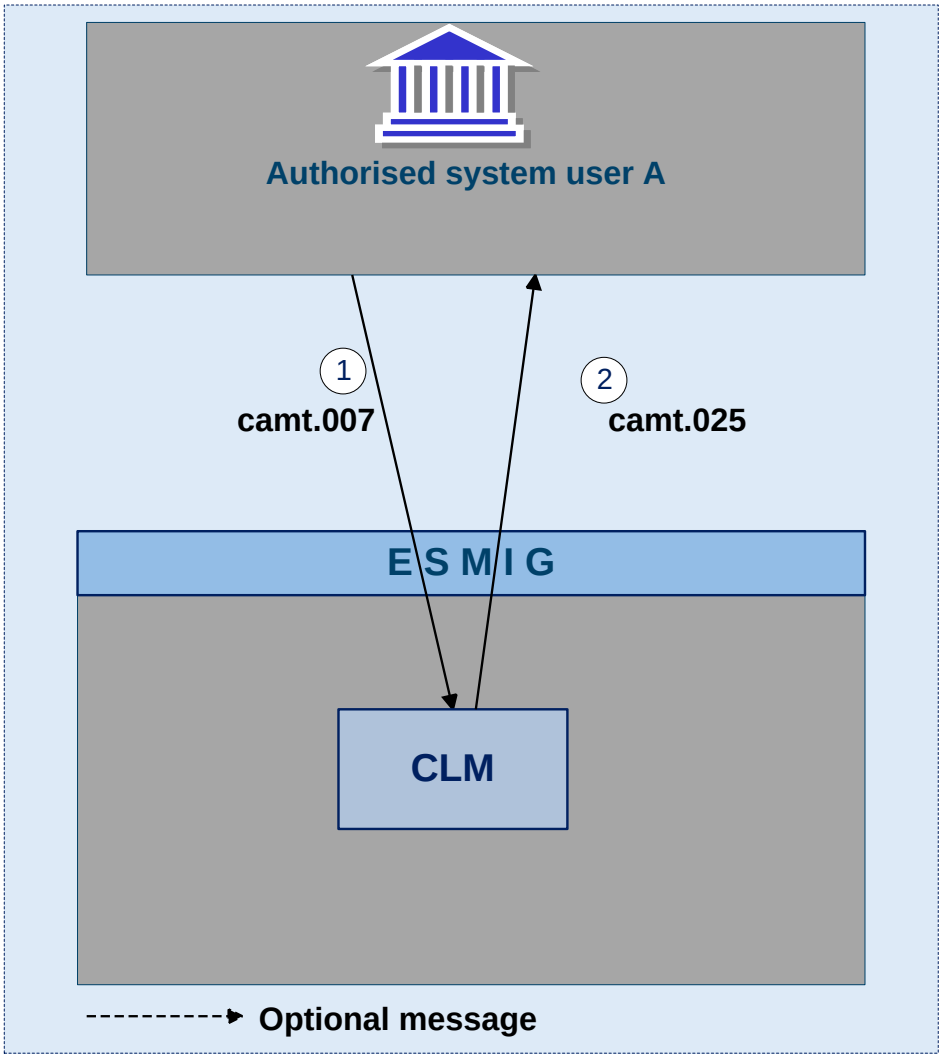


Figure 7 - camt.007

Process description

Step	Processing in/between	Description
1	Authorised system user via ESMIG to CLM	An authorised system user A sends a camt.007 via ESMIG to the CLM service
2	CLM	CLM message check and validation with positive or negative result
3	CLM via ESMIG to the authorised system user	Mandatory feedback to the authorised system user via camt.025

Used messages

- camt.007

- camt.025

Case re-ordering the queued transactions

A system user authorised can change the queue position for an individual or for a sequence of payments. The selected payment or sequence of payments can be placed:

- to the top of the queued payments
- to the end of the queued payments

The re-ordering can be done at any time during the business day. The newly modified queue can be viewed through the Payment Queue query.

Case changing the execution time

Payments can include a time that indicates when they should be settled (transactions with an “earliest debit time indicator”).

Payments can include a time that indicates when they should have been settled (transactions with a “latest debit time indicator”).

The execution time (from/till) may be changed in the CLM business interface (advanced or postponed). The change has no impact on the payment processing, but on the queue management as the time indication only supports the CLM participant’s queue management. The changed execution time is part of the payment queue query result.

Changing the execution time has the following impact on the queue management:

Action	Effect
Deleting the execution time of an urgent transaction (“from“)	Immediate settlement attempt, if the payment reaches the top of the queued urgent payments
Deleting the execution time of a high transaction (“from“)	Immediate settlement attempt, if the payment reaches the top of the queued high payments and no urgent payments are queued
Deleting the execution time of a normal transaction	Including the payment in the next settlement process
Changing the execution time of a urgent, high or normal transaction	Including the payment from the new indicated time

The newly modified execution time can be viewed through the Payment queue query.

6.1.7 Revocation of payments

6.1.8 Processing of payments

6.1.8.1 Entry disposition

6.1.8.2 Comprehensive queue management

6.1.8.3 Dissolution of the payment queue

6.2 Liquidity management

6.2.1 Available liquidity

6.2.2 Liquidity transfer

6.2.2.1 Overview

The main cash account is the central source of liquidity for the different settlement services the CLM participant joined in. Therefore CLM has to ensure the efficient liquidity provision by liquidity transfers within CLM, to other services and between dedicated cash accounts of different services. Furthermore CLM optimises the efficient usage of liquidity for the different services and transfers liquidity between them.

Liquidity transfers are not classified as payments (i.e. pacs); they are cash management instructions using camt messages. The liquidity transfer order message (camt.050) is exchanged between users and the system in order to instruct the transfer of cash from one cash account to another cash account.

Liquidity can be transferred

- between different main cash accounts within the CLM (under certain preconditions)
- between the main cash accounts and the dedicated cash accounts of the different settlement services
- between dedicated cash accounts within the same settlement service (out of scope of this UDFS)
- between dedicated cash accounts of different settlement services (via CLM)

The following types of liquidity transfers exist:

- immediate liquidity transfer order

- event-based liquidity transfer order
- standing liquidity transfer order

In general liquidity transfers are never queued. They are either settled immediately or are rejected. Only under certain conditions automatically generated liquidity transfers can become pending, for instance in the following scenario: CLM main cash account has insufficient liquidity for a central bank operation AND there is not sufficient liquidity on the RTGS dedicated cash account for an automatically triggered liquidity transfer to the main cash account. Any incoming liquidity (up to the required amount) on the RTGS dedicated cash account will then be transferred stepwise to the main cash account until the pending transaction (i.e. the central bank transaction) is completely settled.

For the transfer of liquidity the following rules apply:

Within a service liquidity can be transferred between dedicated cash accounts/main cash accounts belonging to the same liquidity transfer group. Liquidity transfer groups are configured by the respective central bank. A whitelist provides additional control for cash accounts (dedicated cash account or main cash account) by restricting from or to which other cash accounts liquidity transfers are allowed. It is configured by the participants (separate for inbound and outbound) and its usage is optional. The whitelist may apply in addition to the features of the liquidity transfer group for liquidity transfers within a single service and for liquidity transfers across services.

The rules for liquidity transfer groups do not apply for central banks. The rules for the whitelist do not apply if any central bank account is involved or if the accounts involved belong to the same party.

6.2.2.2 Initiation of liquidity transfers

Liquidity transfers are initiated by either the CLM participant itself, by another actor on the participants behalf or by the central bank on the participants behalf via sending the respective liquidity transfer order to CLM.

A liquidity transfer (camt.050) can be submitted to the CLM by

- a participant in the CLM service
- another actor on the participants behalf
- central bank

A liquidity transfer can be initiated as

- immediate liquidity transfer order. The amount is transferred after initiation immediately.
- event-based liquidity transfer order. The amount is transferred once (non-recurring) at a predefined point in time or a predefined event. Events can be defined either by the CLM service or by the account holder. The point of time can be defined by the account holder.
- standing liquidity transfer orders. The amount is transferred regularly at a certain point in time or predefined event.

6.2.2.3 Liquidity transfer process

6.2.2.3.1 Liquidity transfer from CLM main cash account to settlement service

A CLM participant can transfer liquidity from his CLM main cash account to a dedicated cash account within a settlement service (T2S, RTGS or TIPS). The transfer is possible if

- the whitelist authorises the CLM participant to work with the dedicated cash account to be credited
- no whitelist is defined
- both accounts belong to the same party
- a central bank account is involved

Message flow

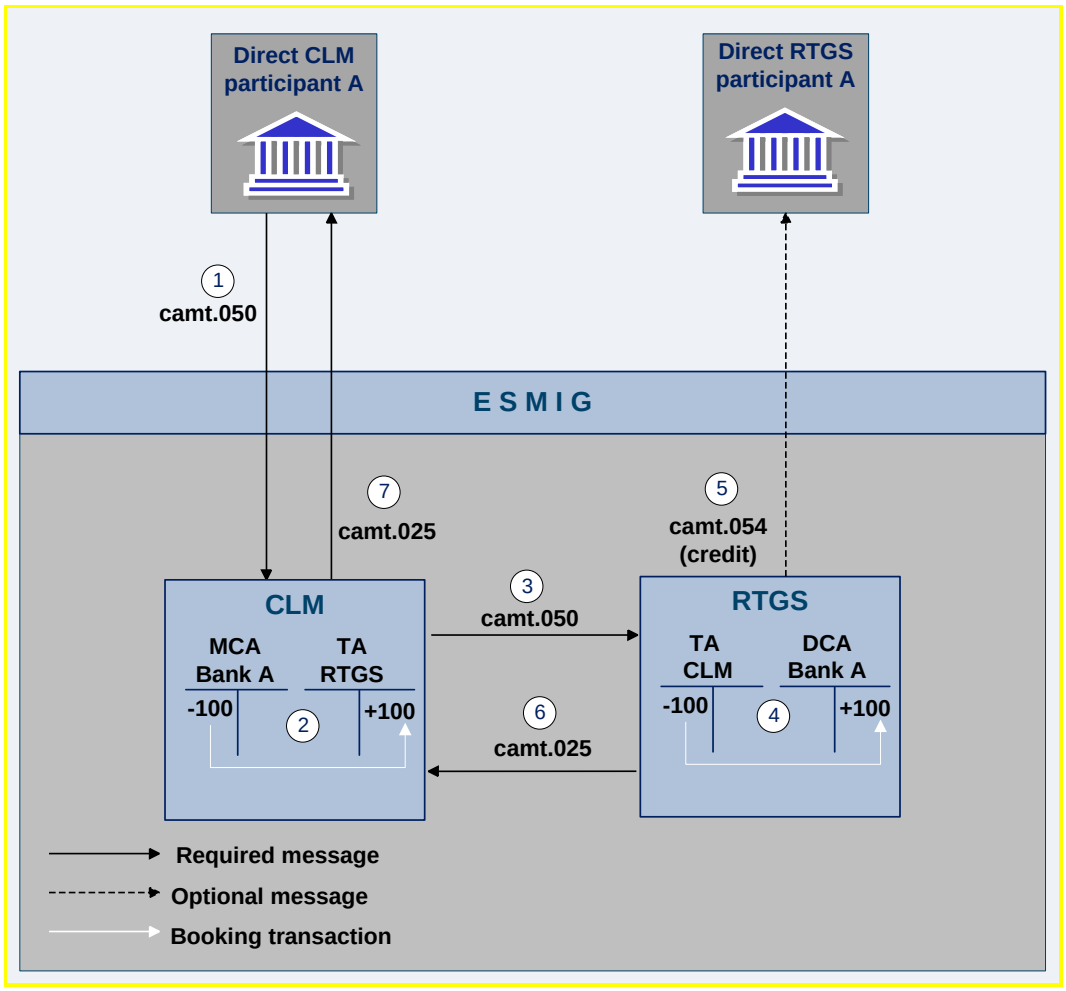


Figure 8 - camt.050 liquidity transfer from CLM main cash account to RTGS dedicated cash account

Process description

Step	Processing in/between	Description
1	CLM participant via ESMIG to CLM	A camt.050 is sent from a direct CLM participant to ESMIG.
2	CLM	Booking on CLM main cash accounts (main cash account -> technical account-RTGS)
3	CLM to RTGS	A camt.050 is forwarded to RTGS service.
4	RTGS	Booking on RTGS dedicated cash accounts (technical account-CLM -> dedicated cash account-RTGS)

Step	Processing in/between	Description
5	RTGS via ESMIG to direct RTGS participant	A camt.054 (credit) is sent by RTGS via ESMIG to the direct RTGS participant (optional).
6	RTGS to CLM	For full execution a camt.025 generated in RTGS will be sent to CLM service.
7	CLM via ESMIG to CLM participant	A camt.025 is sent by CLM via ESMIG to the CLM participant.

Table 1 - process description

Used messages

- camt.050
- camt.054
- camt.025

6.2.2.3.2 Liquidity transfer from settlement service to CLM main cash account

A settlement service participant can transfer liquidity from his dedicated cash account within a settlement service (T2S, RTGS or TIPS) to a CLM main cash account. The transfer is only possible if the whitelist authorises the RTGS participant to work with the main cash account to be credited (or no whitelist is defined).

Message flow

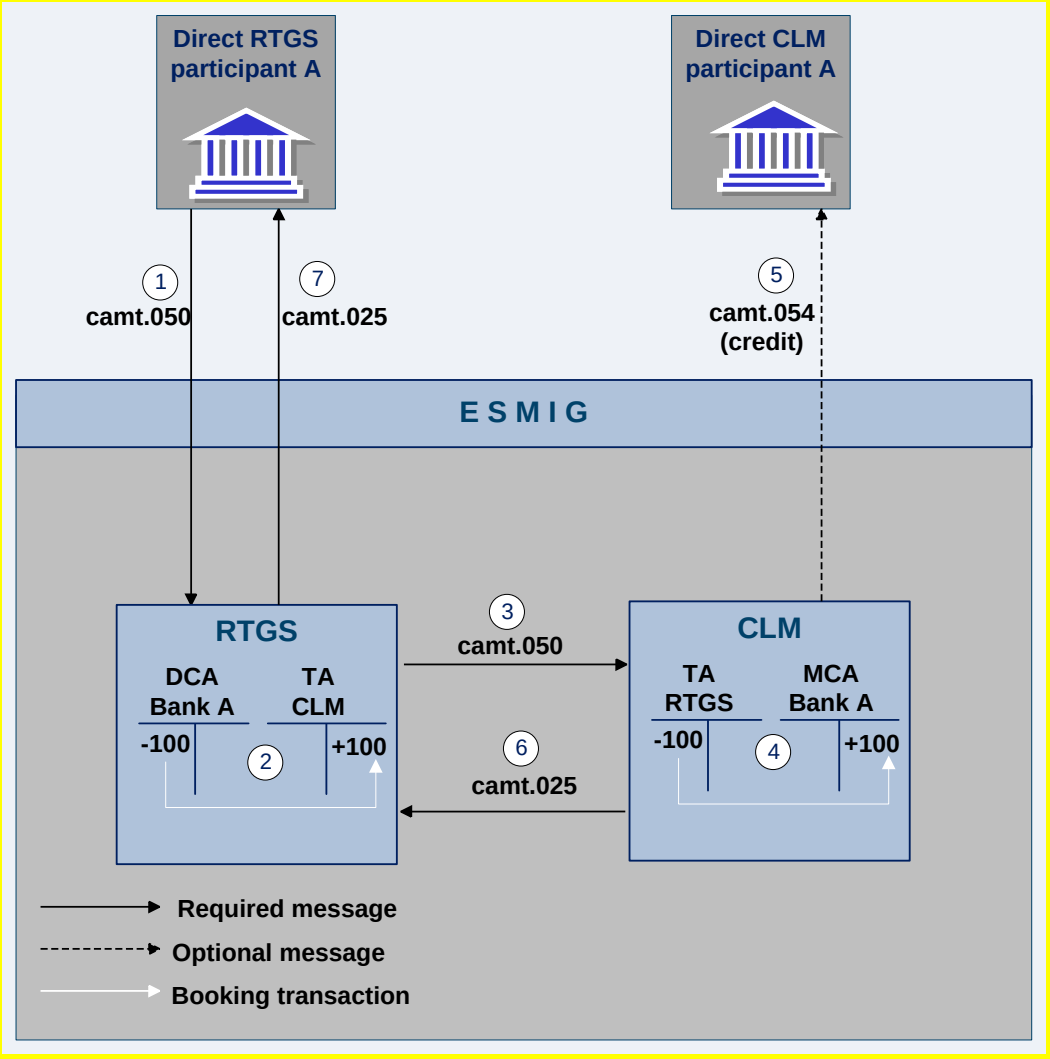


Figure 9 - camt.050 liquidity transfer from RTGS dedicated cash account to CLM main cash account

Process description

Step	Processing in/between	Description
1	RTGS participant via ESMIG to RTGS	A camt.050 is sent from a direct RTGS participant to ESMIG.
2	RTGS	Booking on RTGS dedicated cash accounts (RTGS dedicated cash account -> technical account-CLM)
3	RTGS to CLM	A camt.050 is forwarded to CLM service.
4	CLM	Booking on main cash account (technical account-RTGS -> main cash account)

Step	Processing in/between	Description
5	CLM via ESMIG to CLM participant	A camt.054 (credit) is sent by CLM via ESMIG to the CLM participant (optional).
6	CLM to RTGS	For full execution a camt.025 generated in CLM will be sent to RTGS service.
7	RTGS via ESMIG to direct RTGS participant	For full execution a camt.025 is sent by RTGS via ESMIG to the direct RTGS participant.

Table 2 - process description

Used messages

- camt.050
- camt.054
- camt.025

6.2.2.3.3 Liquidity transfer between two CLM main cash accounts

A CLM participant can transfer liquidity from one main cash account to another main cash account. The owner of the main cash accounts have to be in the same liquidity group and the whitelist authorises the CLM participant to work with the main cash account to be credited.

Message flow

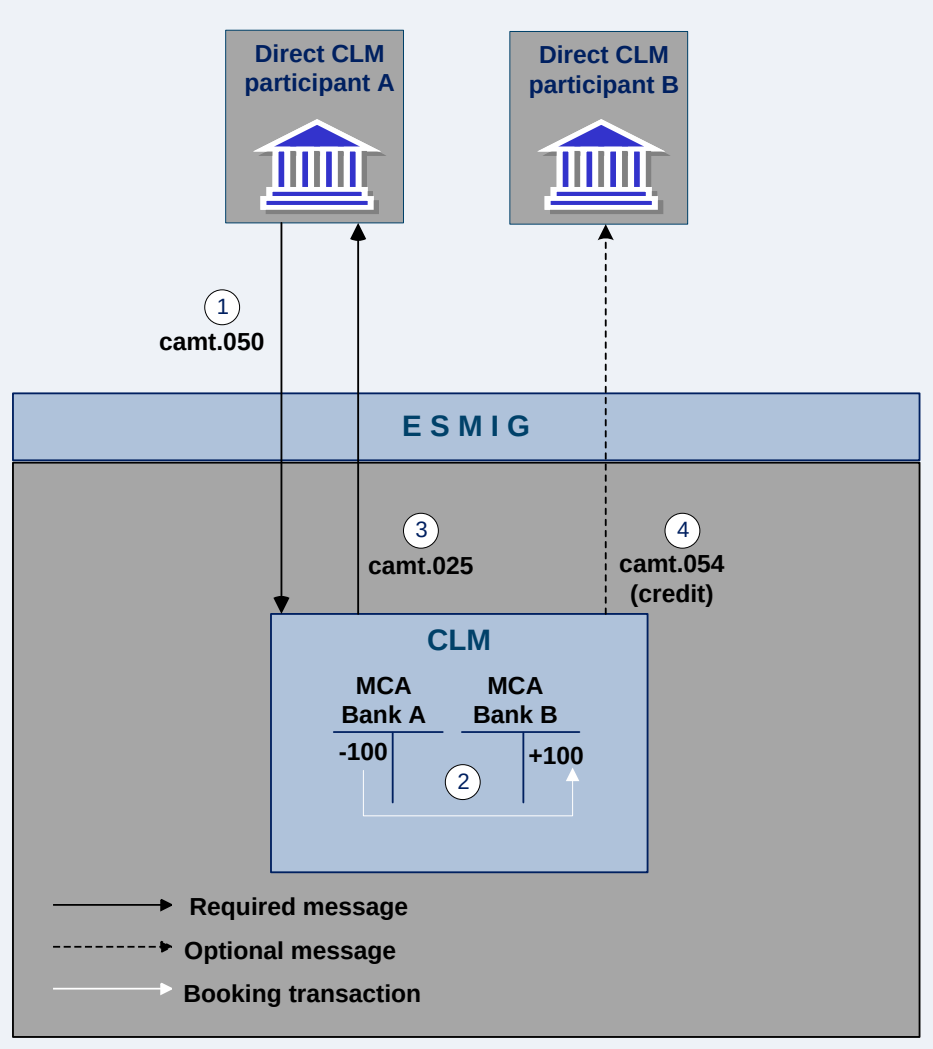


Figure 10 - camt.050 liquidity transfer intra-CLM

Process description

Step	Processing in/between	Description
1	CLM participant A via ESMIG to CLM	A camt.050 is sent from CLM participant A to ESMIG.
2	CLM	Booking on main cash accounts
3	CLM via ESMIG to CLM participant A	A camt.025 is sent by CLM via ESMIG to CLM participant A.
4	CLM via ESMIG to CLM participant B	An optional camt.054 is sent by CLM via ESMIG to CLM participant B.

Table 3 - process description

Used messages

- camt.050

- camt.054
- camt.025

6.2.2.3.4 Liquidity transfer between two dedicated cash accounts in different settlement services

A settlement service participant can transfer liquidity from a dedicated cash account in one settlement service to a dedicated cash account within another settlement service. The transfer is only possible if

- the whitelist authorises the participant to work with the dedicated cash account to be credited
- no whitelist is defined
- both accounts belong to the same party
- a central bank account is involved

Message flow example (liquidity transfer from RTGS dedicated cash account to T2S dedicated cash account)

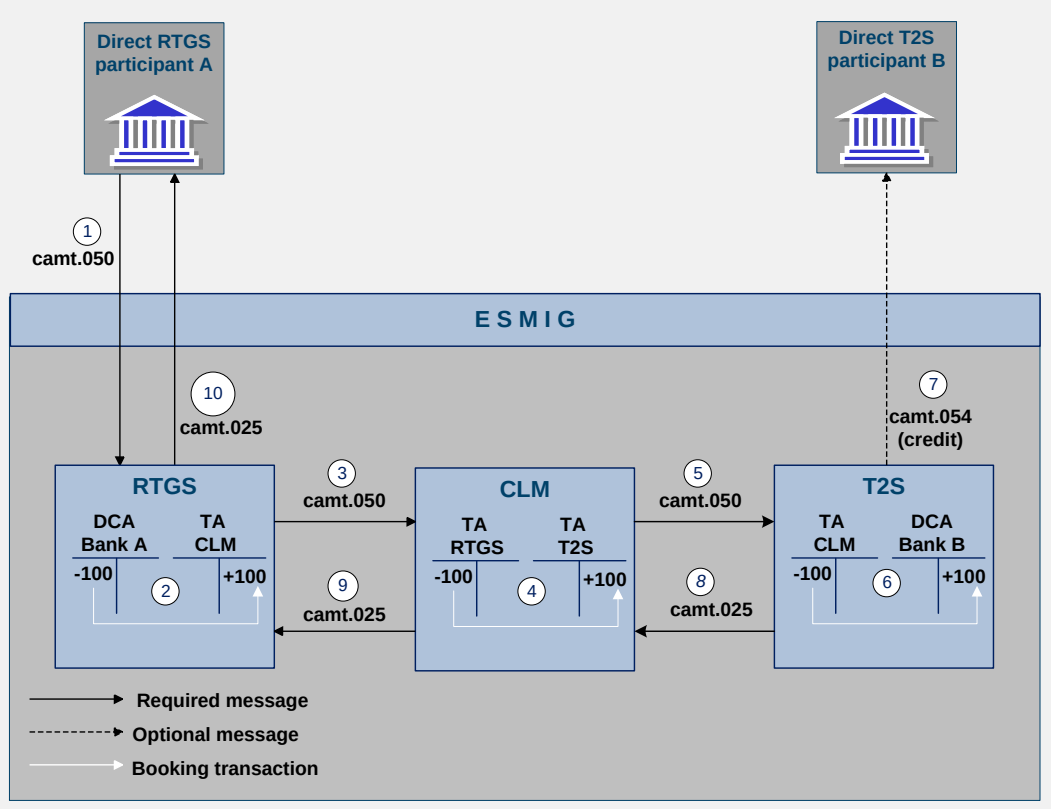


Figure 11 - camt.050 liquidity transfer inter-service

Process description

Step	Processing in/between	Description
1	RTGS participant via ESMIG to RTGS	A camt.050 is sent from a direct RTGS participant to ESMIG.
2	RTGS	Booking on RTGS dedicated cash accounts (RTGS dedicated cash account -> technical account-CLM)
3	RTGS to CLM	A camt.050 is forwarded to CLM service.
4	CLM	Booking on technical accounts in CLM (technical account-RTGS -> technical account-T2S)
5	CLM to T2S	A camt.050 is forwarded to T2S service.
6	T2S	Booking on T2S accounts (technical account –CLM -> dedicated cash account-T2S)
7	T2S via ESMIG to T2S participant	A camt.054 (credit) is sent by T2S via ESMIG to the T2S participant (optional).

Step	Processing in/between	Description
8	T2S to CLM	A camt.025 generated in T2S will be sent to CLM service.
9	CLM to RTGS	CLM forwards the camt.025 to the RTGS service.
10	RTGS via ESMIG to direct RTGS participant	A camt.025 is sent by RTGS via ESMIG to the direct RTGS participant.

Table 4 - process description

Used messages

- camt.050
- camt.054
- camt.025

6.2.2.3.5 Rejection of liquidity transfer orders

Liquidity transfer orders sent to the CLM service have to pass several validations before the liquidity is effectively transferred. Validations performed include technical checks, format checks as well as checks for the correct content.

For different reasons a liquidity transfer can be rejected and returned to the sending actor. The validations are distinguished in two types:

Technical validations

The system reaction on errors during technical validation differentiates between “Technical validation until schema validation” and “Technical validation after schema validation”.

The result of the technical validation can be different depending on the state of the schema validation:

- In case the technical validation until schema validation was not successful a ReceiptAcknowledgement (admi.007) is sent to the sending actor indicating which error occurred.
- In case the technical validation until schema validation was successful, the service performs the technical validation after schema validation.
- In case the technical validation after schema validation was not successful, the service sends the respective ISO message according to the business rules.

Business validations

Rejections after the business validations result in a receipt message (camt.025) is being sent to the sending actor including the respective error code(s) according to chapter Index of business rules and error codes [▸ 88].

6.2.2.3.5.1 Technical validations

Syntax/schema checks

The service shall parse the message and perform a field level validation, e.g. on correct data type, size. The service shall check whether all mandatory fields are populated. If the validation fails, a rejection notification with appropriate reason code must be sent to the sender of the message (depending on the submission channel, a message in A2A mode or an error message on the screen in U2A mode).

Duplicate checks

The service shall ensure that the same message has not already been received on the same business day.

6.2.2.3.5.2 Business validations

The validations described below will be performed in one step in order to capture all the possible breaches; the checks therefore must not stop after the first breach occurring, if there could be further breaches in the subsequent checks. If the validation failed overall, a rejection notification with appropriate reason codes for all breaches which occurred must be sent to the sender.

Check for duplicate liquidity transfer

The service shall carry out a duplicate submission control for incoming liquidity transfers. This control shall include the following fields: Sender of the message; Message Type; Receiver; Transaction Reference Number; Related Reference; Value Date and Amount.

Process specific authorisation checks

The service shall perform service specific authorisation checks. The liquidity transfer order can also be triggered by the scheduler in the case of standing orders.

Liquidity transfer group

The service shall check whether both accounts belong to the same participant or to participants within the same liquidity transfer group or not. If not, the order will be rejected. This check is not performed for CB accounts.

Whitelist check

The service shall check if the sending account is on the whitelist for liquidity transfers of the receiving account (if the receiving account has activated the whitelist feature). CLM shall check if the receiving account is on the whitelist for liquidity transfers of the sending account (if the sending account has activated the white-

list feature). If not, the order will be rejected. This check is not performed for accounts belonging to the same participant, or where the liquidity transfer involves one or more central banks accounts.

Field and reference data checks

The service shall perform the following field and reference data checks:

- field value validation - codes are valid, domain values are within allowed range
- cross-field validation – e.g. currency of the accounts involved is the same as the amount currency
- database checks – e.g. existence of parties and accounts

Subsequent processes and checks

- check vs. amount to be transferred

  The service shall check whether enough liquidity is available. Where there is a lack of liquidity the usual rules for partial execution apply.

- partial request

  If the liquidity transfer is initiated either by an ancillary system on its participants' behalf or by an automatic trigger from the scheduler, RTGS shall settle the liquidity transfer partially. For several standing orders, where the sum of all standing orders for intra-RTGS liquidity transfers of the participant to be settled at the same event is larger than the available liquidity, RTGS shall reduce all respective standing orders in a pro-rata mode.

- update cash balances

  The service shall book the liquidity transfer finally and irrevocably on the two RTGS dedicated cash accounts and shall update the defined value. RTGS shall send a (partly) success notification to the sending party and to the owner of the debited account.

- check on floor/ceiling

  Once the payment is final, the service shall check whether the account balance is below the floor balance or is above the ceiling balance that the account owner defined for the account. This check is performed only where the participant has defined a floor and/or a ceiling for the account. The check is done both on the debited and credited accounts.

  If either is the case, then the second step is to check which action has been specified:

  – Notification to be sent in A2A and/or notification to be sent as an alert in U2A.

  – Event-based liquidity transfer order for submission to central liquidity management to adjust the liquidity on the accounts involved so that the balance of the affected account reaches the specified target amount.

  The outcome of this final check does not affect the finality of the settlement of the payment.

6.2.3 Liquidity management features

6.2.3.1 Liquidity reservation

6.2.3.1.1 Overview

6.2.3.1.2 Liquidity reservation process

6.2.3.1.3 Effect of liquidity reservation

6.2.3.2 Floor/ceiling

6.2.3.2.1 Definition of floor/ceiling threshold

6.2.3.2.2 Breach of floor/ceiling threshold - notification

6.2.3.2.3 Breach of floor/ceiling threshold - automatic liquidity transfer

6.3 Reserve management

6.3.1 Overview

6.3.2 Reserve management process

6.4 Standing facilities management

6.4.1 Overnight deposit

6.4.1.1 Overview

The overnight deposit process is an element of the central liquidity management standing facilities and breaks down into three parts:

- setup of an overnight deposit
- overnight deposit reverse transaction and
- overnight deposit reimbursement and interest calculation

CLM participants can use the deposit facility to make overnight deposits with their national central banks.

As to the setup of an overnight deposit, CLM participants are able to transfer liquidity from their main cash account to the relevant overnight deposit account. It is also possible to activate a reverse transaction in order to reduce the amount deposited in the overnight deposit account. This has to be initiated before the deadline for the usage of standing facilities. CLM shall then calculate the interest to be paid on the overnight deposit and, at the start of the next business day, return automatically the capital amount and credit the interest on the CLM participant's main cash account. In case of a negative interest rate, CLM shall calculate the interest to be paid by the CLM participants on the overnight deposit and, at the start of the next business day, return automatically the capital amount to CLM and debit the interest to be charged from the CLM participant's main cash account. For central bank's outside the Eurosystem however, interest is always accumulated and paid on a monthly basis. CLM calculates the accumulated interest at the end of a calendar month and pays ten days after the first business day of the following month (warehoused payment).

Preconditions

A participant wishing to initiate an overnight deposit needs to:

- be a CLM participant
- be eligible to the overnight deposit facility and
- have an main cash account in CLM
- Dedicated overnight deposit account(s) need to be set up in the CLM.
- For reverse transactions only: An overnight deposit for that business day has been set up previously.
- For interest calculation only: The overnight deposit rate is required by CLM.

Furthermore, as regards the liquidity transfer to the central bank, a control will be in place in order to verify that the total amount envisaged for non-Eurosystem central banks will not be exceeded.

Triggers

The setup and reversal of an overnight deposit can be initiated through:

- an overnight deposit or reverse request sent by the CLM participant in A2A or
- manual input via U2A screen by the CLM participant (or central bank operator acting on behalf of the CLM participant)

The reimbursement of deposited capital and calculation of interest is triggered by the start of the next business day. CLM will automatically trigger the liquidity transfer for the repayment of the capital amount and the interest payment.

Note: There is an exception to this process for non-Eurosystem central banks. In this case interest is calculated at the end of each month and paid ten days after the first business day of the following month (warehoused payment).

Definition of execution times

It is possible for CLM participants to set up and/or to reverse an overnight deposit from the opening time of CLM (i.e. 19:00 and after overnight deposit and marginal lending reimbursement and interest calculation) until the general cut-off for the use of standing facilities (i.e. 18:15 with additional fifteen minutes on the last day of the reserve maintenance period) with the exception of the maintenance window.

Settlement principles

The following principles apply to the processing of liquidity transfer orders linked to overnight deposits:

- attempt to settle liquidity transfer immediately after its submission
- liquidity transfer orders may be revoked as long as they are not executed

6.4.1.2 Overnight deposit process

6.4.1.2.1 Setup overnight deposit

Message flow

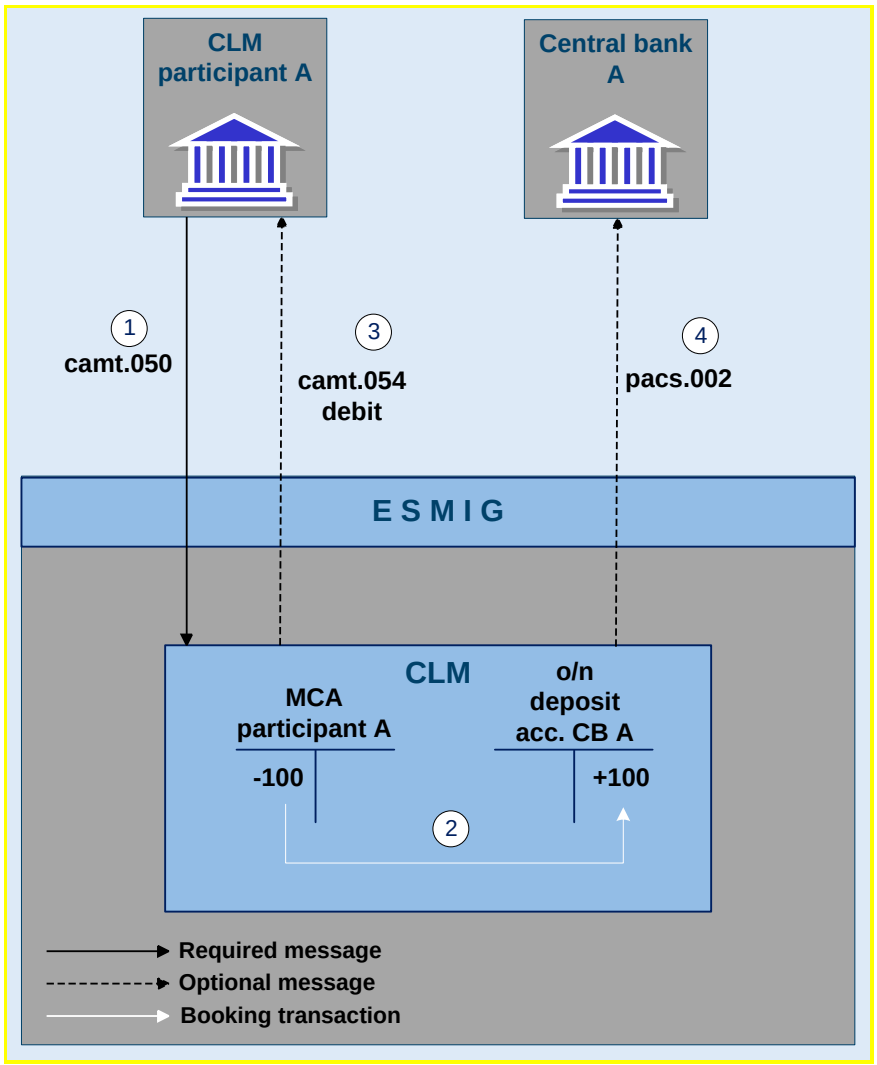


Figure 12 - camt.050 - setup overnight deposit

Used messages

- camt.050 - Liquidity Credit Transfer
- camt.054 - Bank to Customer Debit Credit Notification
- pacs.002 - FI to FI Payment Status Report
- admi.007 - Receipt Acknowledgement

Process description

The process of setting up an overnight deposit in CLM consists of the following four steps:

Step	Processing in/between	Description
1	CLM participant via ESMIG to CLM	The CLM participant sends a camt.050 to CLM.
2	CLM	CLM credits the overnight deposit account of the central bank and debits the main cash account of the participant if validations are positive.
3	CLM via ESMIG to CLM participant	An optional notification (camt.054 debit) is sent to the CLM participant.
4	CLM via ESMIG to central bank	CLM sends an optional acknowledgment (pacs.002) to the central bank.

Table 5 - process description

Expected results

The setup of an overnight deposit leads to a transfer of liquidity from the participant's main cash account to the overnight deposit account of the central bank.

Technical validations

At the reception of an overnight deposit request, the service interface completes the following technical validations:

- check mandatory fields

  The service interface ensures that all mandatory fields in the message received are populated.

- check for duplicate message

  The service interface ensures that the same message has not already been received.

After encountering the first negative validation result, the service interface does continue to validate as far as possible and reports all negative results together in a single message. The service interface rejects the order only after performing all possible technical validations. In case of a negative result of the technical validation, the request is rejected and a negative notification (admi.007) is sent to the instructing CLM participant.

If all technical validations are passed without errors, the request is sent to CLM for further processing, i.e. business validations.

Business validations

Once the technical validations are positively completed, the overnight deposit request goes through the following business validations:

- authorisation check

  CLM checks that only authorised CLM participants send an overnight deposit order for the relevant credit institution.

- validation of the values

  CLM checks that all provided values are valid according to predefined values or cross-field validations.

- account check

  CLM checks that the main cash account and the overnight deposit account mentioned in the request exist and are active for settlement in the relevant currency.

If any of the business validations fails to pass, the overnight deposit request is rejected and a negative notification (pacs.002) is sent to the instructing CLM participant.

6.4.1.2.2 Overnight deposit reverse transaction

Once CLM participants have set up an overnight deposit order, it is possible for the CLM participant (before the deadline for the usage of standing facilities) to activate a reverse transaction in order to reduce the amount deposited in the overnight deposit account.

Message flow

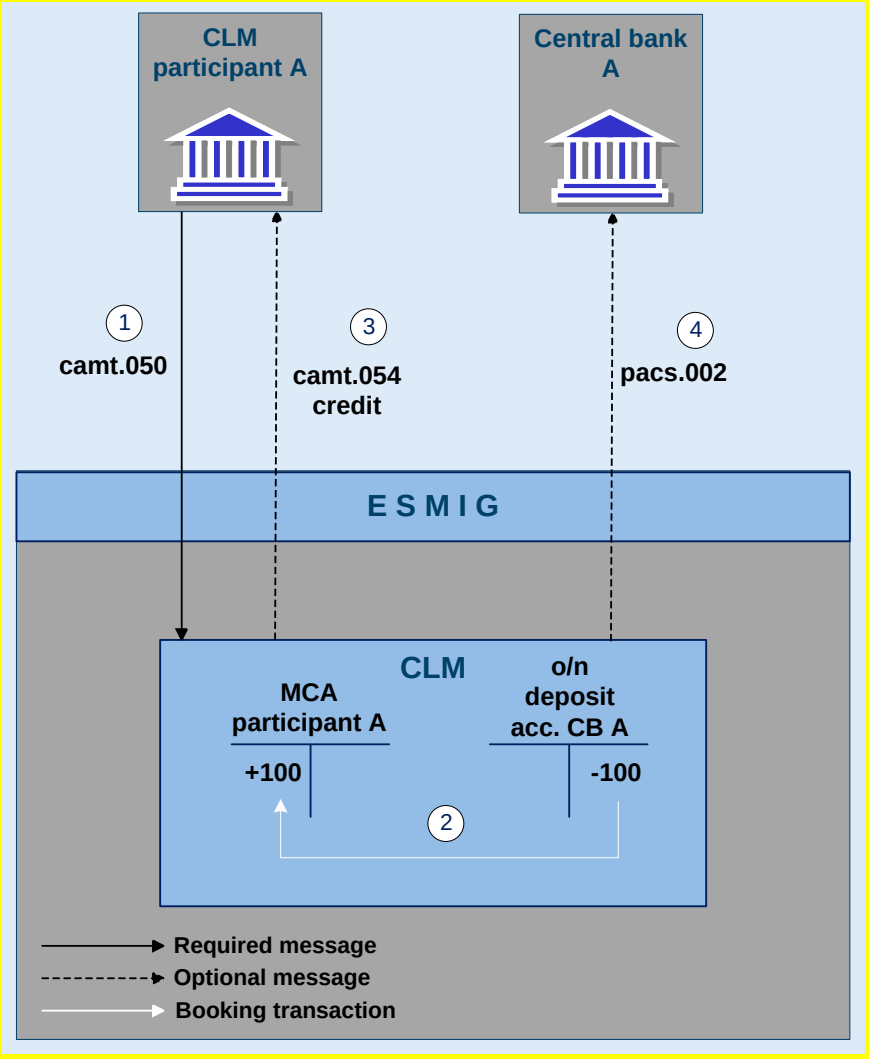


Figure 13 - camt.050 - reverse overnight deposit

Used messages

- camt.050 - Liquidity Credit Transfer
- camt.054 - Bank to Customer Debit Notification
- pacs.002 - FI to FI Payment Status Report
- admi.007 - Receipt Acknowledgement

Process description

The process of reversing an overnight deposit in CLM consists of the following four steps:

Step	Processing in / between	Description
1	CLM participant via ESMIG to CLM	The CLM participant sends a camt.050 to CLM.
2	CLM	CLM debits the overnight deposit account of the central bank and credits the main cash account of the participant if business validations are positive.
3	CLM via ESMIG to CLM participant	An optional notification (camt.054 credit) is sent to the CLM participant.
4	CLM via ESMIG to central bank	CLM sends an optional acknowledgement (pacs.002) to the central bank.

Table 6 - process description

Expected results

The reverse transaction leads to the transfer of liquidity from the central bank's overnight deposit account to the CLM participant's main cash account in the CLM.

Technical and business validations

The same validation processes as for setup of overnight deposits apply.

6.4.1.2.3 Overnight deposit reimbursement and interest calculation

At start of the next business day CLM calculates the interest to be paid on the overnight deposit and automatically sends the capital amount and the interest amount to the participants main cash account.

Message flow

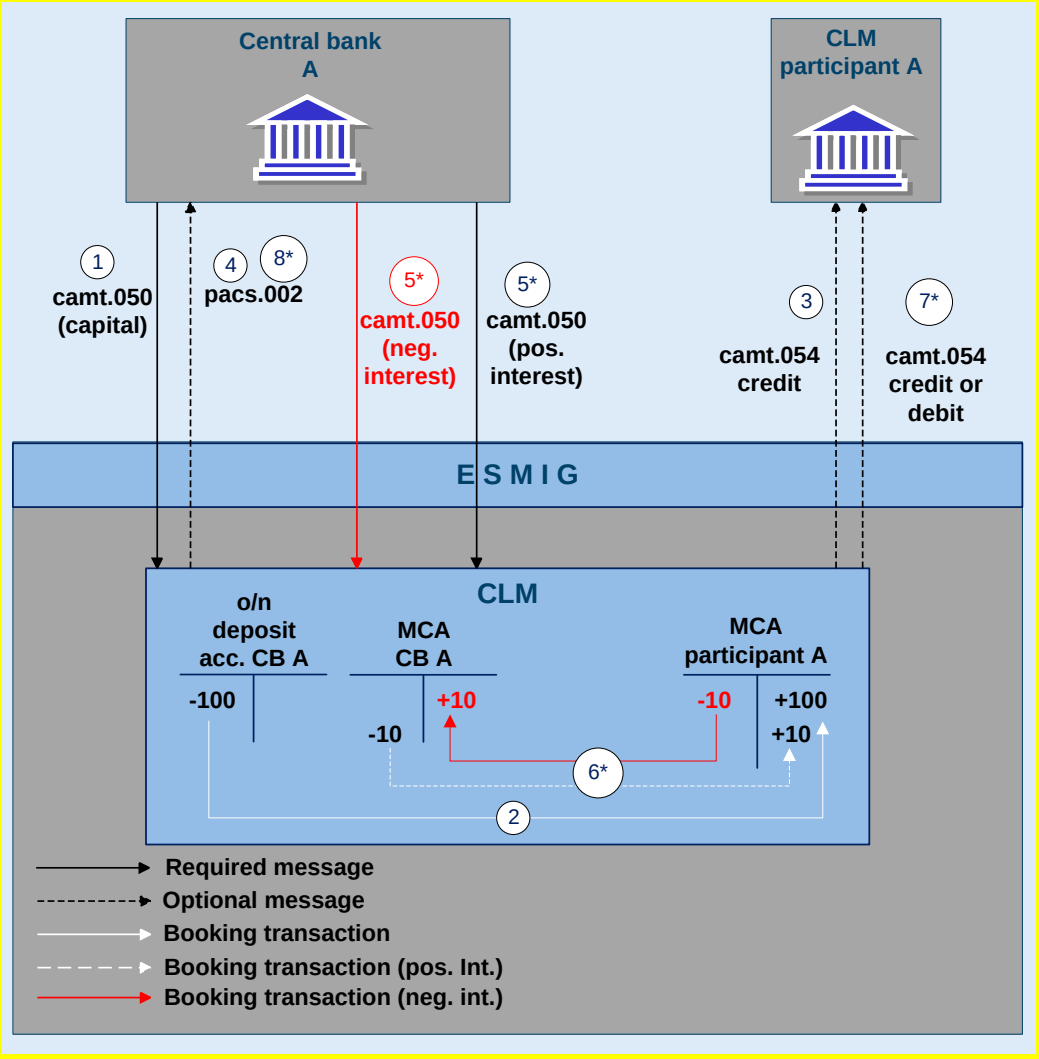


Figure 14 - reimburse overnight deposit

* Interest calculation and payment for non-Eurosystem central bank's is done at the end of the month.

Used messages

- camt.050 – Liquidity Credit Transfer
- camt.054 – Bank to Customer Debit Notification
- pacs.002 – FI to FI Payment Status Report
- admi.007 – Receipt Acknowledgement

Process description

The process of overnight deposit reimbursement and interest calculation in CLM consists of the following eight steps:

Step	Processing in / between	Description
1	Central bank via ESMIG to CLM	The central bank sends a camt.050 to CLM.
2	CLM	CLM debits the overnight deposit account of the central bank and credits the main cash account of the participant if validations are positive.
3	CLM via ESMIG to direct participant	An optional notification (camt.054 credit) is sent to the direct CLM participant.
4	CLM via ESMIG to central bank	CLM sends an acknowledgement (pacs.002) to the central bank.
5	Central bank via ESMIG to CLM	After calculating the interest (negative or positive) CLM generates a camt.050.
6	CLM	CLM debits the main cash account of the central bank and credits the main cash account of the participant if the overnight deposit rates is positive. [1] CLM credits the main cash account of the central bank and debits the main cash account of the participant if the overnight deposit rate is negative. [2]
7	CLM via ESMIG to direct participant	An optional notification (camt.054 credit or debit) is sent to the direct CLM participant.
8	CLM via ESMIG to central bank	CLM sends an acknowledgement (pacs.002) to the central bank.

Table 7 - process description

Expected results

The reverse transaction leads to the transfer of liquidity (deposited capital) from the central bank's overnight deposit account to the CLM participant's main cash account in CLM.

In addition, CLM debits (or credits) the central bank's main cash account and credits (or debits) the participant's main cash account with the calculated interest, depending on whether the overnight deposit rate is positive or negative.

Note: In the case of central banks from non-Eurosystem countries CLM creates warehoused payments for the accumulated interest to be paid on the first business day of the following calendar month.

1 CLM will generate an interest payment even if the overnight deposit rate is zero.

2 CLM will generate an interest payment even if the overnight deposit rate is zero.

The warehoused payments have a settlement date ten calendar days after the first business day of the following month. The respective connected central bank has the possibility to check the interest calculated and to cancel the warehoused payment if the calculation is not correct.

Technical and business validations

The same validation processes as for setup of overnight deposits apply.

6.4.2 Marginal lending “on request”

6.4.2.1 Overview

6.4.2.2 Marginal lending “on request” process

6.4.2.2.1 Setup marginal lending “on request”

6.4.2.2.2 Marginal lending reimbursement and interest calculation

6.4.3 Automatic marginal lending

6.4.3.1 Overview

6.4.3.2 Automatic marginal lending process

6.4.3.2.1 Process automatic marginal lending

6.4.3.2.2 Marginal lending reimbursement and interest calculation

6.5 Reference data management

6.5.1 Concept

6.5.2 Overview

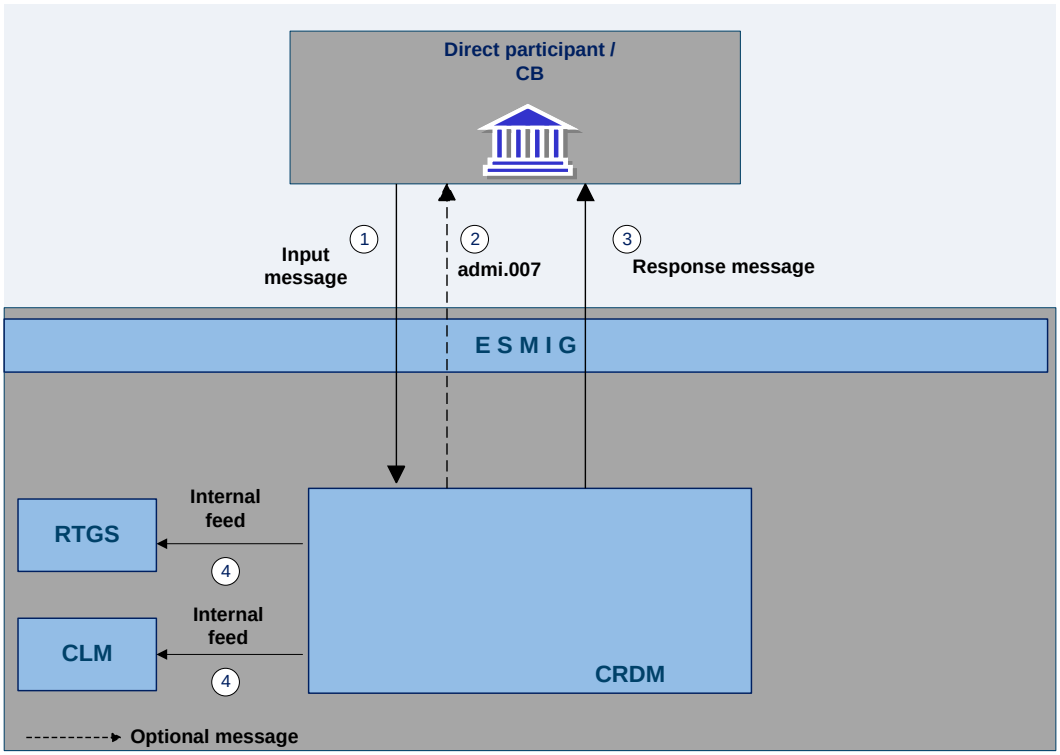
6.5.3 Reference data maintenance process

The common reference data maintenance process can be described as a common message flow that applies to every business scenario.

Upon the sending of a request instructed with an input message, a related response message or a technical validation error message is returned.

6.5.3.1 Reference data objects

The shared generic message flow is as follows:



Step	Activity
1	The authorised actor (CLM or RTGS participant or another actor operating on behalf of the MCA or RTGS owner under a contractual agreement) sends the input message to CRDM to create, modify or delete a common reference data entity.
2	In case of rejection upon technical validation, an admi.007 receipt acknowledgement is sent by CRDM to the sender of the originating request.
3	CRDM performs the business validation and sends to the authorised actor a response message to report processing result.
4	CRDM will propagate the updated information to the subscribing services for their internal processing.

The messages used in the interaction change depending on the business scenario to be covered.

In the following table, for every concerned common reference data entity and related business scenario, the input and response messages are defined.

Business scenario	Input message	Response message
Create standing order	camt.024	camt.025
Modify standing order	camt.024	camt.025
Delete standing order	camt.071	camt.025

6.5.3.2 Reference data maintenance types

6.5.3.3 Validity of reference data objects

6.5.3.4 Reference data archiving and purging

6.5.3.5 Lifecycle of reference data objects

6.5.3.6 Reference data maintenance instructions processing

6.5.3.7 Reference data status management

6.6 Information management

6.6.1 Status management

6.6.1.1 Concept

EMIP services inform their EMIP actors of the processing results. This information is provided to the EMIP actors through a status reporting which is managed by the status management process. The communication of statuses to EMIP Actors is complemented by the communication of reason codes in case of negative result of an EMIP service process.

6.6.1.2 Overview

The status management process manages the status updates of the different instructions existing in EMIP service in order to communicate these status updates through status advice messages to the EMIP actors

throughout the lifecycle of the instruction. The status management process also manages the reason codes to be sent to EMIP actors in case of negative result of an EMIP service process (eg to determine the reason why an instruction is unsuccessfully validated or settled).

The status of an instruction is indicated through a value, which is subject to change through the lifecycle of the instruction. This value provides EMIP actors with information about the situation of this instruction with respect to a given EMIP process at a certain point in time.

Since each instruction in an EMIP service can be submitted to several processes, each instruction in EMIP has several statuses. However, each of these statuses has one single value at a certain moment in time that indicates the instruction's situation at the considered moment. Depending on its instruction type, an instruction is submitted to different processes in T2S. Consequently, the statuses featuring each instruction depend on the considered instruction type.

The following sections provide:

- the generic principles for the communication of statuses and reason codes to EMIP actors
- the list of statuses featuring each instruction type as well as the possible values for each of these statuses
- an overview of the reason codes management

However, reason codes are not exhaustively detailed below but are provided in section Index of status value and codes [▸ 88].

6.6.1.3 Status management process

Communication of statuses and reason codes to EMIP actors

EMIP actors can query, at any point in time, the status values and reason codes of their instructions.

The statuses can be classified into two different types, common to all type of instructions:

- "Intermediate status" - There is a change occurred in any of the statuses of the instruction, but it does not imply the end of the processing of the instruction in EMIP. Further status updates are to be communicated to the EMIP actors until an "end status" is sent.
- "Final status" - This is the last status of an instruction (ie the status that an instruction has when processing for that instruction ends). If the status of an instruction is not of an "end status" type, then the instruction is still under process in EMIP. At a point in time, any instruction in EMIP reaches an "end status", as any instruction is settled, executed, cancelled or denied in the end.

For some specific status updates, the status management process informs the EMIP actors of the status change through the sending of status advice messages (according to their message subscription configuration).

Statuses and status values in EMIP

As previously mentioned, the statuses of an instruction depend on the considered instruction type. The following paragraphs provide the list of statuses and status values.

CLM service statuses are:

- message statuses
- payment statuses

CRDM statuses are:

- reference data maintenance instruction processing status

Message statuses

Indicates the status of the message (not applicable for queries) and it can have the following statuses:

Status value	Definition	Direction	Intermediate status/ final status
System entry	Message status after entering the CLM service	Incoming	Intermediate
Waiting for open queue	Message status of a message arriving before the “Start of day trade phase”	Incoming	Intermediate
Warehoused	Status of a message with a value date in the future or status of a message with the value date of the current business day until it will be forwarded to the processing at the start of the day trade phase	Incoming	Intermediate
Processed	Message status if an incoming message is finally processed independent of whether the result is positive or negative	Incoming	Final
To be provided	Status of an outgoing message ready to be send to ESMIG	Outgoing	Intermediate
Provided	Status of an outgoing message sent to ESMIG	Outgoing	Final

One business case can include one or more single messages which may have different message status. The message status is the detailed status related to the processing of each single message of a business case. The business case status is a result of the message status and the related processing.

Message statuses will not be reported via status message.

Payment statuses

Indicates the status of the payment instruction and it can have the following statuses:

Status value	Definition	Intermediate/ final status	Reported via status message
Valid	Status after positive business validation	Intermediate	-
Warehoused	Status of a payment with a value date of a future business day and status of a payment with the value date of the current business day until it will be forwarded to the processing at the start of the day trade phase. From then on they will be processed normally. To this booking status a time stamp is added. In general, warehoused payments are submitted up to ten calendar days in advance. In this case, the payment message will be warehoused until the day trade phase of CLM with the respective date starts.	Intermediate	
Earmarked	Status of a payment which is ready for booking but not taken into account for various reasons. The booking status earmarked is split into the following business case status: - Accounting stopped due to earliest debit time indicator - AS accounting not yet started due to active information period - Accounting stopped due to exclusion - Pending decision on exclusion - Waiting for end of cycle - Waiting for completion of debits - Waiting for algorithm 4	Intermediate	-
Queued	Status of a payment which is ready for booking but the first booking attempt was unsuccessful. Pending payments are waiting for the next booking attempt. To this booking status a time stamp is added.	Intermediate	-
Revoked	Status of a payment which is revoked by a system user	Final	-

Status value	Definition	Intermediate/ final status	Reported via status message
Rejected	Status of a payment which is rejected by the system or by a system administrator (all payments with error code, except error code for revoked)	Final	Mandatory
Settled	Status of a payment after booking. Final payments cannot be revoked.	Final	Optional
Invalid	Messages which are negatively business validated in the entry disposition and do not lead to a booking attempt	Final	-

Task queue statuses

All data inputs or data changes by the user (called tasks, eg entering a liquidity transfer) are managed in the task queue administration of the respective service. The following statuses apply for CLM service.

Status value	Definition	Transition possible to status	Intermediate/ final status
To confirm	The task must be confirmed by a second user and will not be processed. This status can only occur in U2A for four eyes principle. It is the only status in which a task revocation is possible directly via respective screens.	Processing, revoked, rejected	Intermediate
Processing	The task is ready to be processed at the moment. It can only occur directly after the task initiation (or after “to confirm” in case of four eyes principle).	Waiting, pending, partially pending, revoked, rejected, completed	Intermediate
Waiting	The task can be processed, but the processing is not started till now, eg due to a running or stopped algorithm.	Pending, partially pending, revoked, completed, rejected	Intermediate

Status value	Definition	Transition possible to status	Intermediate/ final status
Pending	A task should be stored with status “pending”, if the task was already tried to process at least one time but it could not be finalised. The processing was interrupted after the storage of entries initiated by the task and before the final processing of these entries. The task will be updated and further processed, if the preconditions for the pending status (eg liquidity increase) are changed.	Partially pending, completed, revoked, rejected	Intermediate
Partially pending	A task should be stored with status “partially pending” if the user's order cannot be processed completely (eg an increase of reservation cannot be executed completely because of lack of liquidity). The order is processed as far as possible. The task will be updated and further processed, if the preconditions for the "partially pending" status (eg liquidity increase) are changed.	Completed, revoked, rejected	Intermediate
Revoked	The task has been revoked by a user.	-	Final
Rejected	An error was detected.	-	Final
Completed	The task was processed successfully and the business case stemming from the task is final. The tasks changing an existing business case (like queue management) are completed, if the respective action is completely processed. The business case (managed payment) does not have to be final.	-	Final

Note: The responsibility for the tasks switches over from the user to the respective service according to the storage of the entry time.

The relevant entry time is stored:

- for two eyes principle: by storage of the task within the responsible service.
- for four eyes principle: by storage of the confirmation.

Note: Tasks with status “waiting“, “processing“ or “pending“ can only be revoked via a new task, eg a credit line can only exist once per participant. Therefore the second credit line change will revoke the first one.

Reference Data maintenance instruction processing status

6.6.2 Report generation

Concept

EMIP services periodically inform with a set of predefined reports which deliver information specifically for the service business. They contain information, which is based on the data available for a party. The respective service triggers the generation of a report based on a business event, eg end of day, or at a predefined time. Please see chapter Index of status value and codes [88] for the list of configurable business events. Depending on the party's preferences the report is either sent out directly after creation or stored for later retrieval via the report query.

Overview

The report types generated by the respective service and the sort of information provided are described below.

In general all reports differ in and are defined by the following characteristics:

- the concerned party
- the sort of information collected
- the moment of data extraction during the business day and
- the reporting period

All information about the necessary attributes in each named category is stored as static data in CRDM and influences the generation of the report.

Report generation process

A generated report is available for download until it is replaced by the next, new generation of it, ie a report that is created at the end of day of the current business day replaces the report that was created at the end of day of the previous business day. The replaced report is no longer available for download. Nonetheless, as any other message, a report can be resent if the report message was sent in A2A mode before.

Sort of information - Report types

The EMIP services provide the following report type:

Report providing service	Report name	ISO message	ISO code
CLM	Statement of accounts	BankToCustomerStatement	camt.053

Concerned party

Each report type provides information on a certain scope of data. The data scope is indicated by the party for which it is configured. In addition to reports on party level, CBs can also opt for reports on system entity level, ie reports providing the CB with information relating to all its parties. CBs can only configure reports on system entity level for themselves.

The concerned party has to be specified, when the report is configured for the first time.

Moment of data extraction

The creation of a report is always triggered at a certain point in time by the respective EMIP service. This point in time can be a specific time, eg 10:00 am or a specific event of the business day, eg end of day. A new report configuration can be set-up at the earliest for the next business day. The moment of data extraction as well as possible validity limitations have to be specified when the report is configured for the first time. The respective service only creates those reports for which the underlying report configurations is valid at the current business day.

Reporting period

The EMIP services distinguish between two different report classifications - complete reports and delta reports, which are all based on the latest available data. The difference between both is the time scope which is considered:

- Complete reports cover the current business day and provide the current values of all selected items at the time of the creation of the report.
- Delta reports also consider the current business day but provide only information on the selected items which values changed since the previous report was created. The previous report can likewise be a complete report or a delta report. Therefore, the creation timestamp of the previous report is considered as the starting point in time for the reporting period. If there is no previous report for the current business day, the SoD is considered as the starting point in time for the reporting period.

Possible recipients of a report

All reports can be received by the technical address of

- concerned party

- another authorised party (eg co-manager)

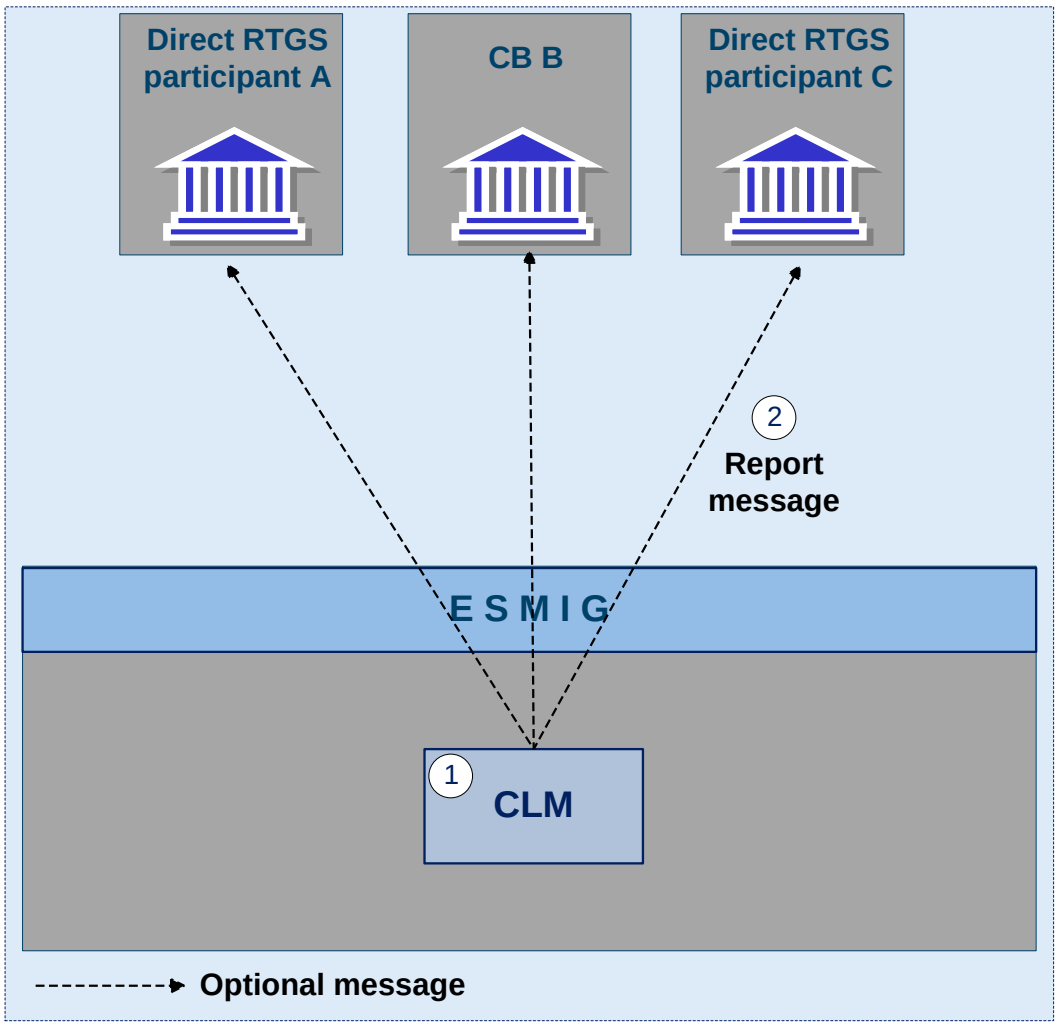


Figure 15 - CLM Report generation process

A created report can be received by one or several receivers. Each party can decide, if it wishes to receive a report directly after its creation or if it wants to query it ad-hoc.

If a recipient wishes to receive a report directly after its creation, this has to be stored in the static data configuration of the report. That means the subscription of a report is independent from the message subscription.

If a recipient does not wish to receive a report directly after its creation but to query it afterwards, this behaviour of the service has to be stored in the CRDM configuration of the report as well. Also this recipient is stored as recipient of a report.

As a general principle the recipient(s) of a report can be different from the concerned party. For information about the setup of report configuration for specific concerned parties and recipients of a report please see UHB chapters related to report configuration setup.

Preconditions for report creation

In order to avoid unnecessary processing and storage the respective service does not create reports automatically. So, to initiate the creation of a report, the requiring receiver has to configure the report in advance. The configuration of the report has to be done via the graphical user interface of CRDM, which is described in the UHB.

This configuration is then stored as static data and is valid until the receiver decides that the report has not to be created anymore or until the “valid to” date stored within the report configuration is reached.

Communication channel

The respective service offers direct communication to applications via XML-messages in application-to-application mode (shortly A2A mode) as well as screen-based online access for connected users in user-to-application mode (U2A mode).

All reports that are offered by the EMIP services are available both in A2A and U2A mode.

In A2A mode the receiver gets the specific report pushed, provided that the push preference for the report is stored for the receiver in static data. Otherwise the report is just stored after generation.

To pull formerly created reports, a report query has to be sent either via the graphical user interface to the respective service or via A2A mode with the specification of the report instance asking for. In case the user has the respective privilege to obtain the requested report, it is sent out to the inquirer. Please see chapter Query management [▸ 69].

Parameter synthesis

The following parameters are specified for the setup of a report.

concerned process	parameter	created and updated by	mandatory/ optional	possible values	hint
Setup of a report	Report type	CRDM actor	Mandatory	Statement of accounts	
Setup of a report	Concerned party	CRDM actor	Mandatory	N/A	
Setup of a report	System entity wide reporting flag	CRDM actor	Mandatory	Yes, No	This flag can only be set to “Yes” for CBs as they are eligible for system entity wide reports.

concerned process	parameter	created and updated by	mandatory/ optional	possible values	hint
Setup of a report	Moment of data extraction	CRDM actor	Mandatory	Time event, business event	
Setup of a report	Reporting period	CRDM actor	Mandatory	Complete report, delta report	
Setup of a report	Possible recipient of a report	CRDM actor	Mandatory	N/A	
Setup of a report	Communication channel	CRDM actor	Mandatory	Push mode, pull mode	
Setup of a report	Valid from	CRDM actor	Mandatory	ISO-date	
Setup of a report	Valid to	CRDM actor	Optional	ISO-date	The field „Valid To" is the only field that can be amended after the report configuration has been stored.

Detailed information on the sort of information - report type - statement of accounts

It includes information on one main cash account of a dedicated CLM participant. It is only possible to configure this report as complete report for the end of day. The report is not available during the day and it is not available as delta version.

The report provides information about all items that have been booked to the account and balance information of the current business day. It does not include information from other services, ie there is no report including CLM and RTGS information.

Used messages

- camt.053

6.6.3 Query management

6.6.3.1 Concept

Queries are provided by EMIP services to the system user as a means of satisfying his information needs on demand. He can obtain information on different business items by submitting query requests to EMIP services. These are answered on the basis of the latest data available in EMIP services.

6.6.3.2 Overview

EMIP services provide a range of predefined query types, which the system user can use to request information on business items. All user queries are available for all authorised system users of EMIP services.

They can send queries to EMIP services in A2A mode or in U2A mode. Generally, all queries are processed in real time. Exceptions occur during the maintenance window. Queries sent in A2A mode during the maintenance window are queued and notice of the queued status is given immediately to the requesting system user. The query request is answered after the end of maintenance window. It is not possible to send queries in A2A and U2A mode during the maintenance window.

6.6.3.3 Query management process

Initiating queries

In order to obtain the desired information the system user needs to submit a query to an EMIP service. For the communication with EMIP services in A2A mode all query and response messages are set up as XML messages compliant with the ISO20022 standard. For the communication with EMIP services in U2A mode a graphical user interface based on a standard browser application is provided.

Case: query request on CLM service

Message flow

Process description

Step	Processing in/between	Description
1	CLM participant via ESMIG to CLM	An authorised system user of a CLM participant A sends a query message via ESMIG to the CLM service
2	CLM	CLM message check and validation positive
3	CLM via ESMIG to CLM participant	Query response (positive or negative) via ESMIG to CLM participant A generated by the CLM service

Used messages

- See following table

In general an authorised system user can send each query in A2A mode as well as in U2A mode. However, there are some queries which are only accessible via U2A mode. Query availability in the respective communication mode is shown in the table below.

Related service	Query type	Initiation via GUI (U2A mode)	Initiation via XML message (A2A mode)		
			Query request message	Query response message for operational error	Query response message for business data
CLM	Account Statement Query	X	-	-	-
CLM	Audit Trail for CLM Query	X	GetAudit		ReturnAudit
CLM	Available Liquidity CLM Query	X	camt.003 GetAccount	camt.004 Return Account	camt.004 Return Account
CLM (- overall)	Available Liquidity Overall Query	X	camt.003 GetAccount	camt.004 Return Account	camt.004 Return Account
CLM	Credit Line on single Main Cash Account Query	X	New message or camt.003 GetAccount	New message or camt.004 ReturnAccount	New message or camt.004 ReturnAccount
CLM	Penalty Query	X	camt.998 GetPenalty_RM	camt.998 ReturnPenalty_RM	camt.998 ReturnPenalty_RM
CLM	Current Reservations Query	X	camt.046 GetReservation	camt.047 ReturnReservation	camt.047 ReturnReservation

Related service	Query type	Initiation via GUI (U2A mode)	Initiation via XML message (A2A mode)		
			Query request message	Query response message for operational error	Query response message for business data
CLM	Minimum Reserve Query	X	camt.003 GetAccount	camt.004 Return Account	camt.004 Return Account
CLM	Settlement Information Query	X	camt.998 GetSettlementInformation	camt.998 ReturnSettlementInformation	camt.998 ReturnSettlementInformation
CLM	Transactions for CLM Query	X	camt.005 GetTransaction	camt.006 ReturnTransaction	camt.006 ReturnTransaction
CRDM	Audit Trail for CRDM Query	X	GetAudit	ReturnAudit	ReturnAudit
CRDM	Calendar Query	X	GetCalendar	ReturnCalendar	ReturnCalendar
CRDM	Direct Debit Mandate Query	X	GetDirectDebit	ReturnDirectDebit	ReturnDirectDebit
CRDM	Directory Query	X	GetDirectory	ReturnDirectory	ReturnDirectory
CRDM	Error Code Query	X	GetErrorCode	ReturnErrorCode	ReturnErrorCode
CRDM	Event Query	X	camt.018 GetBusinessDayInformation	camt.019 ReturnBusinessDayInformation)	camt.019 ReturnBusinessDayInformation
CRDM	Main Dedicated Cash Account Reference Data Query	X	acmt.025 AccountQueryList	acmt.026 AccountListReport	acmt.026 AccountListReport
CRDM	Message Subscription Query	X	-	-	-
CRDM	Participant Reference Data Query	X	reda.015 PartyQuery	reda.017 PartyReport	reda.017 PartyReport
CRDM	Party Reference Data Query	X	reda.015 PartyQuery	reda.017 PartyReport	reda.017 PartyReport
CRDM	Role Query	X	-	-	-

Related service	Query type	Initiation via GUI (U2A mode)	Initiation via XML message (A2A mode)		
			Query request message	Query response message for operational error	Query response message for business data
CRDM	Standing Order Liquidity Query	X	camt.069 GetStandingOrder	camt.070 ReturnStandingOrder	camt.070 ReturnStandingOrder
CRDM	Standing Order Reservations Query	X	camt.046 GetReservation	camt.047 ReturnReservation	camt.047 ReturnReservation
Scheduler	System Time Query	X	camt.018 GetBusinessDayInformation	camt.019 ReturnBusinessDayInformation	camt.019 ReturnBusinessDayInformation
CRDM	Whitelist Query	X	-	-	-
Billing	VAT Query	X	-	-	-
Billing	Invoice Query	X	-	-	-

The different types of queries in EMIP services are static regarding the set of selection parameters, which can be mandatory, optional or conditional. RTGS and CLM service do not offer dynamic queries.

Preconditions for successful processing of queries

The relevant EMIP service validates the plausibility of the search criteria that were specified by the system user. In addition, the relevant service ensures that the sender of the query is allowed to retrieve the requested information by checking, whether the system user has been granted the necessary privilege.

Only if the system user possesses the necessary privilege to use the initiated query, the requested business information is provided. The privilege has to be granted in advance.

Providing data for queries

If all checks performed by respective service were successful, it extracts the requested business information from the production data. The system user receives the latest available data. If one of the plausibility and privilege checks performed by respective service fails, the system user receives a response indicating the error that has occurred.

Retrieving the query response

In case the extraction of the query data is successful, the respective service sends a query response containing the requested business information back to the requesting system user. In case the extraction of the

query data returns a zero result, the requesting system user receives appropriate information. If a retrieval of the query result fails, then an error response is provided to the system user.

If the system user has sent the query via U2A mode, the response is given to the system user in U2A mode. The U2A dialogue is described in more detail in the UHB.

If the system user has sent the query via A2A mode, the response is given to the same system user in A2A mode. The respective service does not allow the routing of the query response to a dedicated technical address.

Parameter synthesis

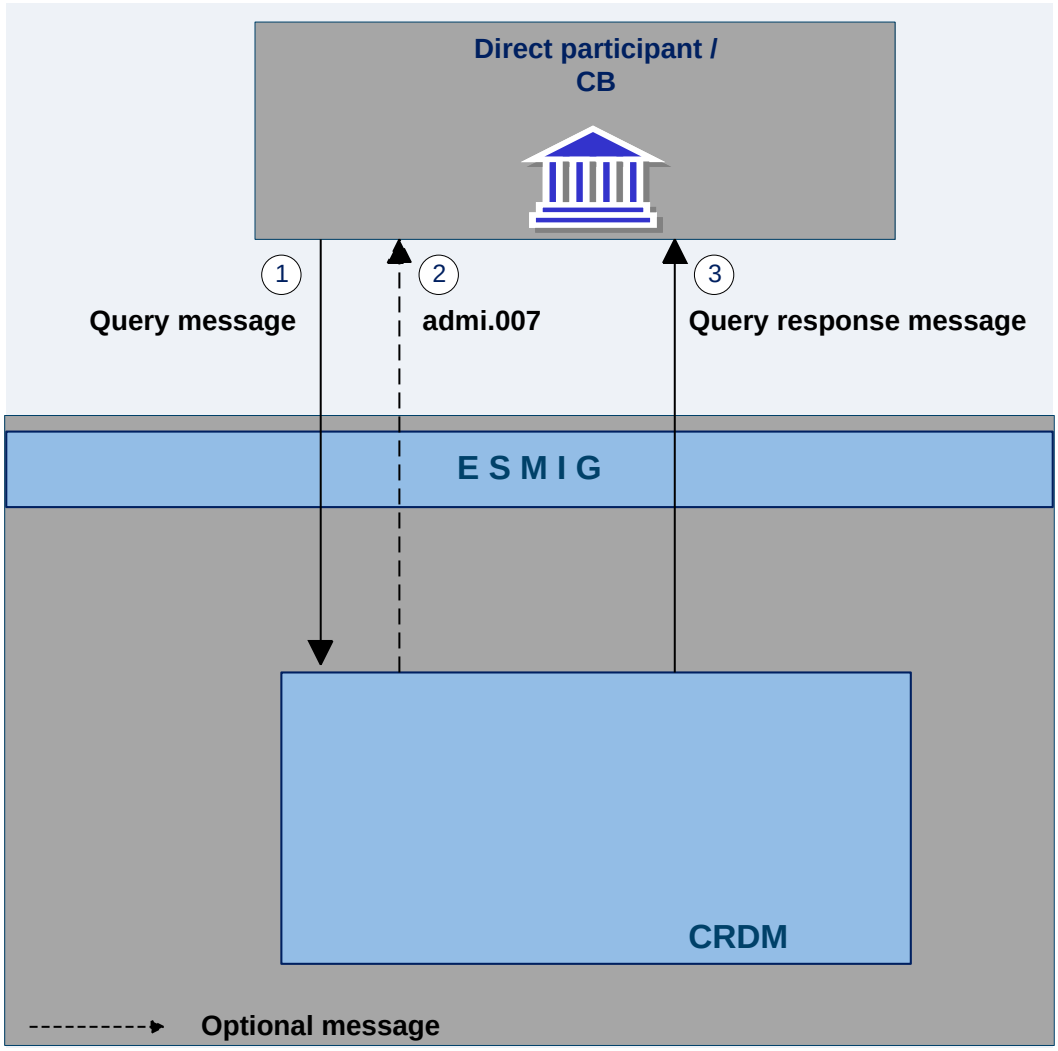
No specific configuration from the system user is needed.

6.6.3.3.1 Common reference data query

The common reference data query can be described as a common message flow that applies to every business scenario.

Upon the sending of a query instructed with an input message, a related query response message or a technical validation error message is returned.

The shared generic message flow is as follows:



Step	Activity
1	The authorised actor (CLM or RTGS participant or another actor operating on behalf of the MCA or RTGS owner under a contractual agreement) sends the query message to CRDM to retrieve a set of common reference data entity.
2	In case of rejection upon technical validation, an admi.007 receipt acknowledgement is sent by CRDM to the sender of the originating query.
3	CRDM performs the business validation and sends to the authorised actor a query response message to report processing result that is retrieved records or business error found during the validation.

The messages used in the interaction change depending on the query to be performed.

In the following table, for every concerned common reference data entity, the query and query response messages are defined.

CRDM entity	Query message	Query response message
Standing order	camt.069	camt.070

7 Data warehouse

8 Billing

9 Legal archiving

10 Contingency services

11 Catalogue of messages

11.1 Introduction

11.2 General information

11.2.1 Message validation

11.2.2 Communication infrastructure

11.3 List of messages

11.3.1 Account management (acmt)

11.3.2 Administration (admi)

11.3.3 Cash management (camt)

11.3.3.1 camt.003

11.3.3.1.1 Overview and scope of the message

11.3.3.1.2 Schema

11.3.3.2 camt.004

11.3.3.2.1 Overview and scope of the message

11.3.3.2.2 Schema

11.3.3.8.1 Overview and scope of the message

11.3.3.8.2 Schema

11.3.3.9 ModifyStandingOrder (camt.024)

11.3.3.9.1 Overview and scope of the message

This chapter illustrates the ModifyStandingOrder message.

The ModifyStandingOrder message is sent by an actor authorised to create or modify standing orders for liquidity transfers.

The ModifyStandingOrder message is replied by a camt.025 to return a positive technical response to the sender of the message or to provide detailed information in case of an error.

11.3.3.9.2 Schema

Outline of the schema

The ModifyStandingOrder message is composed of the following message building blocks:

MessageHeader

This block is mandatory and provides with the message identification provided by the requesting actor.

StandingOrderIdentification

This block is mandatory and provides with all the key information to identify an existing standing order to be amended or a new standing order to be created.

NewStandingOrderValueSet

This block is mandatory and provide with the pieces of information related to the standing order to be modified or created.

It includes the amount to be transferred, the required account references to perform the transfer, the intended validity period and the execution type in terms of event identification.

References/links

The schema and the related documentation in HTML/PDF format as well as the message examples are provided within the MyStandards repository under the following link:

https://www.swift.com/mystandards/CSLD/camt.024.001.05

11.3.3.10 GetStandingOrder (camt.069)

11.3.3.10.1 Overview and scope of the message

This chapter illustrates the GetStandingOrder message.

The GetStandingOrder message is sent by an authorised actor to retrieve standing order information.

The GetStandingOrder message is replied by a camt.070 to return the retrieved standing order information or to provide detailed information in case of an error (eg no rows retrieved).

11.3.3.10.2 Schema

Outline of the schema

The GetStandingOrder message is composed of the following message building blocks:

MessageHeader

This block is mandatory and provides with the message identification provided by the requesting actor.

RequestType

This block is optional and can be used to specify which kind of query must be performed.

StandingOrderQueryDefinition

This block is mandatory and provides with all the search criteria that must be used to filter standing order records in the CRDM coverage. Possible criteria are account and BIC.

References/links

The schema and the related documentation in HTML/PDF format as well as the message examples are provided within the MyStandards repository under the following link:

https://www.swift.com/mystandards/CSLD/camt.069.001.02

11.3.3.11 ReturnStandingOrder (camt.070)

11.3.3.11.1 Overview and scope of the message

This chapter illustrates the ReturnStandingOrder message.

The ReturnStandingOrder message is sent by CRDM to an authorised actor to provide with requested standing order information.

The ReturnStandingOrder message is sent as a response to a previously sent camt.069.

11.3.3.11.2 Schema

Outline of the schema

The ReturnStandingOrder message is composed of the following message building blocks:

MessageHeader

This block is mandatory and provides with the message identification provided by the requesting actor as well as the original business query message identification and the request type specifying the kind of query that has been performed.

ReportOrError

This block is mandatory and includes either the retrieved records or the error occurred during the query processing (eg no records retrieved).

Report

This block is mandatory and provides with all the pieces of information related to the retrieved standing order.

References/links

The schema and the related documentation in HTML/PDF format as well as the message examples are provided within the MyStandards repository under the following link:

https://www.swift.com/mystandards/CSLD/camt.070.001.03

11.3.3.12 DeleteStandingOrder (camt.071)

11.3.3.12.1 Overview and scope of the message

This chapter illustrates the DeleteStandingOrder message.

The DeleteStandingOrder message is sent by an actor authorised to delete standing orders for liquidity transfers.

The DeleteStandingOrder message is replied by a camt.025 to return a positive technical response to the sender of the message or to provide detailed information in case of an error.

11.3.3.12.2 Schema

Outline of the schema

The DeleteStandingOrder message is composed of the following message building blocks:

MessageHeader

This block is mandatory and provides with the message identification provided by the requesting actor.

StandingOrderDetails

This block is mandatory and provides with all the key information to identify an existing standing order to be deleted. Both identification and account identification must be provided.

References/links

The schema and the related documentation in HTML/PDF format as well as the message examples are provided within the MyStandards repository under the following link:

https://www.swift.com/mystandards/CSLD/camt.071.001.02

11.3.4 Headers (head)

11.3.4.1 head.001

11.3.4.1.1 Overview and scope of the message

This chapter illustrates the BusinessApplicationHeader (BAH) V01 message.

For payment messages between bank A and bank B, FROM will identify bank A and TO will identify bank B. For service messages between bank A and the MI (eg pacs.009 connected payment, liquidity messages,...), FROM will identify bank A and TO will identify the MI.

11.3.4.1.2 Schema

Outline of the schema

The BAH message is composed of the following message building blocks:

FROM

The sender that has created this message for the receiver that will process this message. FROM BIC must have exactly 11 characters.

TO

The receiver designated by the sender who will ultimately process this message. TO BIC must have exactly 11 characters.

BusinessMessageIdentifier

Identifies unambiguously the message. The BusinessMessageIdentifier has maximum 35 characters.

MessageDefinitionIdentifier

Contains the MessageIdentifier that defines the message. It must contain a MessageIdentifier published on the ISO 20022 website.

Business service (optional)

Specifies the business service agreed between the sender and the receiver under which rules this message is exchanged. To be used when there is a choice of processing services or processing service levels. Example: E&I.

CreationDate

Date and time when this message (header) was created.

CopyDuplicate (optional)

Indicates whether the message is a copy, a duplicate or a copy of a duplicate of a previously sent ISO 20022 message.

PossibleDuplicate (optional)

Is a flag indicating if the message exchanged between sender and receiver is possibly a duplicate.

Signature (optional)

Contains the digital signature of the business entity authorized to sign this message.

Related (optional)

Specifies the BAH of the message to which this message relates. It can be used when replying to a query; it can also be used when cancelling or amending.

Business rules applicable to the schema

11.3.4.1.3 The message in business context

The BAH contains information to correctly process the message payload by means that every messages exchanged between CLM and the participants respectively CLM and the other services includes such an information. The relation between BAH and message payload is exactly one to one.

The BAH includes the following main information:

- document routing (e.g. sender, receiver, information about the message)
- document identification (e.g. MessageDefinitionIdentifier, creation date, creation time)
- document processing information (e.g. sender, service, COPY, possible duplicate)

11.3.5 Payments clearing and settlement (pacs)

11.3.6 Reference data (reda)

12 Index and digital signature

12.1 Index of business rules and error codes

12.2 Index of status value and codes

12.3 Index of instruction references

12.4 Digital signature on business layer

13 Additional information for central banks

13.1 Role of central banks in CLM

13.2 Reference data for central banks

13.2.1 Specific data for central banks

13.2.2 Setup of CLM related reference data

13.3 Settlement of payments - specific functions for central banks

13.3.1 Payments linked to monetary policy operations

13.3.2 Cash withdrawals

13.4 Credit line management

13.4.1 Credit line update

13.4.1.1 Overview

13.4.1.2 Credit line update process

13.4.2 Connected payment

13.4.2.1 Overview

A connected payment is a payment initiated by a central bank system or CB operator that triggers a change in the credit line of the CLM participant and an immediate debit/credit of its account to compensate the change in its credit line. Therefor the CLM participant needs a MCA.

The processing of connected payments is not possible between the CB general cut-off for the use of standing facilities (ie 18:40) and the start of the provisioning of liquidity for the new business day (ie 19:00), as well as during the maintenance window.

A connected payment leads to the increase or decrease of the CLM participants credit line and at the same time to a corresponding debit or credit of its MCA. (**Note:** the connected payment will be processed on all or nothing basis). Connected payments are not queued and can therefore not be revoked.

13.4.2.2 Connected payment process

The following payment flow illustrates a connected payment with positive validation and settlement on the basis of a pacs.009:

Message flow

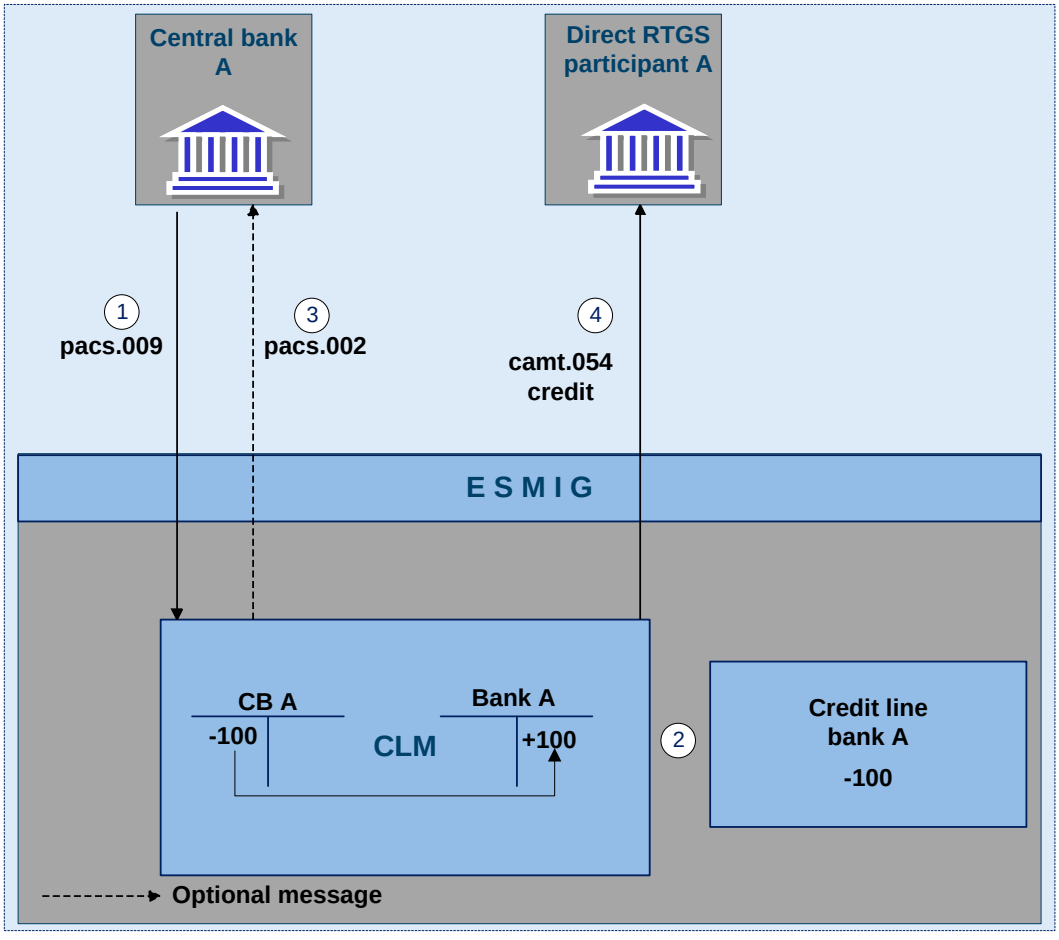


Figure 16 - pacs.009 connected payment

Process description

Step	Processing in/between	Description
1	Central bank via ESMIG to CLM	The central bank sends a pacs.009 including codeword CONPAY via ESMIG to the CLM
2	CLM	CLM check and validation positive Debit CB account and credit MCA participant A simultaneously decrease credit line for participant A (settlement amount must not be equal to credit line change) if business validation positive
3	CLM via ESMIG to central bank	Creation and forwarding of pacs.002 by the CLM (optional) via ESMIG to central bank
4	CLM via ESMIG to CLM participant	Creation and forwarding of camt.054 (credit) by the CLM via ESMIG to CLM participant A

Used messages

- pacs.009
- pacs.002
- camt.054

The following payment flow illustrates a connected payment with positive validation and settlement on the basis of a pacs.010

Message flow

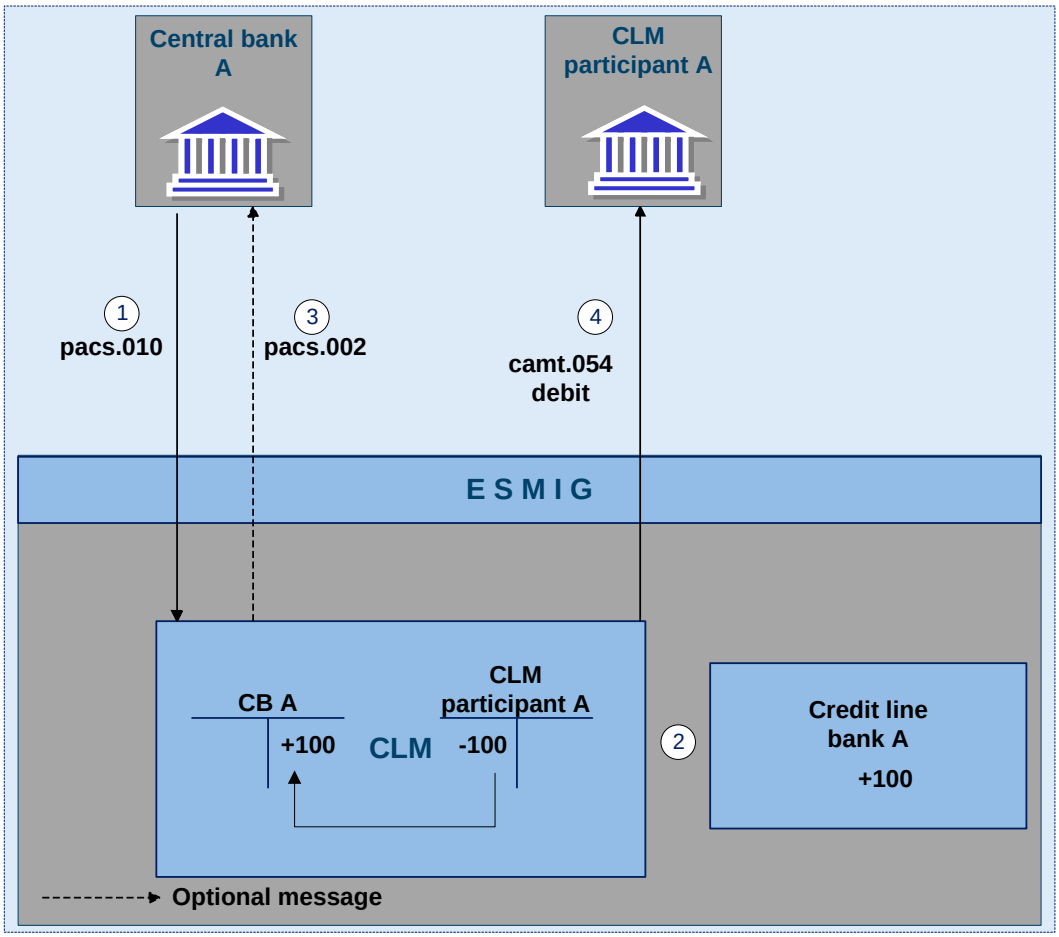


Figure 17 - pacs.010 connected payment

Process description

Step	Processing in/between	Description
1	Central bank via ESMIG to CLM	The central bank sends a pacs.010 with codeword CONPAY and the credit line change via ESMIG to the CLM
2	CLM	CLM check and validation positive Credit CB account and debit MCA participant A simultaneously increase credit line for participant A (settlement amount must not be equal to credit line change) if business validation positive
3	CLM via ESMIG to central bank	Creation and forwarding of pacs.002 by the CLM (optional) via ESMIG to central bank
4	CLM via ESMIG to CLM participant	Creation and forwarding of camt.054 (debit) by the CLM via ESMIG to CLM participant A

Used messages

- pacs.010
- pacs.002
- camt.054

13.5 End-of-day procedures

13.6 Query management - central bank specific queries

13.7 Business/liquidity monitoring for central banks

13.8 Reserve management - specific functions for central banks

13.9 Standing facilities - specific functions for central banks

13.10 Data warehouse - specific functions for central banks

13.11 Billing - specific functions for central banks

13.12 Contingency services - specific functions for central banks

13.13 Specific requirements for central banks of "out" countries

14 Glossary