HCT INST MESSAGE FLOW DESCRIPTION

BUSINESS TERMS AND CONDITIONS

ANNEX NO 25.

H-1054 Budapest, Vadász utca 31. +36 1 428 5600 +36 1 269 5458 www.giro.hu

1 Introduction

The GIROInstant (GIROInst) service continuously processes, clears and settles HCT Inst transaction[1] messages 24 hours a day and every Calendar Day of the year. In addition to the regulations detailed in the SCT Inst Scheme Rulebook[2] the HCT Inst Scheme Rulebook contains also the Hungarian specialties, the clearing and settlement processes in accordance with the related – payment – regulations.

1.1 Purpose of this document

This document presents the rules, processes, standards and practical information necessary to ensure the interoperability of interbank instant payment transactions.

Present document

- ✓ contains definitions of rules and obligations of the Scheme,
- ✓ gives reliable information on the functions of the Scheme,
- ✓ details the clearing and settlement processes.

1.2 References, related documents

ID	Title
EPC[1] rules, standards	
EPC 004-16	SEPA INSTANT CREDIT TRANSFER (SCT INST) SCHEME RULEBOOK
EPC 122-16	SEPA INSTANT CREDIT TRANSFER (SCT INST) SCHEME INTERBANK IMPLEMENTATION GUIDELINES[2]
ISO rules	
ISO 20022 pacs.002.001.03 FIToFIPaymentStatusReportV03 pacs.008.001.02FIToFICustomerCreditTransferV02 pacs.004.001.02 PaymentReturnV02 pacs.028.001.01 FIToFIStsReqV01 camt.029.001.02 ResolutionOfInvestigationV03 camt.056.001.01 FIToFIPaymentCancellationRequestV01	Financial Services – Universal Financial Industry message scheme

[1] European Payments Council / Európai Pénzügyi Tanács

[2] The ISO2002 standard provides a detailed description of the structure and use of standards to facilitate development

ID	Title
Related legislation	
MNBr.	35/2017. (XII.14.) MNB Decree
Other documents	
Guidance issued to facilitate the use of the above message standards by banks [3]	

1.3 Changes

Date	Content
1 December 2023	The value limit amount for instant credit transfer has been removed.

2 General overview

Services implemented on GIROInstant system operated by GIRO Zrt. – as system operator – are based on open standards. The processing does not need manual intervention (e.g. it is STP[5]), instantly clears and settles individual credit transfer orders.

2.1 Services provided by GIROInstant

2.1.1 Basic service

Clearing and settlement of payment transactions according to HCT Inst payment scheme

Clearing and settlement is

a) pre funded
b) continuous (every day of the year),
c) real time,
d) credit transfer,
e) This is done against the individual balances of clearing members' instant settlement accounts, in addition to the collateral held in the central account held by the MNB.

2.1.2 Addictional functions

Secondary account identifiers

[3] HCT Inst Message Implementation Guideline, which is made available by GIRO Zrt. on its website, subject to registration, at the time of entry into force of these Rules..

Information on the handling and processing of secondary account identifiers can be found in a separate Annex 26. Clients of Clearing Members may also initiate an instant transfer transaction with a secondary account identifier, but Clearing Members must always submit the instant transfer message to GIROInstant with the IBAN format account number and the corresponding bank identifier.

Request to pay

Information on the Payment Request Service can be found in a separate Annex 27.

2.2 Specifics of processing according to the HCT Inst Scheme

2.2.1 The type of transaction can be:

The original transaction (pacs.008) or all other transactions after the processing of the original transaction (pacs.002, pacs.004. camt.056, camt.029, pacs.028).

the message identifier determines the type and whether it involves a transaction or contains a notification:

- ✓ pacs.nnn - a transaction that modifies the balance of the Clearing Members' instant settlement account, or confirms the result of processing, or notifies the balance modification of the instant settlement account (payment clearing and settlement),
- ✓ camt.nnn - notification not to modify the balance of Clearing Members (cash management))

Additional information needs to be provided in case of post-transfer

- ✓ reference to the antecedent credit transfer instruction,
- ✓ reason for transfer initiation,
  - Missing final status report (Initiating Clearing Member)
  - Beneficiary Direct participant's confirmation regarding the transfer's
    - fulfillment, the availability of the transferred amount (immediate or at a later time) for the beneficiary (ACSP or ACWC),
    rejection (RJCT and the reason for rejection),
  - The Initiating Clearing Member's or the account holder's reason for recalling the transfer,
  - Response of the Beneficiary Clearing Member to the Recall
    - fulfillment and the return of fund,
    - rejection of recall and the reason for rejectionl.

The GIROInstant service

- ✓ check
  - The uniqueness of the transaction message and batch identifier within a message type,
    - the validity of the reason code in the:

- in recalls and responses to recalls,
- Positive confirmation by the Beneficiary Clearing Member (ACSP or ACWC).

In the event of an invalid reason or an incorrect status report by the Beneficiary Clearing Member, the processing of the transaction concerned will be stopped

- invalid reason code (HU76) in case of recall and recall-answer
- an incorrect status report with an error code "Timeout expired" (in the final status report);

✓ <u>does not check the</u>

- validity of the year (except in Acceptance Date and Time),
- relation of BIC and bank organization code in IBAN (according to Verification Table),
- validity of bank organization code (according to Verification Table),
- structure of Hungarian BBAN in IBAN,
- The reason code in the negative feedback given by the Beneficiary Clearing Member for the transfer. The Beneficiary Clearing Member may use the rejection codes as agreed between banks and/or as provided in the list of codes available on the ISO 20022 website, which are not used by GIROInstant,,
- The accuracy of the original transfer data referenced in the recall and recall responses, and does not match the content of the data in such transactions with the original transfer data referenced. It is the obligation of the Clearing Member submitting a recall and recall response transaction to accurately reference in such transaction all data in the original message as required by the Standard.

The table below shows the transaction types and identifiers, the initiating / sending party and some of the codes from the code list available on the ISO 20022 website

type	id	initiator / sender	feedback / reason
Payment	pacs.008	Debtor agent	
status report positive response	pacs.002	Beneficiary Party Clearing Member	transferred amount is available for the client - immediately: ACSP - at a later time: ACWC
status report negative response (rejection)	pacs.002	Beneficiary Party Clearing Member	Payment is rejected: RJCT, because the beneficiary's - account is invalid: AC03 - account is blocked: AC06 - account is closed: AC07 - account cannot accept this type of transaction: AG03 - deceased: MD07
recall	camt.056	Payer	- duplicated message: DUPL - technical problem: TECH - suspected fraud: FRAD
		Payer Party Clearing member	- recall initiated by customer: CUST

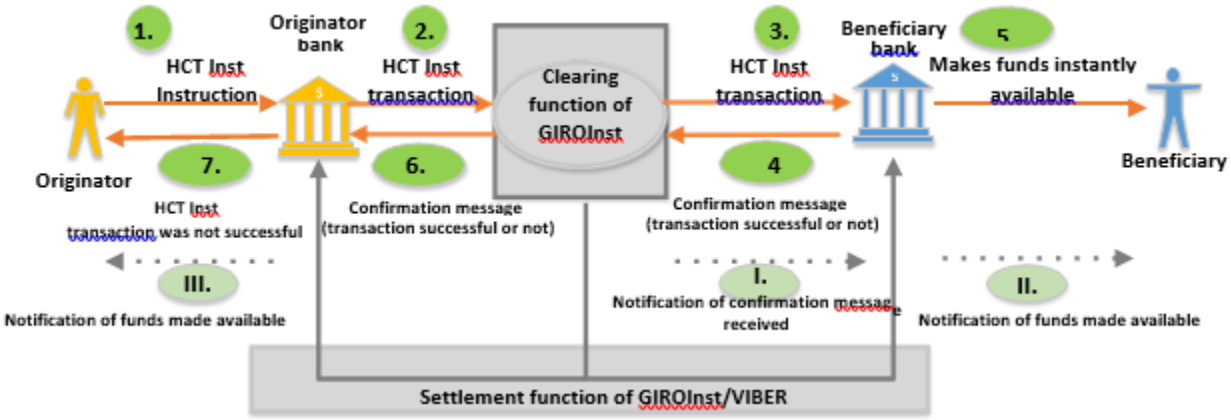
type	id	initiator / sender	feedback / reason
			- invalid amount: AM09 - incorrect IBAN: AC03
recall fulfillment, return of funds	pacs.004	Beneficiary Party Clearing Member	- return of funds after recall: FOCR (Following Cancellation Request)
rejection of recall	camt.029	Beneficiary Party Clearing Member	recall request rejected: RJCR, because - beneficiary customer rejected the repayment: CUST - legal requirement: LEGL - recalled funds have already been returned: ARDT - account closed: AC04 - lack of funds: AM04 - no response from customer regarding recall request: NOAS no transfer arrived referred in the recall request: NOOR
investigation message	pacs.028	Paying Party Clearing Member	a GIROInstant - resend the final status report, or - indicates that the transfer referred to has not been received: NOOR
final status report the transfer process has been completed	pacs.002	GIROInstant platform	*Error / unable to process / not forwarded transfer*: RJCT - Lack of obligated clearing member cover - nem egyedi azonosító: AM05 - érvénytelen devizanem: CURR - érvénytelen összeg: AM01 / AM12 (fillér > 0) - túl késői küldés (az időpecséthez képest): AB06 - érvénytelen időpecsét: DT01 Notes: this table gives only some of the reasons for refusal as examples. Detailed control conditions and reasons for refusal are given in ISO 20022.
			an error-free transfer forwarded to the Beneficiary - in the event of a reply from the Beneficiary's Clearing Member within the time limit - if the reply is correct and intelligible, the feedback code sent by the Beneficiary's Clearing Member - if the reply is unintelligible, the reason: deadline expired AB05 (Paying Party Clearing Member) TM01 (Beneficiary's Clearing Member) - Response by the Clearing Member of the Beneficiary after the deadline (in case of a reply from the beneficiary) processing of transfer due to expiry of the deadline has been completed: AB05 (Payee's Clearing Member)

type	id	initiator / sender	feedback / reason
			TM01 (Clearing Member of the Beneficiary) Note: both parties concerned, i.e. the Paying Party and the Clearing Member of the Beneficiary, will receive the message.)
responsefor uninterpretable messages	-	GIROInstant platform	the message sender is notified in a SOAP message, in case of not processable messages, where the message body only contains „invalid <message type>" for example in the following cases: - wrong format (XSD), - invalid characters, ived from unauthorised endpoint

3 Flow charts

The following section presents an overview of the message flows describing the logic behind the individual steps as well as their roles in clearing and settlement.

Figure 1 - HCT Inst processing - Logical flowchart of a successful message flow



1. The Originator Bank receives an instant payment instruction from the Originator. The payer carries out the necessary steps to prepare for the execution of the instant payment: following receipt of the transaction and user's authentication it generates the timestamp, validates the instruction and reserves the amount on the client's account. As a final step it creates the HCT Inst transaction.

2. The Paying Party Clearing Member will transmit the instant transfer to GIROInstant. Authorizes GIROInstant to block the amount necessary to complete the instant transfer in the Paying Party Clearing Member's Instant Settlement Account, thereby ensuring settlement and executionn. GIROInstant shall block the funds for the instant transfer in the Paying Party's Clearing Member's instant settlement account with GIROInstant in preparation for settlement and execution.

3. GIROInstant will transmit the instant transfer message to the Clearing Member of the Beneficiary's party. The Clearing Member of the Beneficiary Party may be assured that, on the basis of the blocking of the Clearing Member of the Paying Party's Instant Settlement Account, the Instant Transfer transmitted to it will be cleared and settled, if accepted. The Clearing Member of the Beneficiary Party shall promptly verify that the amount of the instant transfer can be made available to the Beneficiary Party

4. The Beneficiary's Party Clearing Member will inform GIROInstant that

   ✓ Received the instant transfer,

   ✓ is able to instantly process the HCT Inst transaction (positive confirmation)

5. The GIROInstant platform will execute the settlement on the instant settlement accounts; debit the Paying Party's Clearing Member (by decreasing the balance of the Paying Party's Clearing Member's GIRO Instant Instant Settlement Account with the blocked amount) and credit the Beneficiary's Clearing Member (by increasing the balance of the Beneficiary's Clearing Member's GIROInstant Instant Settlement Account with the amount of the transfer), and notify both the Paying Party and the Beneficiary's Clearing Member of the settlement..

6. The debtor agent

   - debits its debtor’s account (by the amount reserved in step 1)
   - notifies the debtor - according to the service contract between the bank and the debtor – that the transferred amount has been made available to the beneficiary. The notification itself and the time needed for it is not part of the scheme.

   The Beneficiary clearing member

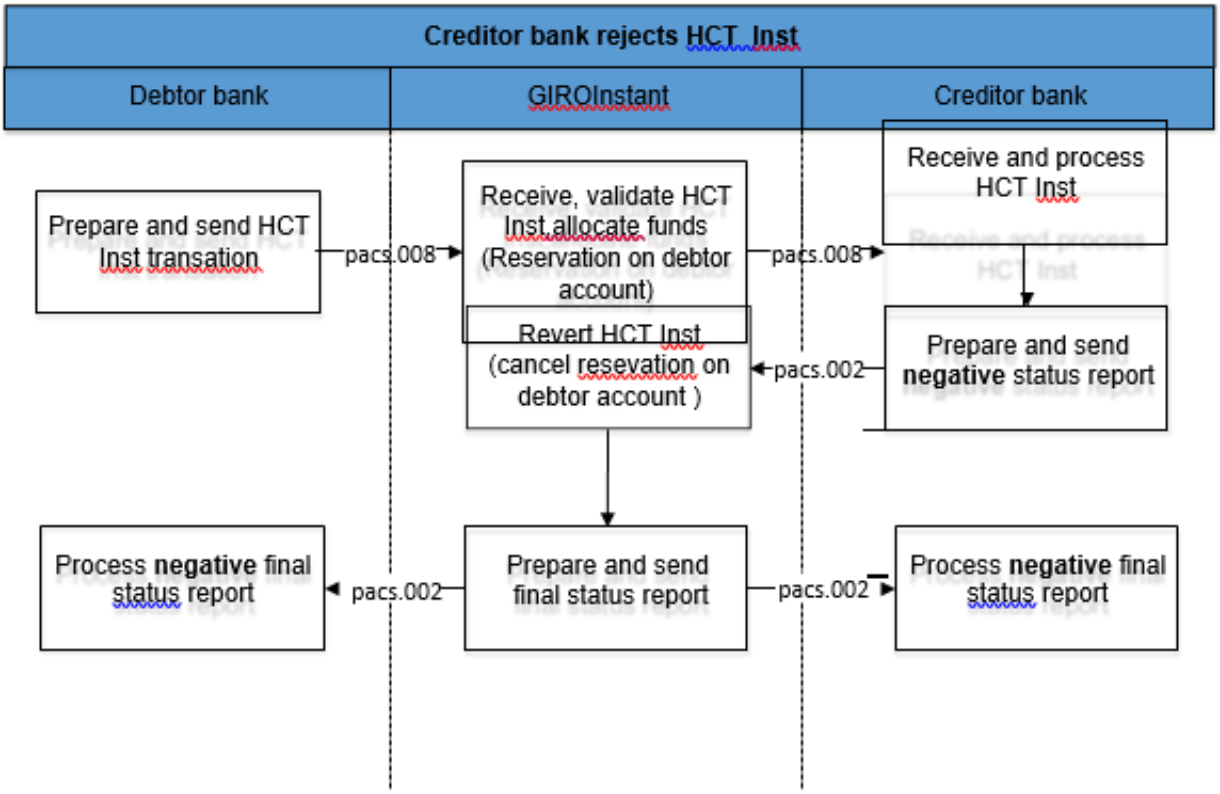
   - After receiving the positive response from GIROInstant in Step 4, the Beneficiary will receive the notification of completion in the form of a final status report and will instantly make the amount of the instant transfer available to the Beneficiary.
   - Notifies the Beneficiary of the availability of the amount in accordance with the provisions of the Framework Agreement between the Beneficiary and the Clearing Member. The notification itself and the time spent on it are not part of the scheme.

3.1 The process of an accepted, settled instant transaction

The scheme applies the following principles which are to be respected by all scheme participants:

1. If the GIROInstant platform forwards an instant transfer to the Clearing Member of the Beneficiary Party, the Clearing Member of the Beneficiary Party has no credit risk towards the Clearing Member of the Paying Party for the amount of the transaction. This settlement certainty is ensured by the GIROInstant platform's collateral lock

2. When the Clearing Member of the Paying Party transmits an instant transfer message to the GIROInstant platform, the Clearing Member of the Paying Party also authorises the



GIROInstant platform to block the amount of the transaction in the Clearing Member's instant settlement account in GIROInstant, thereby creating the necessary funds for the settlement and completion of the instant transfer.

3. It is the responsibility of the Beneficiary Clearing Member to confirm the acceptance or rejection of the instant transfer transaction to the Paying Party Clearing Member.

4. The Paying Party's Clearing Member will complete the transaction on the basis of this final status report sent by the GIROInstant platform to the Beneficiary's Clearing Member, that is, it will debit the Paying Party's account in case of a positive status report and unblock the amount from the Paying Party's account in case of a negative status report.

Figure 2 - Successfully processed instant transfer and status report

The GIROInstant platform receives the instant transfer, carries out the necessary formal and content checks, followed by the verification of the funds and then blocks the amount of the instant transfer in the debtor agent instant settlement account. It will then forward the instant transfer transaction to the creditor agent. If the Creditor agent confirms the creditworthiness of the transaction in the form

of a positive status report, the GIROInstant platform shall finalise the transaction by debiting the Instant Settlement Account of the creditor agent crediting the Instant Settlement Account of the Beneficiary Party, thus settling the transaction between the Clearing Members.

3.2 GIROInstant rejects the instant credit transfer transaction

The GIROInstant platform will reject an instant transfer transaction if it is not appropriate based on the content check or if it is not possible to block an amount in the debtor agent instant settlement account sufficient to execute the instant transfer (insufficient funds).

In this case, a negative final status report will be sent to the debtor agent with the corresponding error code and the amount will not be blocked in the account of the Debtor Agent.

Based on the XSD validation, messages containing inappropriate or invalid characters will only receive a SOAP response from the platform indicating that they are incorrect

Figure 3 - Instant transfers rejected by the GIROInstant platform

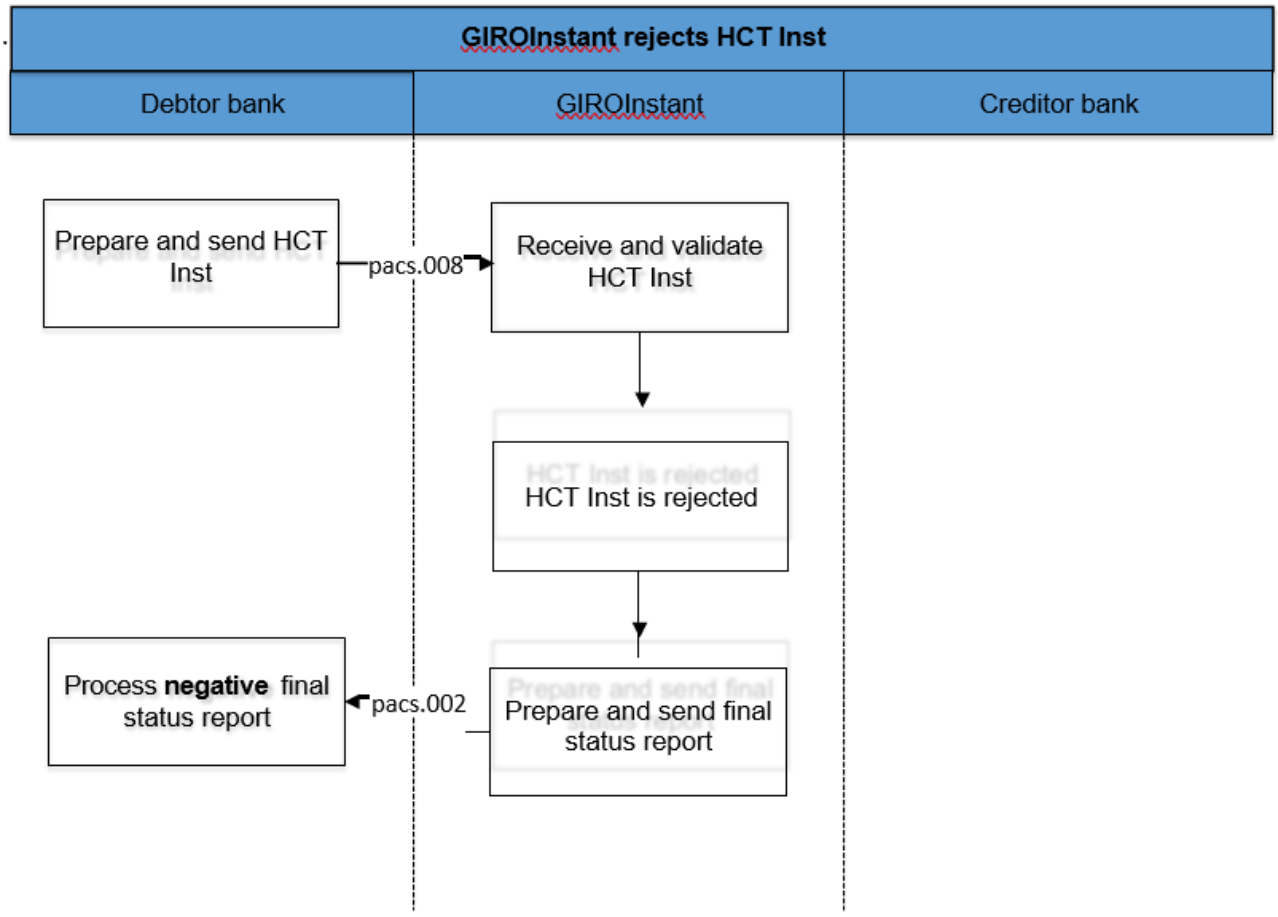
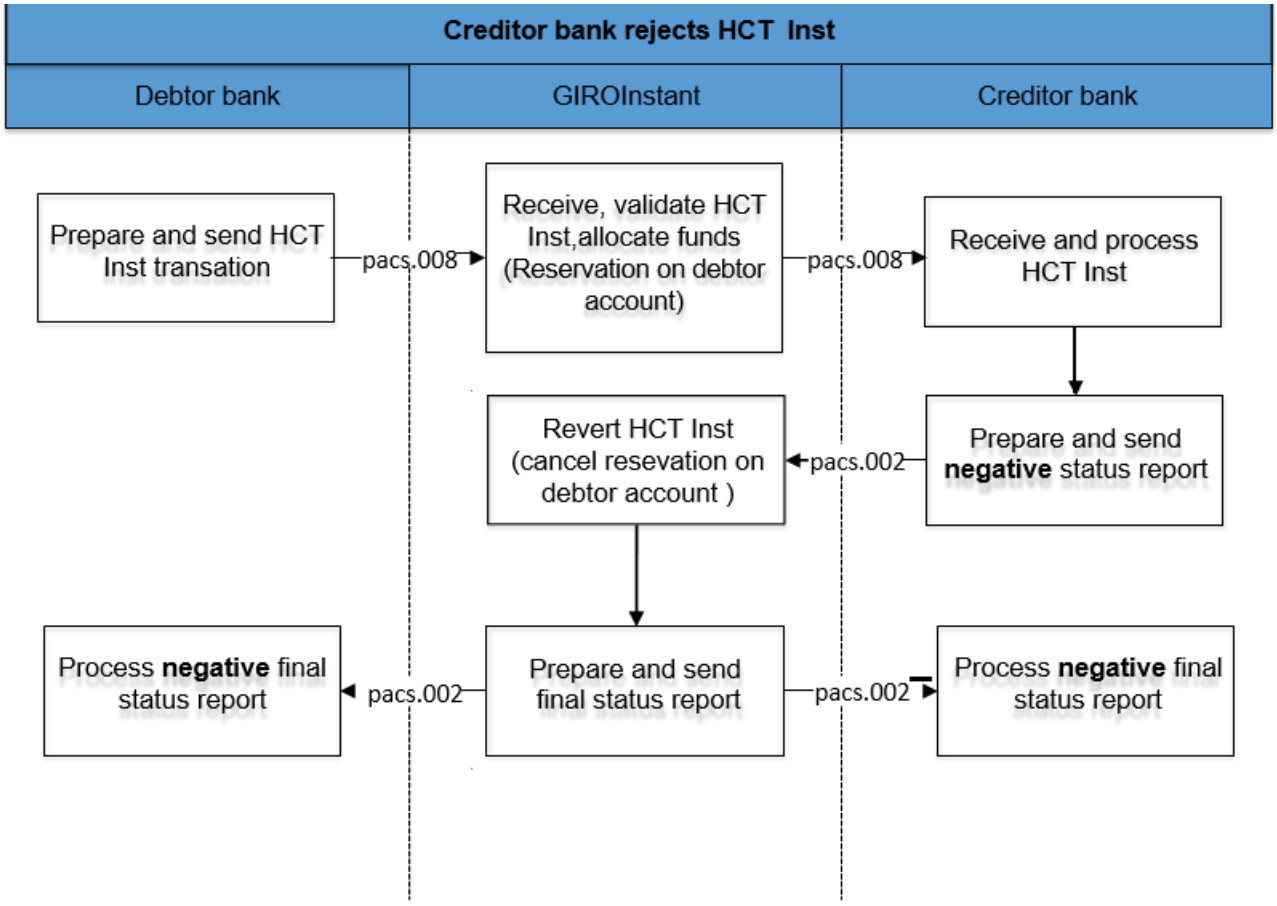


Figure 3. – Instant payment transaction rejected by GIROInstant

3.3 The Beneficiary Clearing Member rejects an instant credit transfer

The Clearing Member of the Beneficiary Party may refuse an instant transfer for both formal and substantive reasons, such as if the account number of the Beneficiary Party is unknown. In such a case, the Beneficiary shall report back to the GIROInstant platform in the form of a negative status report, indicating the relevant error code of the reason for the rejection. The processing of the instant transfer shall end when the GIROInstant platform notifies both the Paying Party and the Clearing Member of the Beneficiary of the failure of the instant transfer in the form of a final status report and unblocks the amount of the instant transfer in the Clearing Member's instant settlement account of the Paying Party.

Figure 1 - Rejection of an instant transfer by a Clearing Member of a Beneficiary Party



3.4 The Beneficiary Party's Clearing Member resends the status report

If the Beneficiary Bank does not receive a final status report from the GIROInstant platform within the timeout limit, then the Beneficiary Bank may resend the original pacs.002 positive or negative status report to GIROInstant.

The response from the GIROInstant platform will be re-sent in the form of a positive or negative final status report, depending on the final status of the instant transfer. The Clearing Member of the Beneficiary Party may replay the message up to 5 times within 24 hours of the processing of the transaction, using the original data used in the original message (message and transaction ID and content).

The final status of an instant transfer will always be communicated by the GIROInstant platform to the Clearing Members involved in the transaction, in the form of a final status report, which cannot be overridden by the Clearing Members..

GIRO Zrt., the operator of the GIROInstant platform, can investigate the status of the transaction at any time without resubmitting the transaction through the GIROInstant Operator Portal - hereinafter referred to as the Operator Portal - and by analysing the reports. The investigation by GIRO Zrt. must be initiated by the Clearing Members.

Figure 2 – The Beneficiary party's clearing member resubmits the status report

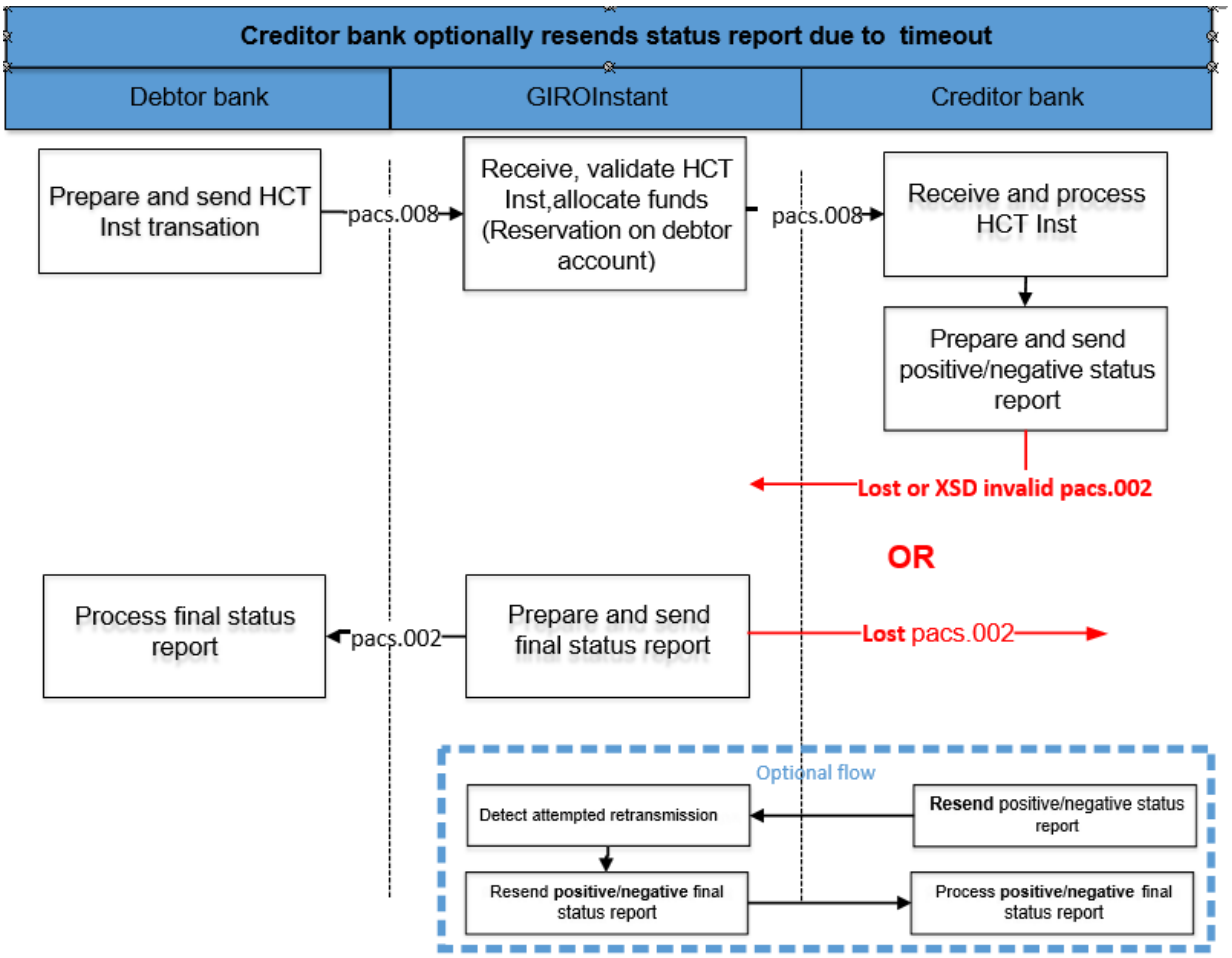


Figure 5. – Optional resending by the Beneficiary Bank

3.5 The Beneficiary Clearing Member receives a status report with no previous history

There may be a case where the Beneficiary's Clearing Member did not receive or was unable to process the forwarded instant transfer and did not send a status report. In such a case, GIROInstant will reject the transaction due to timeout and send a final status report to both Clearing Members involved in the instant transfer.

3.6 The Debtor Agent resends the transfer

The way messages are exchanged between GIROInstant and the Clearing Member and the technical success characteristics of message exchanges are described in the Technical Connection Guide and the WSDL Implementation Guide referenced therein. In the event of a message delivery failure due to technical reasons, the Debtor Agent may resend the original instant transfer (pacs.008) once.

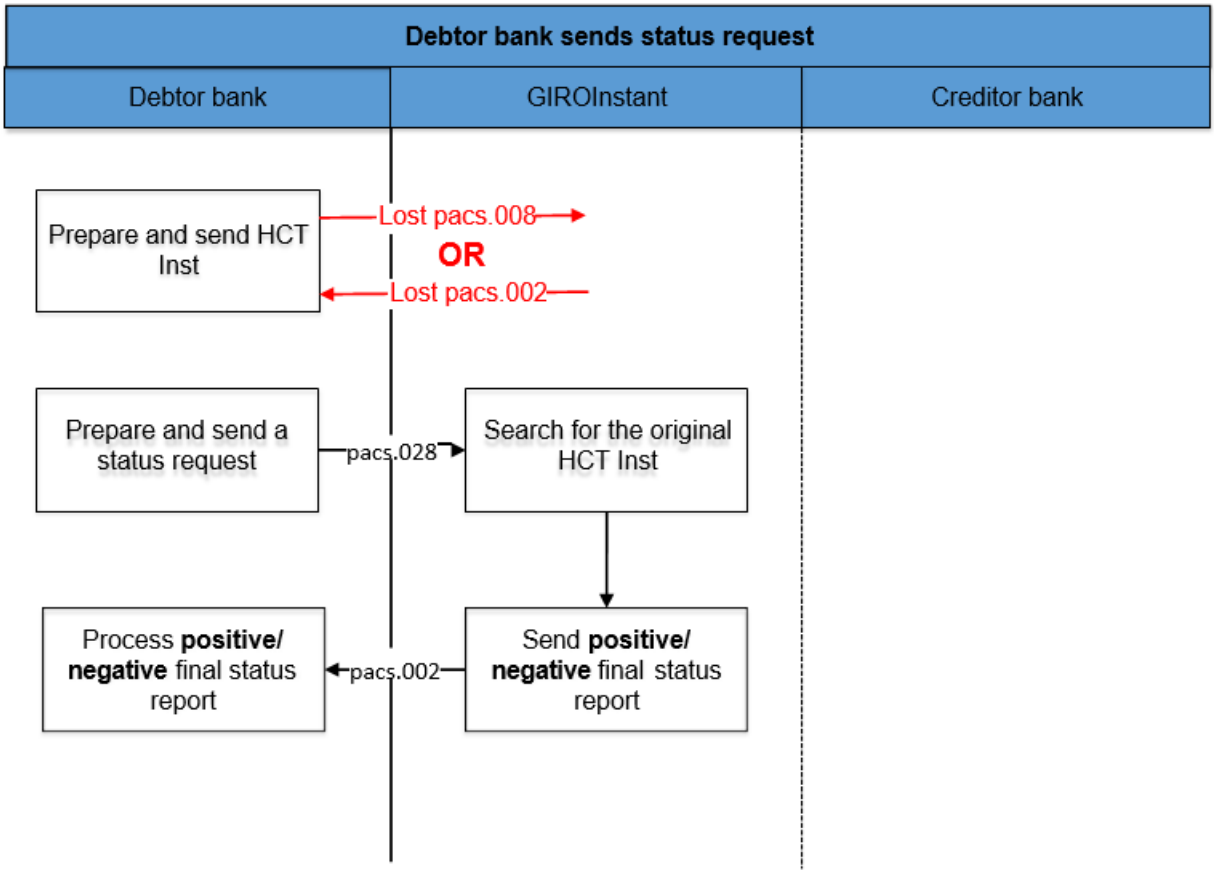
3.7 The Debtor Agent sends an investigation message

If the Debtor Agent has not received a final status report after the timeout, it may use the standard investigation process (send message pacs.028) to clarify the status of the instant transfer. If GIROInstant finds the instant transfer referred to in the investigation message (pacs.028), it will resend the corresponding final status report. If not found, the GIROInstant platform sends a negative final status report to the Debtor Agent.

Sending an investigation message to the Debtor Agent is only allowed after a timeout and may be repeated up to 5 times within 24 hours after the instant transfer has been sent.

GIRO Zrt. may investigate the status of an instant transfer at any time without resubmission through the Operator Portal or by analysing the reports, such type of investigation must be requested by the Clearing Member from GIRO Zrt.

Figure 3. – The Debtor Agent sends an investigation message after the timeout



3.8 Incorrect status report from the Creditor Agent

Non-interpretable status reports from a Credtior Agent will not be processed further. This includes status reports received via unknown/not yet defined communication channels, status reports stuck in a security check, and status reports that cannot be matched with a previous instant transfer. The above cases require manual investigation.

For messages containing incorrect or invalid characters based on XSD validation, the GIROInstant platform will only return a SOAP response message indicating the incorrectness and the transaction will fail due to timeout, which GIROInstant will notify both Clearing Members in a final status report.

3.9 The Debtor Agent sends recall which is accepted by the Beneficiary's Clearing member

After the final status report has been sent by the GIROInstant platform, the instant transfer is considered final. An instant transfer is called a recall if the Debtor Agent wishes to recall a previous transaction. A recall can therefore only be initiated by a Debtor Agent who wishes to recall a previous instant transfer that has already been executed, either at the request of the Debtor or at his own discretion.

The Paying Party Clearing Member may initiate a recall for the following reasons:

- ✓ duplication (error code: DUPL)
- ✓ an incorrect instant transfer caused by a technical problem (error code: TECH)
- ✓ The instant transfer is fraudulent (error code: FRAD).

The Debtor Agent has 30 days to respond to an instant transfer recall initiated by the Creditor Agent within 30 days of the transfer..

The Debtor Agent may initiate a recall at the request of the Debtor for the following reasons (recall initiated by the Debtor):

- ✓ debtor transferred the wrong amount (error code: AM09)
- ✓ debtor specified wrong account to credit (error code: AC03)
- ✓ other reason, not specified by debtor (error code:CUST)

A recall initiated by the Debtor agentat the request of the Debtor may be sent up to the last day of the 13th month after the original instant transfer, which shall also have a 30-day response period.

The GIROInstant platform does not monitor the compliance with the deadline, does not check the date of the instant transfer / callback / callback response.

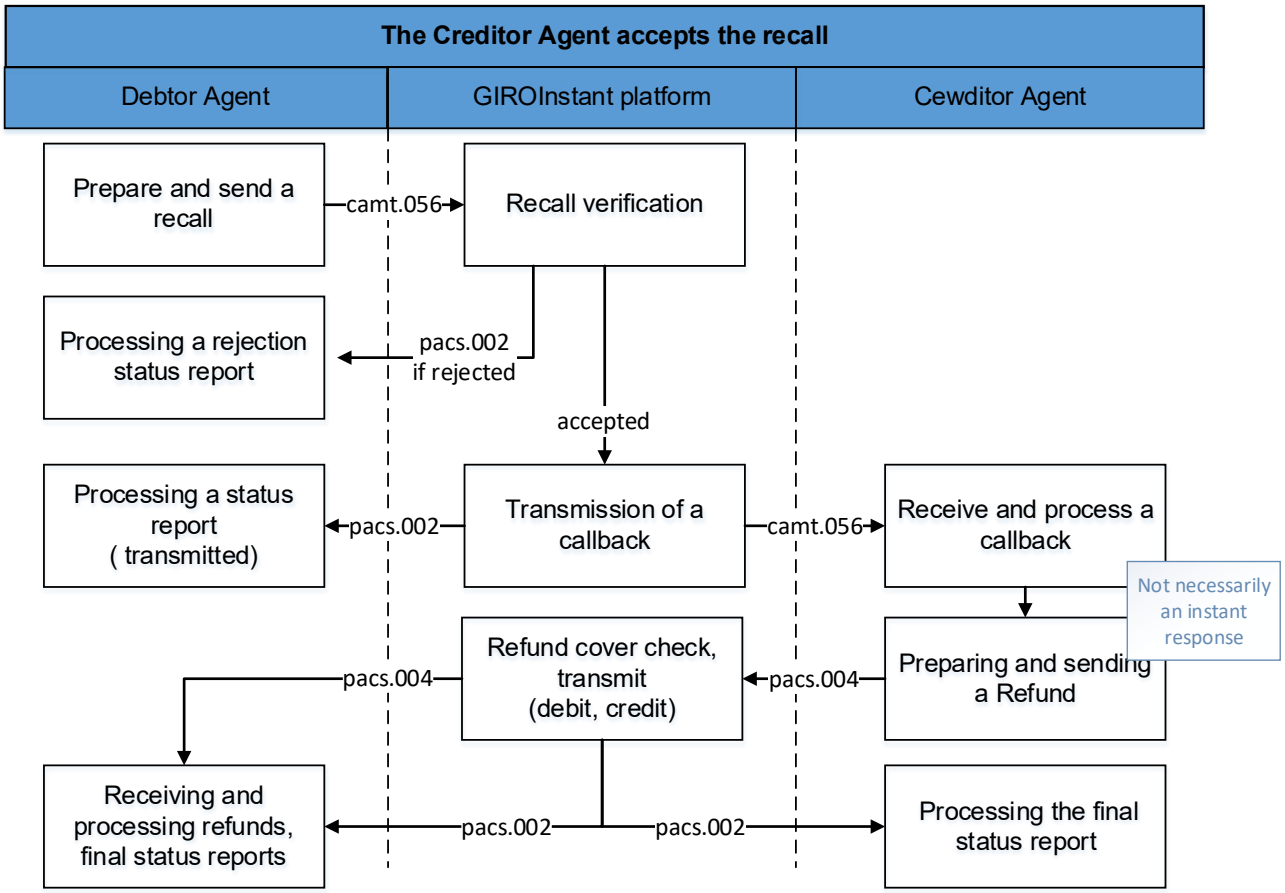
The Debtor Gent sends a callback in the form of a camt.056 callback message to the GIROInstant platform. GIROInstant validates the message and forwards it to the Creditor Agent. No margin calls or liquidity movements are made in this step.

The Debtor Gent will decide, within a specified period of time (30 days), in consultation with the creditor, if necessary, whether to approve or reject the recall.

If the Creditor Agent accepts the callback, it will reply to the callback with a message of type pacs.004. The chargeback is immediately processed by the GIROInstant platform, the Clearing Member sending the message is debited, the Clearing Member receiving the message is credited and the message is forwarded to the Debtor Agent of the instant transfer.

Both the Debtor and the Creditor Agent will receive a final status report from the GIROInstant platform on the positive result of the refund.

Figure 7 The Creditor Agent accepts the recall



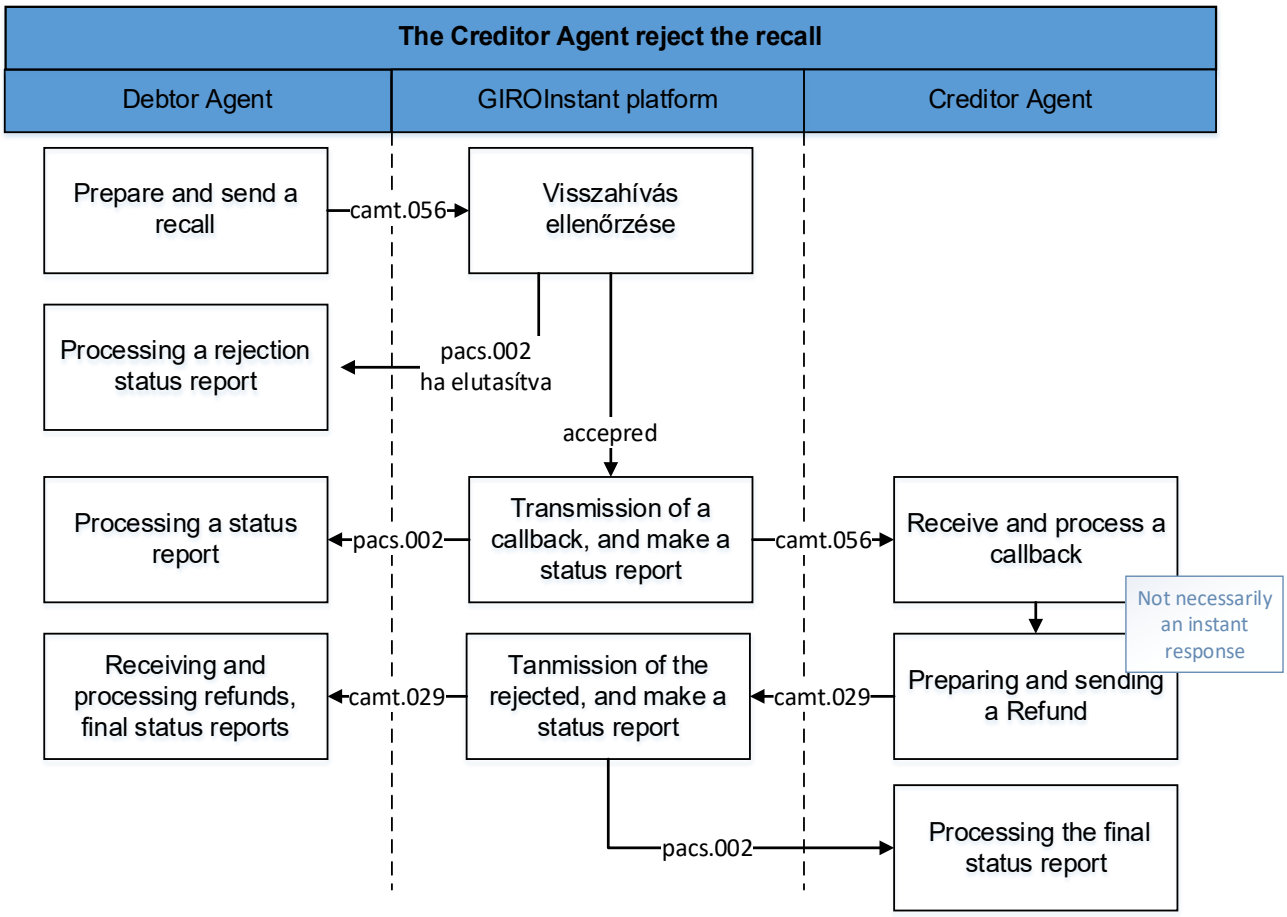
.....

3.10 The Debtor agent sends recall which is rejected by the Creditor Agent

If the Creditor Agent rejects the callback, it will respond to the callback with a Callback Rejection camt.029. After validation, the GIROInstant platform forwards the rejection response to the Debtor Agent for processing.

A positive or negative status report will be sent to the Clearing Member of the Beneficiary's Party for the rejection of the recall, depending on the validation of the GIROInstant. The status report will be sent in the form pacs.002 and the formally unintelligible file (XSD or character set error) will be answered by the GIROInstant platform with a SOAP message.

Figure 8 The Creditor Agent rejct the recall



4 Hungarian specialities

This section contains the deviations from the SCT_Inst scheme and the ISO20022 standard due to Hungarian specialities.

CHARACTER SET

Only Hungarian accented characters (in the "extended" ASCII range above 128) may be used in the text type fields of the HCT Inst message (if they are not identifiers), except for all the basic UTF-8 characters (in the range 32-127).

CURRENCY

The currency of HCT Inst transactions may only be Hungarian Forint (HUF).

SUMMARY

HCT Inst messages can contain amounts larger than the legally prescribed limit because the participants can agree (bilaterally or multilaterally) to process larger amounts. GIROInstant does not check the value of amount to be transferred. The fractions of the amount contained in the message (if forwarded) must be 00.

GIRO Zrt. will publish the identifiers of the Clearing Members who have declared that they send and/or receive transfers in GIROInstant in amounts other than the limit set by law.

TIME LIMIT FOR UNIQUENESS

Message IDs must be specific within the same message type for 7 calendar days. The duration is not defined in the SCT Inst schema.

If the identifier is not unique within the message type, the transaction is rejected by the platform.

ERROR CODES

If a HCT Inst instruction is rejected due to a reason not specified in the ISO20022 code list, the reason for rejection may be specified with a Hungarian - HU*nn* – error code. he full current list of error codes is published by GIRO for Clearing Members.

RECALL AND REPLIES

While SCT Inst defines a max. 10-day timeframe for recalling instructions, HCT Inst allows Debtor Agent 30 days (after instant payment) to recall a message. Reasons for the recall may be: technical error,

duplication, possible fraud/money laundering, etc. Creditor Agent also has 30 days at their disposal to reply to the recall (SCT Inst allows for 10 days only

ACCURACY OF TIMING

The time stamp indicating the start of the execution time shall be given to the nearest millisecond.
The time stamp must be entered with the time at which "the Dbtor Agent has received the instant transfer order and the authentication has been completed", in accordance with the relevant MNB Regulation.
If the Debtor authentication has already taken place prior to the initiation of the transfer transaction, the time stamp shall indicate the receipt of the transfer transaction by the Payer's payment service provider.

If the Debtor authentication has not been completed prior to the initiation of the transfer transaction, the Debtor Agent shall prepare and place the time stamp for the instant transfer after the customer authentication.

In the event of a dispute between the Clearing Member and GIRO Bank over the interpretation of the time stamp due to a different time synchronisation, the time known to GIROInstant shall be deemed to be the relevant time.

PROXY IDENTIFIER

The instant transfer shall indicate that the Debtor or, in the case of a payment request, the Beneficiary Party has given the order by providing proxy identifier, which the Clearing Member shall include in the instant transfer or the Service Provider shall include in the payment requestl.

A proxy identifier can only be included in an instant transfer if :

- the Instant Credit Transfer has no history of a payment request and the Instant Credit Transfer order was initiated by the Paying Party by entering the Beneficiary's secondary identifier,
- the instant credit transfer is related to the approval of a payment request and the payment request order was initiated by the Beneficiary by entering the Paying Party's secondary account number.

AN INSTANT TRANSFER IN CONNECTION WITH A PAYMENT REQUEST

In an instant transfer that fulfils a payment request, two fields carry the information that clearly indicates that the instant transfer is related to a payment request.

- EndToEndIdentification field of credit transfer must contain the value of RtP instruction’s EndToEndIdentification field thus guaranteeing the relation of the two transactions. (See Hungarian Guideline (”RTP-REF” Hungarian rule)
- PaymentIdentification / InstructionIdentification field of credit transfer must indicat

among others – that the credit transfer fulfills a RtP instruction. (See Hungarian Guideline "RTP-REF")

The following Hungarian rules make it possible that information present in RtP instruction is also present and extended in credit transfer (mainly in the above mentioned InstructionIdentification field):

- "RTP-MOD" possibility to modify the requested amount
- "RTP-PART" sequence number of instalment in case of modifiable amount
- "RTP-LAST" last payment in case of modifiable amount
- "RTP-AMT" original amount of RtP instruction (in InstructedAmount field of credit transfer)

FEE-PAYER IN THE INSTRUCTIONS

In the instant transfer it is possible, but not mandatory, to indicate which Clearing Member is the payer of the GIROInstant fee (FEE-PAYER): theDebtor Agent (DEBT), or the Creditor Agent(CRED), or the Clearing Members participating in the instant transfer shared (SHAR).

The fees of GIRO Zrt. are set out in the Interbank Clearing System Fee Regulation. The tariffs do not currently use this field for the calculation of fees.

To be noted
FEE-PAYER, RTP-IND, RTP-MOD, RTP-PART, RTP-LAST and H-SWIFT must be shown in the same PaymentIdentification/InstructionIdentification field (see in HCT_Inst Message Implementation Guidelines) as follows]

Examples for indicating the fee payer and/or the additional data if the credit transfer is an answer to a request to pay:

1. SHAR (shared pay costs)
7. CRED-R-M3 (costs are paid by the Beneficiary, the credit transfer fulfills a RtP instruction with modifiable amount, the current payment is the 3rd instalment)
8. DEBT-R-M (costs are paid by the Debtor, the credit transfer fulfills a RtP instruction with modifiable amount)
9. -R (the credit transfer fulfills a RtP instruction)
10. -R-M2F (the Instant transfer fulfills a RtP instruction with modifiable amount, the current payment is the 2nd and at the same time the last instalment)
11. CRED-R-M15F (costs are paid by the Beneficiary, the credit transfer fulfills a RtP instruction with modifiable amount, the current payment is the 15th and at the same time the last instalment).

TYPE OF THE PAYMENT SITUATION

In the instant transfer, a standard ISO 20022 code can be used to indicate the type of payment status of the instant transfer in the Purpose field of the message, e.g. physical purchase, online purchase, bill payment, P2P money transfer, etc. (The full list of codes is available on the ISO website)).

The instant transfer linked to the payment request must include the payment status code of the payment request. In order to avoid any confusion, the group transfer reference codes should not be used in the instant transfer.

INDICATION OF SWIFT TRANSFER

In the HCT_INST (pacs.008) instant transfer, it is possible to indicate the identifier of the transfer initiated by SWIFT message (H-SWIFT flag, value: -S<transaction identifier>)

DISPLAY DATA OF MEDIUM

The transfer (in the Regulatory Reporting block), the code of the type of data medium must be indicated (H-DATA/1) and its identifier (H-DATA/2) as follows:

code	description
CustomerID	Customer identifier (at bill payment)
CredTranID	Beneficiary's internal transaction identifier
InvoiceID	Identifier of bill or invoice
LoyaltyID	Identifier of regular customer of discount system
MerchDevID	Identifier of commercial device (cash register, POS)
NAVCheckID	National Tax and Customs Office's Verification code
ShopID	Identifier of commercial unit, store

CLEARING MEMBERS NOT SENDING A TRANSFER

Some Clearing Members are only able to receive (pacs.008) instant transfers and send (pacs.002) status reports confirming the completeness of the received instant transfer. The time limit and timeout also apply to these Clearing Members, and they must therefore immediately send a positive or negative status report on the acceptance or rejection of the transfer transaction for all their instant transfers, as required by the MNB Regulation, 24 hours a day, 7 days a year.

The process for processing withdrawals of instant transfers sent to Klíring members who are only connected on the receiving side is different from the general process. All recalls (camt.056) will be answered by a rejection of the recall (camt.029) by Clearing Members connected only on the receiving side, respecting the execution times. If the recall is executed by the Clearing Member of the Beneficiary Party receiving the instant transfer only, the recalled amount will be returned by InterGIRO2 (hereinafter referred to as IG2) to the Clearing Member of the Paying Party of the original instant transfer by means of an intraday settlement (pacs.008). After the successful completion of the IG2 transfer, the Clearing Member receiving the instant transfer only shall send a recall rejection in the

appropriate format (camt.029) to the initiating Clearing Member via the GIROInstant platform, informing it that the amount requested in camt.056 has already been transferred in whole or in part in IG2.

In the case of a non-standard recall completion, GIROInstant and IG2 transactions cross-reference each other by structured completion of their unstructured message.

Structured filling: references are listed in the predefined order between predefined separators.

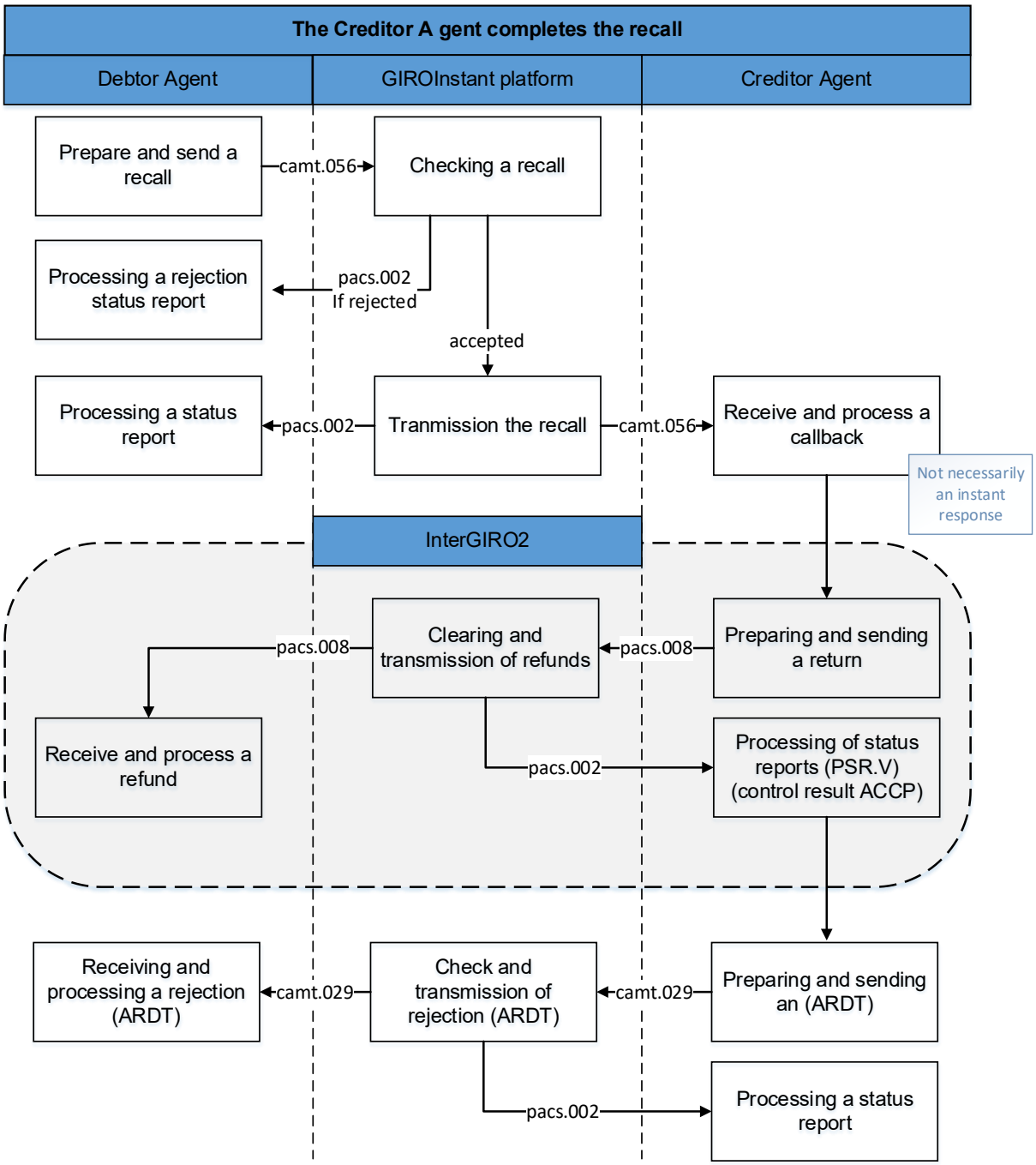
GIRO Zrt. publishes the identifiers of the Clearing Members who do not send transfers in GIROInstant, but only receive them.

A NON-STANDARD "RECALL - RECALL RESPONSES" PROCESS

The processing flow of the "transfer - recall - recall-response" from the point of view of the Creditor Agent

1. receive an instant transfer (pacs.008) in GIROInstant
   - mandatory reply: send pacs.002,
   - Receiving and processing the final status report (FSR, pacs.002) sent by GIRO Zrt;
2. receive and process a recall (camt.056) in GIROInstant;
3. transfer the recalled amount (send transaction pacs.008) in IG2-
4. rejection of the recall (sending transaction camt.029 with ARDT reason) in GIROInstant.

4. ábra – Visszahívás-visszahívás válaszok – szabványostól eltérő – folyamata



CROSS-REFERENCES

Cross-referencing facilitates reconciliation, the putting together and pairing of the transactions concerned.

In transactions, the date is in ISODateTime format (yyyy-hh-nn), in cross-references the format without hyphens (yyyy-hhnn) is used.

The fields storing the referenced data are reported according to ISO20022 pacs.008 transfer and camt.029 reject recall.

COMPLETION OF A RECALL IN IG2

In the unstructured message (CdtTrfTxInf/RmtInf/Unstrd) of the remittance transfer (code pacs.008), reference to GIROInstant transactions should be made as follows.

- ✓ # (constant) marking – GIROInstant cross-references start
- ✓ GIROInstant (constans)
- ✓ # (separator)
- ✓ GIROInstant (pacs.008) azonnali Transfer Paying party's bank 8/11 character BIC code

(*CreditTransferTransactionInformation/DebtorAgent/FinancialInstitutionIdentification/BIC*)

- ✓ # (separator)
- ✓ GIROInstant (pacs.008) settlement date of the transfer (yyyymmdd))

(*GroupHeader/InterbankSettlementDate*)

- ✓ # (separator)
- ✓ GIROInstant (pacs.008) transfer ID (max. 35 characters)

(*CreditTransferTransactionInformation/PaymentIdentification/TransactionIdentification*)

- ✓ # (separator)
- ✓ GIROInstant (camt.056) **8/11 character BIC code of the bank initiating the recall**

(*Assignment/Assigner/Agent/FinancialInstitutionIdentification/BIC*)

- ✓ # (separator)
- ✓ GIROInstant (camt.056) recall creation date (yyyymmdd)

(*Assignement/CreationDate*)

- ✓ # (elválasztójel)

GIROInstant (camt.056) recall ID (max. 35 characters)

(*Assignement/Identification*)

- ✓ # (constanst) marking GIROInstant cross-references end

Példa:**#GIROInstant#GIROHUHA#20181215#GIROINSTANTpacs008azonosito#GIROHUHA#20181218#GIROINSTANTcamt056azonosito#**

Comment

Several transfers can be entered in one sending batch (ICF.I) in IG2.

REFUSE TO RECALL IN GIROINSTANT FOLLOWING A REFERRAL IN IG2

Transaction camt.029 referring to the IG2 transfer:

- ✓ status: RJCR,

- ✓ reason: ARDT (amount already refunded),
- ✓ in the message of the structural thread (CancellationDetails/TransactionInformationAndStatus/
- ✓ Original TransactionReference/RemittanceInformation/Unstructured) should refer to the IG2 transfer as follows.
    - # (constans) mark - IG2 cross-references start
    - **IG2** (constans)
    - # (separator)
    - IG2 (pacs.008) Transfer Paying party's bank 8/11 character BIC code (*CdtTrfTxInf/DbtrAgt/FinInstnId/BIC*)
    - # (separator):
    - IG2 (pacs.008) settlement date of the transfer (yyyymmdd) (*GrpHdr/IntrBkSttlmDt*)
    - # (separator)
    - IG2 (pacs.008) ransfer ID (max. 35 **characters**) (*CdtTrfTxInf/PmtId/TxId*)
    - # (constans) mark – IG2 cross-references end

Example:: **#IG2#GIROHUHC#20190211#IG2pacs008azonosito#**

Comment

In the rejection of the recall, we have not specifically marked the references to the details of the original transfer, as (by default) the rejection of the recall should repeat the main details of the original (pacs.008) instant transfer in the block provided for this purpose.

(CancellationDetails/TransactionInformationAndStatus).

The IG2 cross-references can be followed by the actual communication, if required

5 Rejection codes

The basic instant transfer service does not check the content of the rejection code in the negative status report provided by the Clearing Member of the Beneficiary Party for the instant transfer.
The Clearing Member of the Beneficiary Party may use the codes from the code list available on the ISO 20022 website, except for the codes used by MS03 and GIROInstant[4].

6 Reports

Final status report

In the GIROInstant platform, each transaction is cleared and settled immediately when GIROInstant has generated the final status report (pacs.002) from the positive status report sent by the Clearing Member of the Beneficiary Party for the transfer, or the Clearing Member of the Paying Party has received the return (pacs.004) as a positive response to the callback. In settlement and execution, the instant settlement account of the Clearing Member of the Paying Party will be credited with the value of the instant transfer and at the same time the amount will be credited to the instant settlement account of the Clearing Member of the Beneficiary Party. In the event of a refund, the amount refunded shall be credited immediately to the Instant Settlement Account of the Clearing Member of the Beneficiary Party and simultaneously credited to the Instant Settlement Account of the Clearing Member of the Paying Party.

Reconciliation reports

The aim of reconciliation is to make sure that all participants processed the same transactions. In case the reconciliations reveal discrepancies in the transactions further investigation is needed.

To perform the reconciliation, so-called Reconciliation Cycles have been introduced in GIROInstant. Each Reconciliation Cycle follows each other every hour, so that there are 24 Reconciliation Cycles per calendar day. Each Reconciliation Cycle ends on the hour, with the last cycle of the day ending at 00:00. If, as a result of the reconciliations described above, the Clearing Members are not notified of a Reconciliation, the reports on the settlement account turnover shall be deemed final and therefore authentic at the end of each Reconciliation Cycle. Each transaction, upon receipt in GIROInstant, is automatically assigned to a Reconciliation Cycle. A transfer is completed in the cycle in which it was received by GIROInstant. Once the closing time of a given cycle has been reached, transactions received after the cycle closing time are automatically reclassified to the next cycle, so that the GIROInstant platform ensures that each transaction is only included in one Reconciliation cycle.

[4] HCTInst Message Implementation Guideline contains the codes used by GIROInstant..

Reconciliation is the responsibility of the Clearing Members. The GIROInstant platform generates reports on each Clearing Member's own transactions and on the transactions of the Indirect Participants belonging to each Clearing Member at each Reconciliation Cycle and at the end of the Settlement Day. The reports only include completed transactions that have reached final status, i.e. the platform waits for all relevant transactions to reach final status before compiling the reports.

Intraday reports

- CRR

At the end of the reconciliation cycles the so called CRRs (Cycle Reconciliation Report) get sent out that contain the Clearing member and its Indirect participants' incoming and outgoing pacs.008 and pacs.004 transactions that have been processed in the given cycle, broken down to number, amount, sender and receiver

A CRR forms is: XML.

- CTR

At the end of each reconciliation cycle the so called CTR (Cycle Transaction Report) is also generated that contain the Clearing member and its Indirect participants' incoming and outgoing transactions that have been processed in the given cycle, broken down to three groups.:

- ✓ Successful, sent transactions: messages sent successfully (booked) by the patricipant
  - o - pacs.008 (CT – Credit Transfer),
  - o - pacs.004 (RCT – Returned Credit Transfer),
  - o - camt.056 (REC - Recall),
  - o - camt.029 (RNK – Recall Not Acknowledged),
  - o - pacs.028 (INV - Investigation),
  - o - pain.013 (PAR – Payment Activation Request) és
  - o - pain.014 (PARSR – PAR Status Report).
- ✓ Successful, received transactions: messages received successfully (booked) by the patrcipant
  - o - pacs.008 (CT – Credit Transfer),
  - o - pacs.004 (RCT – Recalled Credit Transfer),
  - o - camt.056 (REC - Recall),
  - o - camt.029 (RNK – Recall Not Acknowledged),
  - o - pain.013 (PAR – Payment Activation Request) és
  - o - pain.014 (PARSR – PAR Status Report).
- ✓ Unsuccessful, failed transactions: messages sent by the participant unsuccessfully (rejected)

- - pacs.008 (CT – Credit Transfer),
- - pacs.004 (RCT – Recalled Credit Transfer), 000
- - camt.056 (REC - Recall),
- - camt.029 (RNK – Recall Not Acknowledged),
- - pacs.028 (INV - Investigation),
- - pain.013 (PAR – Payment Activation Request) és
- - pain.014 (PARSR – PAR Status Report).

✓ **Unsuccessful received transactions: unsuccessful messages transmitted to the Clearing Member (rejected by the Clearing Member or by GIROInstant due to "time out" in the absence of a response from the Clearing Member)**

- - pacs.008 (CT – Credit Transfer),

Failed transactions sent include transactions rejected by GIROInstant or, in the case of a transfer, by the Creditor. Since only the rejection code determines which party (GIROInstant or Creditor) rejected the transfer, the Creditor cannot use GIROInstant's rejection codes, e.g. AB06.

In addition to the messages of the Clearing Members, the report also includes, in a separate section, the closed - margin adjustment messages (Bank Account/Collateral Checking Module messages) and correction operations. Successful and unsuccessful margin adjustment messages are listed in a separate group.

The report also includes, among other things, the opening and closing book balances of the clearing member.

CTR reports have to be downloaded by Clearing Members via API or GIROInstant Monitor, they are not sent automatically by the platform.

A CTR forms is: XML.

End of day reports

- DRR

At the end of each settlement day, after the closing of the last reconciliation cycle (at 0:00), the GIROInstant system prepares the so called DRR (Daily Reconciliation Report) alongside the actual intraday CRR. The DRR contains the given Clearing mebmer and its Indirect participants' all incoming and outgoing pacs.008 and pacs.004 transactions that have been processed that day, broken down to number, amount, sender and receiver. The structure of the DRR is identical to the CRR's. The difference is the transaction set that is being reported.

A DRR form is: XML.

- DTR

Every calendar day, at the end of the settlement day, i.e. at the close of the last Reconciliation Cycle, the platform generates the end-of-day transaction report, the Daily Transaction Report (DTR), in addition to the current transaction report (CTR). The structure of the DTR is the same as the CTR, but the report does not contain a cycle, but the settlement day's transactions per Clearing Member and their corresponding Indirect Participants. The structure of the DTR is the same as described for the CTR report, but the cycle ID in the DTR is 00.

The DTR report must be downloaded by the Clearing Members themselves and is not sent automatically by the platform.

A DTR form is: XML.

The reconciliation process

The execution of reconciliation is the responsibility of the Clearing member. In case a Clearing member cannot process or download a given report, or the report gets lost, the participant has the possibility to download them later via the GIROInstant Monitor (multiple times even).

DTR reports must be downloaded by the Clearing member because these reports will not be sent out automatically.

In case of summary report:

The Clearing member prepares the appropriate data sets from its own system.

- ✓ Compares the results with the contents of the CRR and DRR reports.
- ✓ In case there is no difference the reconciliation can be closed.
- ✓ In case of difference there is a possibility to download a transaction list via the GIROInstant Monitor for a given time period, which list contains all the transactions of the Clearing member and its Indirect participant's.
- ✓ The exact reason for the difference can be deduced from the checking of the transaction list compared to the Clearing member own dataset, and further investigation can be carried out..

In case of reports on transaction level

The Direct participant prepares the detailed transaction list from its own system.

- ✓ Compares the results with the contents of the CTR and DTR reports.
- ✓ In case there is no difference the reconciliation can be closed.

- ✓ In case of difference the exact reason for the difference can be deduced from the checking of the transaction report compared to the Direct participant's own dataset, and further investigations and instructions can be carried out.

SECONDARY ACCOUNT ID MESSAGE FLOW DESCRIPTION

BUSINESS TERMS AND CONDITIONS

ANNEX NO 26.

1 Introduction

The document is a description of the message flow process description of the Secondary Account Identification Service, which is an additional service of GIROInstant and is processed continuously (0-24 hours) all days of the year. The document contains a high-level description of the functions of the Secondary Account Identification Service and information on the management and processing of messages.

This document is intended to assist Clearing Members and Service Providers in using the Secondary Account Identification Service.

1.1 References, related documents

ID	Title
EPC[5] rules, standards	
EPC 004-16	SEPA INSTANT CREDIT TRANSFER (SCT INST) SCHEME RULEBOOK
EPC 122-16	SEPA INSTANT CREDIT TRANSFER (SCT INST) SCHEME INTERBANK IMPLEMENTATION GUIDELINES[6]
ISO rules	
ISO 20022	Financial Services – Universal Financial Industry message scheme
Related legislation	
MNBr.	35/2017. (XII.14.) MNB Decree
Other documents	
Guidance issued to facilitate the use of the above message standards by banks [7]	

[5] European Payments Council / Európai Pénzügyi Tanács

[6] The ISO2002 standard provides a detailed description of the structure and use of standards to facilitate development

[7] HCT Inst Message Implementation Guideline, which is made available by GIRO Zrt. on its website, subject to registration, at the time of entry into force of these Rules..

2 General ovewiew

Linking Proxy identifiers to payment account numbers facilitates the use and spread of instant payment.

Features of the service are:

- ✓ Continuous (24/7/365) online operation.
- ✓ Non funds transfer messages.
- ✓ A reply for looking up IBAN corresponding to the proxy ID given in the message will be sent within a maximum of 1 second after the receipt of the lookup request by GIRO Zrt.
- ✓ A reply for inquiring proxy identifier(s) corresponding to IBAN given in the message will be sent within a maximum of 5 seconds after the receipt of the inquiry by GIRO Zrt.
- ✓ A reply to a registration message will be sent within a maximum of 5 second after the receipt of the registration request by GIRO Zrt.
- ✓ A reply to a delete message will be sent within a maximum of 5 second after the receipt of the delete request by GIRO Zrt.

GIRO Zrt. Central Proxy Identifiers Database (or central database) provides for the storage and real time management of proxy identifiers and related data. Proxy identifiers – at the launch of the service – are mobile telephone numbers with international prefix (country code), e-mails and tax Ids. Over the compulsory minimum fixed by MNB decree – i.e. it is only expected to store mobile telephone numbers or tax Id of the countries of EEA – GIRO database can provide wider possibilities for Users and can store proxy identifiers from any country.

In addition to the mandatory minimum required by the MNB Decree, which only requires the recording of mobile phone numbers and tax identification number or tax number belonging to EEA countries, the GIRO Zrt. database provides a wider scope for Service Providers and Clearing Members and can accommodate secondary account identifiers belonging to any country.

Registration, deletion and inquiry on proxy identifiers can only be initiated by account holding payment service providers connected to the service. Other legal or personal entities are not allowed to address the central infrastructure for such a purpose. Other legal entities (not holding payment accounts) can be connected to the service but they can not use the above mentioned functions, they can only use the look up function.

2.1 Functions of the proxy identifier system

- ✓ **Registration:** Payment account and the related proxy identifier are registered simultaneously in the database. Registration can only be initiated by a clearing member
- ✓ **Deletion:** simultaneous deletion of the payment account and the related proxy identifier from the database. Deletion can only be initiated by a clearing member
- ✓ **Lookup:** giving the proxy identifier the corresponding payment account number can be looked up.
- ✓ **Inquiry:** only the Customer, who has made registration has the right to inquire with a specific payment account. The results of an inquiry are all the proxy identifiers belonging to the given payment account.

Initiating the above listed functions happens one by one using the parameters for a particular function's request, input parameters of an XML

2.2 Execution time

The beginning of measurement of the expected execution time belonging to the Proxy identification functions is the receipt of message or request by GIROInstant, which is measured to an accuracy of thousandth seconds. These functions have no timeout, so one can also get a response to the message or request over the expected execution time. In the case of the Lookup function the expected execution time is maximum one second. Planned execution time for Registration, Deletion and Inquiry is maximum 5 seconds. The start of timing is the time of receipt of the message, as defined by the GIROInstant platform.

3 Flowcharts

The following definitions are used in flowcharts:

NAME OF FUNCTION	REQUEST (figure)	REQUEST (Standard references)	Response (figure)	RESPONSE (Standard References)
Registration	**registration XML**	NASRegisterAliasInformationRequest	**status XML**	NASRegisterAliasInformationResponse
Deletion	**deletion XML**	NASDeleteAliasInformationRequest	**status XML**	to the initiator of deletion: NASDeleteAliasInformationResponse
			notification XML	to the registering party, if it is different from the initiator of deletion: NASDeleteAliasInformationNotification
Lookup	**REST call URL**	https://{host:port}/nas-ws/api/v1/bic/{value}/aliasInformation/phone/?alias={value}	**response XML**	NASAliasInformationResponse
Inquiry	**REST call URL**	https://{host:port}/nas-ws/api/v1/bic/{Value}/aliasInformation/IBAN/?alias={value}	**response XML**	NASAliasInformationResponse

Requests for the Lookup and Inquiry function are processed by GIRO Zrt. Secondary Identification Message Implementation Guide of the GIRO can be sent using the HTTPS-based URL.

The Lookup and Inquiry functions use the GET method while the Registration and Deletion functions use the POST method of the HTTPS.

3.1 Registration

Registration of a proxy identifier - initially the mobile phone number with international prefix (country code), the email address, the tax identification number with international prefix (country code) of natural persons and/or corporations in any country-, can be carried out by sending the details of the name and the payment account. The e-mail address is always stored in the Proxy database as a lower case letter.

Only one payment account number can be associated with one proxy identifier – in order to obtain unambiguous relationship - but one payment account can have multiple proxy identifiers, thus an account can have multiple owners or multiple types of proxy identifiers.

The Registration process can only be performed if the proxy identifier to be registered has not yet been registered to another payment account. If the proxy identifier has been registered previously, then the system notifies about it, and the previous registration has to be deleted before the new Registration.

Data associated with a proxy identifier are not changeable. Therefore in order to modify the name or the BIC or the account, the account holding Clearing member must delete the proxy identifier and re-register it again with the correct data.

Figure 1 Registration process

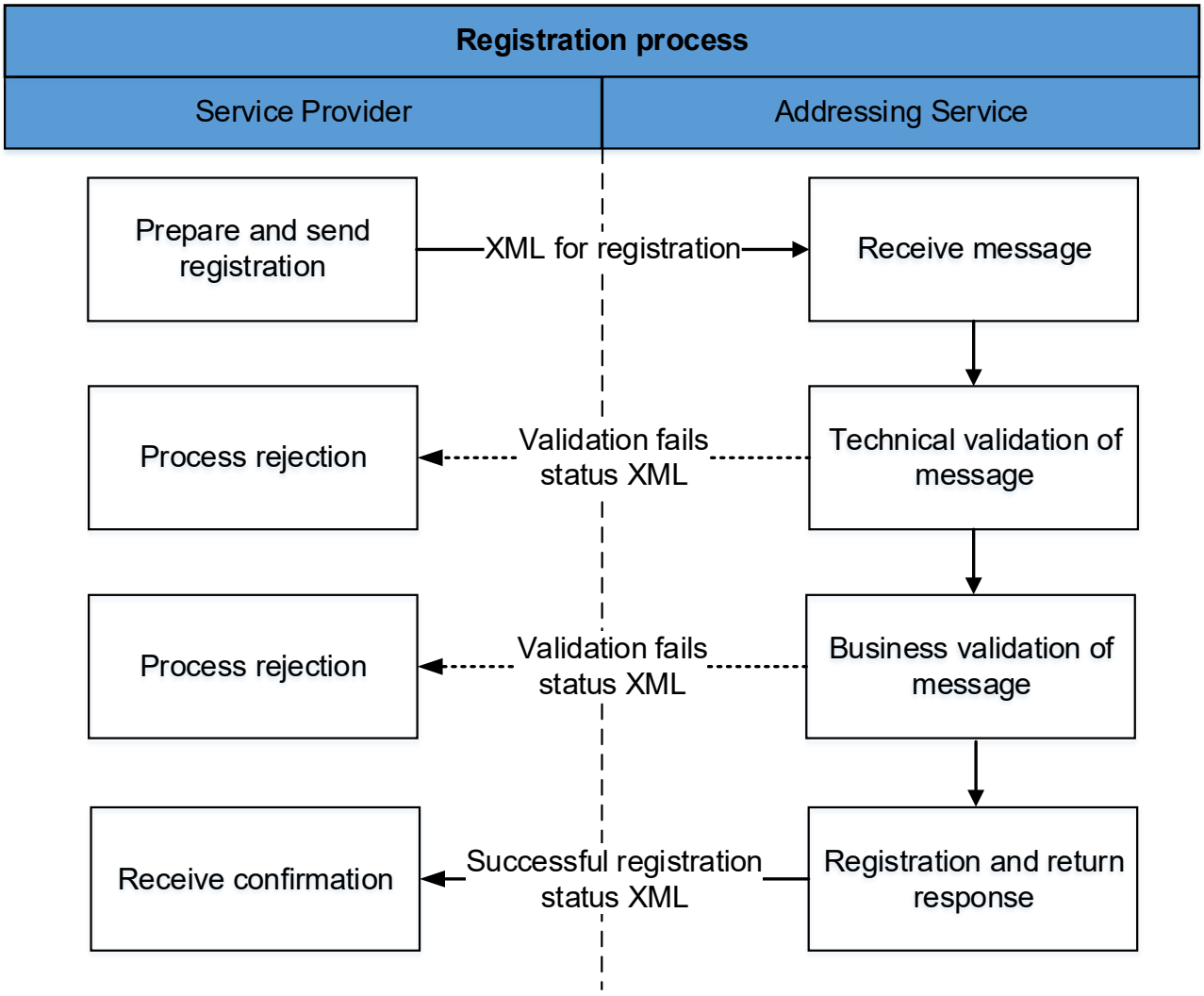


Table 1 Registration Process

Registration process	
Description	The registration proceeds one by one. GIRO Zrt. GIROInstant system receives the proxy registration message in a standardized format. If the validation fails, the system rejects the registration. The standard rejection message will be sent to the initiating Clearing member. If the validation has succeeded, the identifier specified in the message will be registered in the Central Proxy Database. The system sends a registration confirmation message to the initiating Clearing member. Upon successful registration, the proxy becomes immediately available for lookup.
Participants	✓ Account holding (registering) Clearing member ✓ GIRO Zrt. GIROInstant System (Addressing Service)
Clearing member side	
Requirements	✓ Payment service provider must verify the customer's right to the account and to the proxy identifier before registering a proxy identifier. ✓ Only the account holding payment service provider can fulfill this task
Content of message, validation	✓ Before submission, the registering party has to verify, that the proxy identifier is correct and belongs to the customer. ✓ Only mobile numbers can be registered as proxy identifier, landline numbers are not allowed. They have to be registered with country code between "+" and "-"; in case of a Hungarian number "+36-". ✓ Example, Hungarian mobile: <MobNb>+36-307654321</MobNb> ✓ The validation of the email addresses is the responsibility of the payment service providers. Recommended maximum length: 70 characters. Example: <EmailAdr>lev.elek@mail.hu</EmailAdr> ✓ The validation of the tax identification number or tax number is the responsibility of the payment service providers. Tax identification number and tax number have to be registered with country code prefix (HU). Tax number has to be registered with the individual number (8 characters) without VAT code and area code. Example, Hungarian tax number: <Othr>TXNB:HU12345678</Othr> Example, Hungarian tax ID: <Othr>TXID:HU9876543210</Othr>

	✓ When registrating tax number or tax ID other than Hungarian, type TXID has to be used. ✓ The system can be expanded with other proxy identifiers in the future. Their code types will be agreed with market demands. <Othr>Type:Value</Othr>
Message format	✓ XML
Execution	✓ The XML message is sent to the server using the POST method to the URL. https://{host:port}/nas-ws/api/v1/nasRegisterAliasInformation
GIROInstant platform	
Validations	✓ Duplication check to validate if the proxy identifier with the given proxy identifier type has already been registered in the system. ✓ Formal validation of the registration message: the central infrastructure performs syntax validation of the registration message, i.e. compares it to the message template (XSD validation). ✓ BIC and IBAN validation. ✓ Registration can be submitted by the account holding payment service provider, i.e. BIC of the submitter has to be the same as the BIC belonging to the IBAN of the account to which the proxy should be linked. The financial service provider can only register the accounts that are held with them. ✓ Name formal validation. ✓ Detailed description of validations can be found in Message Implementation Guidelines
Execution	✓ Proxy identifier data registration in the central database.
Response messages	✓ Reject o Negative answer, if the function can not be performed. o The answer contains the reason of the rejection. ✓ Confirmation o Positive answer, if the function has been performed.
Message format	✓ XML

3.2 Deletion

A registered proxy identifier can be deleted. For example the proxy identifier will be deleted if its owner does not want to use it anymore, or wants to link it to another payment account, or if the BIC, the account number, or the name will be changed. If there is a need to link the already registered proxy identifier to a new payment account then the system will inform about the already established link, and the previous registration must be deleted before the new relationship can be registered.

Deletion must also be performed if the proxy identifier does not belong to the available to entitledanymore or the annual data reconciliation was unsuccessful or negative feedback was received from the available to entitled.

Our system supports annual data reconciliation and deletion with a „ProxyYearlyReport" XML report that can be downloaded by the respective account holding bank.

Figure 2 Deletion process

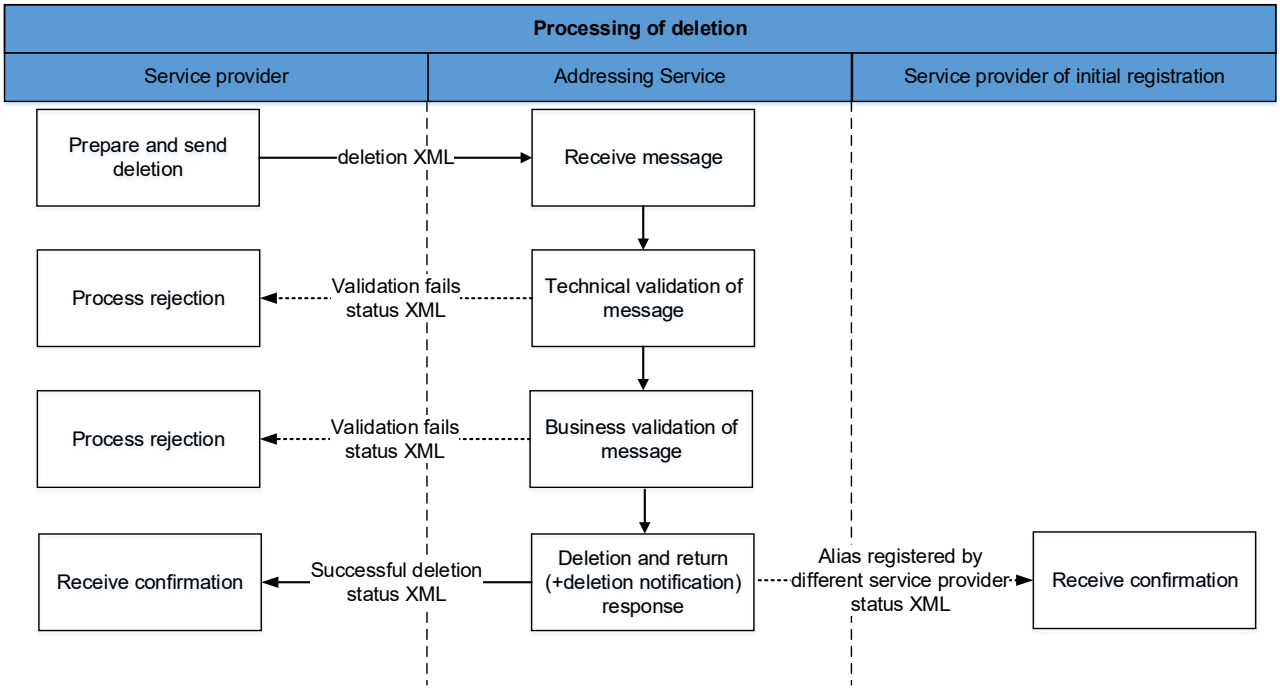


Table 2 Process of cancellation

Process of cancellation	
Description	The GIRO GIROInstant system receives the standard proxy identifier deletion message. If the validation fails, the system rejects the deletion of the proxy identifier. A rejection message will be sent to the Clearing member. If the validation has succeeded, the identifier in the message will be deleted from the Central Proxy Database. The system sends a deletion confirmation message to the Clearing member. If an already registered proxy identifier needs to be linked to a new account and the new account is managed by a different service provider as the previously linked account, the Clearing member of the new account can initiate deletion. If this is the case, the deletion notification will be sent to the new Clearing member.
Participants	✓ Account holding (registering) Clearing Member ✓ New account Clearing member ✓ GIRO Zrt. – GIROInstant system
Clearing member side	
Requirements	Only the Clearing member can fulfill this task.
Message content, validation	Before the submission, the Clearing membery has to verify, that the proxy identifier is correct and belongs to the customer.
Message fomrat	XML
Execution	XML messages are sent to the server using the POST method on the URL: https:// {host:port}/nas-ws/api/v1/nasDeleteAliasInformation
GIRO Zrt. GIROInstant platform	
Validations	✓ Formal validation of the proxy identifier: the central infrastructure performs only a syntax check of the proxy identifier. ✓ BIC validation. ✓ Detailed description of validations can be found in Message Implementation Guidelines.
Execution	✓ Looking up data belonging to the Proxy identifier and deleting them from the central database

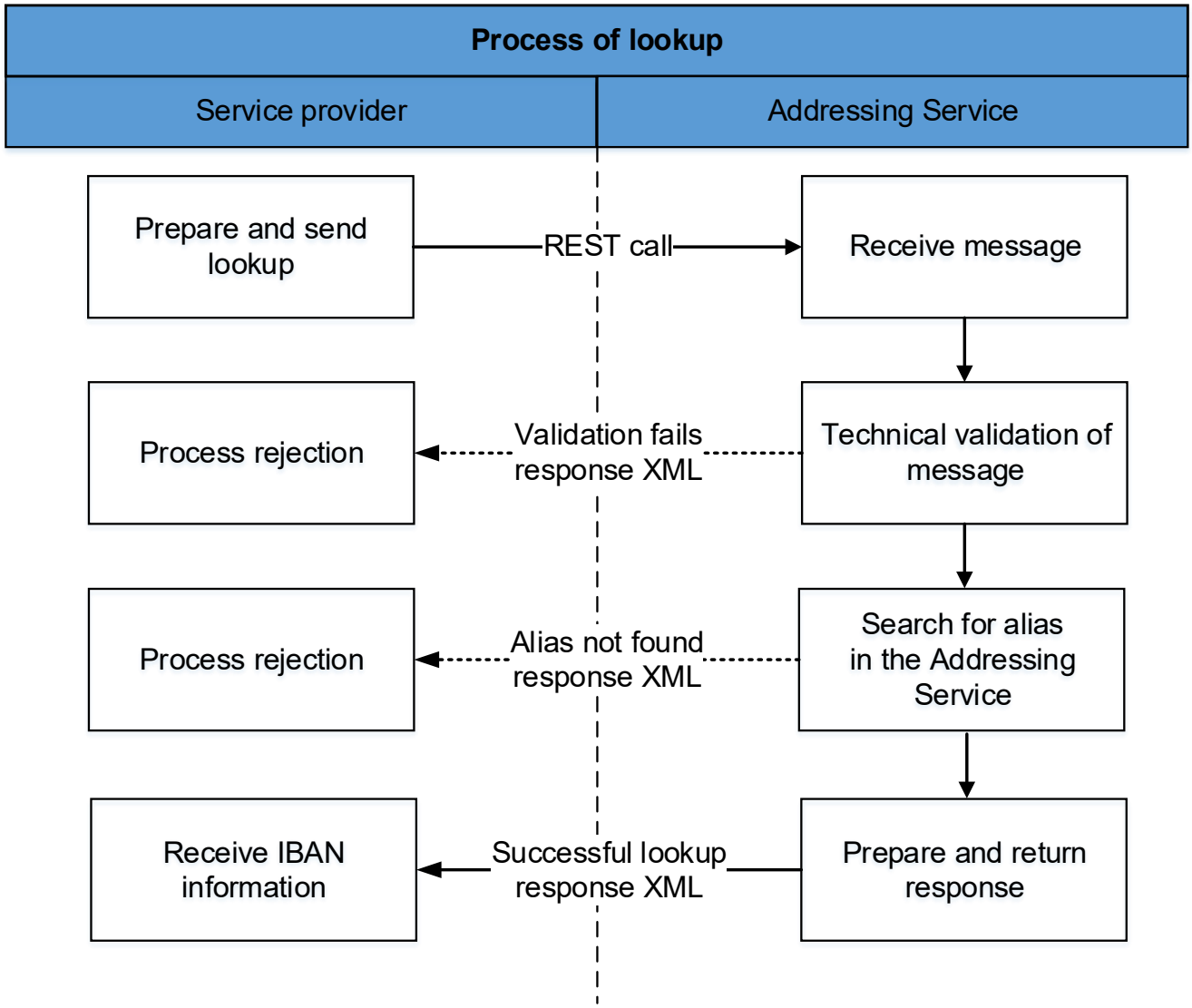
Response messages	✓ Reject o Negative answer, if the function can not be performed. The answer contains the reason of the reject. ✓ Confirmation o Positive answer, if the function has been performed. ✓ Deletion notification o Notification to the Clearing member, if the deletion successfully fulfilled.
Message format	✓ XML

3.3 Lookup

The lookup function gives back the account number information (BIC + IBAN) and name associated with an existing proxy identifier (type + identifier). These payment account details and name information must be provided in the instant payment and request to pay transactions.

The Clearing member looks up the proxy identifier in the Central Proxy Identifier Database operated by GIRO even if the customer orpaying party is its own customer. It is the Clearing member interest and responsibility to execute the lookup with correct data. The GIRO's Central Proxy Identifier Database contains always the most up-to-date data. If the Clearing member builds its own database based on the registration and deletion messages, the transactions must be executed with the data stored in the central database, i.e. it is the clearing member, if the executed transaction's account number does not correspond to the account number registered in the central database.

Figure 3 Lookup process



In the case of an instant transfer, the Debtor Agent or Service Provider shall not return the IBAN account number and the available name associated with the proxy identifier to the Debtor, and in the case of a payment request, the Creditor agent or Service Provider shall not return the IBAN account number and the available name associated with the proxy identifier to the Beneficiary. In the event of an unsuccessful Lookup, it may be returned in both of the above cases that no instant transfer or payment request can be initiated for the proxy identifier provided by the Beneficiary.

Table 3 Lookup process

Lookup process	
Discription	The GIRO zrt. GIROInstant receives the standard proxy identifier lookup REST message. If the validation fails, the system rejects the Proxy identification lookup

	message. A standard reject message will be sent to the initiating party. If the validation has succeeded, the identifier in the message will be looked up in the Central Proxy Database and sends a message to Clearing Member IBAN, BIC and the name of account holder. The system also sends a notification if there is no hit at all i.e. there is no proxy identifier in the database.
Participants	Initiator: ✓ Payment service provider, who is authorized to use lookup function of the Proxy identifier database. ✓ GIRO GIROInstant
Clearing Member or Service Provider	
Message content, validation	The lookup party has to verify before the submission, that the proxy identifier is well-formed (syntactically correct).
Message format	REST call
Execution	Lookup options regarding the various proxy identifiers can be found in the Giro zrt Message Implementation Guidelines, e.g. based on mobile phone numbers the following: https://{host:port}/nas-s/api/v1/bic/{value}/aliasInformation/phone/?alias={value}
Example	GET https://nas.realtime247.giro.hu/nas-ws/api/v1/bic/OTPVHUHB/aliasInformation/phone/?alias=+36-207654321
GIRO Zrt. GIROInstant platforms	
Validation	✓ Formal validation of the proxy identifier: the GIROInstant performs only a syntax check of the proxy identifier. ✓ Detailed description of validations can be found in Message Usage Guidelines.
Execution	✓ Looking up in database IBAN, BIC and account holder's name that belong to the proxy identifier
Response messages	✓ Reject o Negative answer, if the function can not be performed. The answer contains the reason of the rejection. ✓ Negative confirmation o Feedback to the Clearing Member, that the lookup has no results at all. ✓ Results list o Positive answer to the Clearing member with the results, i.e. BIC + IBAN and name.

Message format	✓ XML

3.4 Inquiry

During the inquiry process the system returns all proxy identifiers registered to the inquired payment account. The Inquiry initiator must be only the Clearing Member. An inquiry can be initiated only by the registrator account holding payment service provider. The process of the inquiry is identical with the lookup process.

Figure 4 Process of inquiry

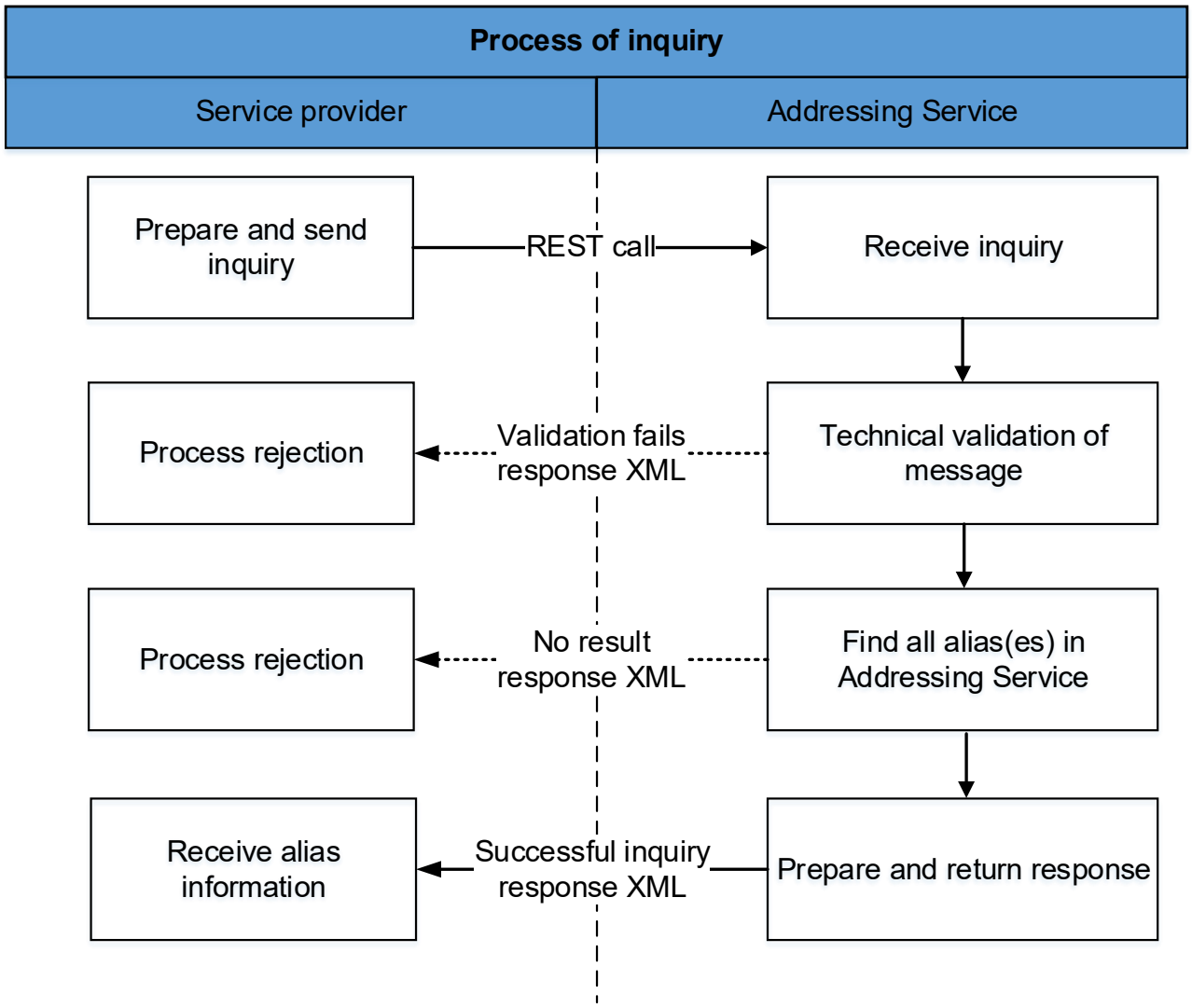


Table 4 Inquiry process

Inquiry process	
Description	The Proxy Identifier System operated by GIRO receives the standard proxy identifier inquiry message (REST call). If the validation fails, the system rejects the inquiry of the proxy identifier. A rejection message will be sent to the initiating party. If the validation has succeeded, all data belonging to the given IBAN will be retrieved from the Central Proxy Database and the data belonging to proxy identifier will be sent to the Initiator. The system sends back a notification if there are no hits at all i.e. no data were found in the database.
Participants	✓ The Clearing Member holding the payment account ✓ GIRO Zrt. – GIROInstant syste,
Clearing member	
Requirements	Only the Clearing member can fulfill this task.
Message content, validation	Before submitting, the Clearing Member must check that the IBAN account number is formally correct and that it is the correct IBAN for the query.
Message format	REST call
Execution	https://{host:port}/nas-ws/api/v1/bic/{Value}/aliasInformation/IBAN/?alias={value}
Example	GET https://nas.realtime247.giro.hu/nas-ws/api/v1/bic/OTPVHUHB /aliasInformation/IBAN/?alias=HU99117731261111111100000000
GIRO Zrt. rendszere	
Validations	✓ Inquiry can be submitted from the Clearing menber, i.e. BIC must be the same as that of the inquiring party. ✓ A detailed description of the checks can be found in the GIRO Zrt. Proxy Identification Message Application Implementation Guide.
Execution	✓ All proxy identifiers belonging to the given IBAN will be inquired from the Database
Response message	✓ Reject Negative answer, if the function can not be performed. The answer contains the reason of the rejection. ✓ Feedback

	Feedback to the initiator, that the inquiry has no results at all i.e. the inquired IBAN has not been found in the database. ✓ Results list Positive answer to the initiator with the results, i.e. all the found proxy identifiers and names.
Message format	✓ XML

3.5 Reports

- PTR

At the end of each calendar day, i.e. at the close of the day, a separate PTR (Proxy Transaction Report) is generated for the transactions associated with the proxy account identifiers, which can be downloaded by Clearing Members or Service Providers via API or GIROInstant Monitor. In the PTR, the Registration, Cancellation, Lookup and Query messages initiated by a given Clearing Member are detailed, and for Service Providers, the Lookup messages are detailed in the report.

A PTR form is: xml.

- PYR

The secondary account identifiers' annual validation and deletion are supported with the PYR (Proxy Yearly Report) report that available for the respective account holding bank. The report contains all secondary account identifiers that registered by the bank which will have the registration anniversary 40 calendar days later.

A PYR form is: xml.

A detailed description of the reports can be found in the GIRO Zrt. will be published on GIROnline.

REQUEST TO PAY MESSAGE FLOW DESCRIPTION

BUSINESS TERMS AND CONDITIONS

ANNEX NO 27.

1 Introduction

Request to Pay service is available 365 days a year and operates non-stop (0-24). It verifies and transmits messages related to the Request to Pay service. This rulebook contains the description of the service, its functions, user rules and information on the handling and processing of Request to Pay messages, in accordance with the current Payment Service Regulation.

The current document details the rules for connecting to the Request to Pay service for users wishing to join to the service. It also provides an overview of message flow processes and practical information on usage and standards.

1.1 References, Related documents

Identification	Title
EPC[8] rules, standards	
EPC 004-16	SEPA INSTANT CREDIT TRANSFER (SCT INST) SCHEME RULEBOOK
EPC 122-16	SEPA INSTANT CREDIT TRANSFER (SCT INST) SCHEME INTERBANK IMPLEMENTATION GUIDELINES
ISO standards	
ISO20022	Financial Services – Universal Financial Industry message scheme Creditor Payment Activation RequestV06, pain.013 – Payment Initiation Payment Activation Request Status ReportV06, pain.014 – Payment Response
Related legislation	
MNB rendelet	Decree Nr 35/2017. (XII.14.) of the Governor of the National Bank of Hungary (MNB) on the carrying out of payment transactions.
Other documents	

[8] European Payments Council

Identification	Title
Guidance to facilitate the application of the above message standards in banking[9]	

1.2 Changes

Date	Content
1 December 2023	Chapter 5: the value limit amount for instant credit transfer has been removed, and modified paragraph Message flow between non-Clearing Members.
1 January 2024	New chapter 1.2. Changes Chapter 5: added new parapraph Purpose code of request to pay

2 General Overview

The GIROInstant system operated by GIRO Zrt. is based on open standards. No manual processing is required, it is considered STP (Straight Through Processing).

2.1 The concept of request to pay

Request to Pay is based on standardised messages in the instant payment system sent by the requester (Payee) to the Payer to initiate payment. Request to pay is a non-payment message which contains all data required by the Paying party to initiate instant payment and for the service provider of the Requesting party to process the said payment. The Requesting party may request instant money transfer from the Paying party via its own service provider. Request to pay may also be sent directly to GIRO Zrt. if an agreement to do so is in place.

The purpose of the request to pay is to automate payment initiation on the Payer's side. The Paying Party receives in the request to pay all the details of the individual credit transfer from its payment service provider and after the verification of the data, the payer may approve the credit transfer.

2.2 Characteristics of request to pay service

The Sending (Requesting) party may submit the request to pay to its service provider in a way that instead of the name and the domestic account number of the Paying party the secondary account identifier (proxy) is used. In such a case it is the responsibility of the service provider of the Requesting party to identify the name and account number of the Paying party using the Secondary Account

[9] The "VAS Message Implementation Guideline" will be available on the website of GIRO Zrt. subject to registration.

Identifier Database (directly or via a payment service provider) and submit the request with the appropriate data.

Requesting party may set the validity of the request to pay. Based on the regulations, validity is a maximum of 2 calendar months after submission, lasting until 24:00 on the last calendar day. The system does not check the validity of the request, messages are relayed regardless.

It is possible to indicate in the request whether the payable amount may be modified by Paying party

The message responding to the request to pay and the message initiating the request to pay are not compared, the content of the messages is not checked by the system providing the service.

Apart from payment service providers legal entities registered in Hungary may also join the service if they comply with GIRO Zrt.'s policy conditions.

A request to pay may only be made by a clearing member or service provider who is eligible according to GIROInstant's records.

The Sender's (Requester's) service provider must deliver the request to pay to Paying party's service provider within 5 seconds after the receipt of the message. The Paying party's service provider forwards the accepted request to pay to Paying party without delay and according to the agreement between Paying party and its service provider.

In the lack of agreement between Paying party and its service provider the Paying party's service provider may refuse to forward the request to pay to Paying party.

Within 5 seconds the Paying party's service provider notifies the submitting party's service provider about the rejection or forwarding the message to Paying party. In turn, Requester's service provider notifies Requester party about the delivery or rejection.

3 The process of request to pay

There is no set way of communication between customer and service provider in the flowcharts. Between service providers and the central system there is a flow of standard ISO messages, the types of which are indicated in the charts. Request to Pay messages need to be submitted in pain.013 format. In reply various pain.014 messages may arrive. "GrpSts" indicates the status of the request. The status may be:

- ✓ Received and forwarded to Paying party (RCVD = received),
- ✓ Rejected (RJCT = rejected)
- ✓ Settled (ACCP = accepted).

GIRO Zrt. will validate the submitted request to pay and its response according to formal and business rules. If the conditions for validation are not fulfilled

- ✓ request to pays are rejected by GIRO Zrt. with the error code pain.014
- ✓ GIRO Zrt. interrupts the processing in case of responses to the request to pay and the withdrawal of the request to pay,
    - the request to pay remains unanswered,
    - the request to pay recall message does not reach the addressee.

GIRO Zrt. does not "pair" request to pays and request to pay recall messages with replies, nor does it check whether the references to the request to pay data in the reply to the request to pay or recall are correct.

3.1 Request to pay – positive flow

Figure 1. – Request to pay – initiation, approval and settlement in case of banking service providers

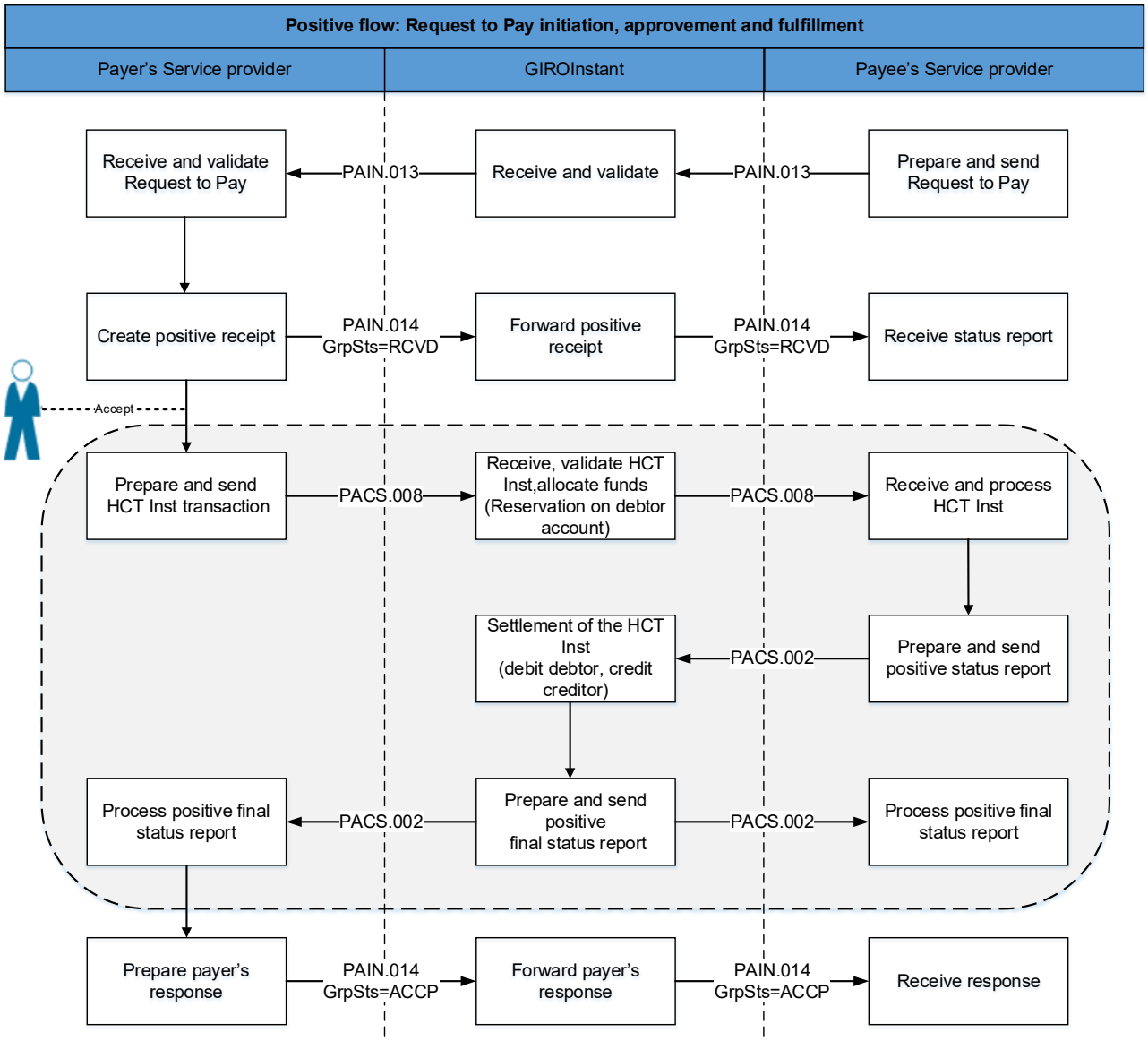


Figure 1: Positive flow: Payment initiation, approvement and fulfillment

Steps in case of banking service providers:

- ✓ Requesting party or its banking service provider submits request to GIRO Zrt. in pain.013 format (after substituting secondary account identifier with bank data if necessary).

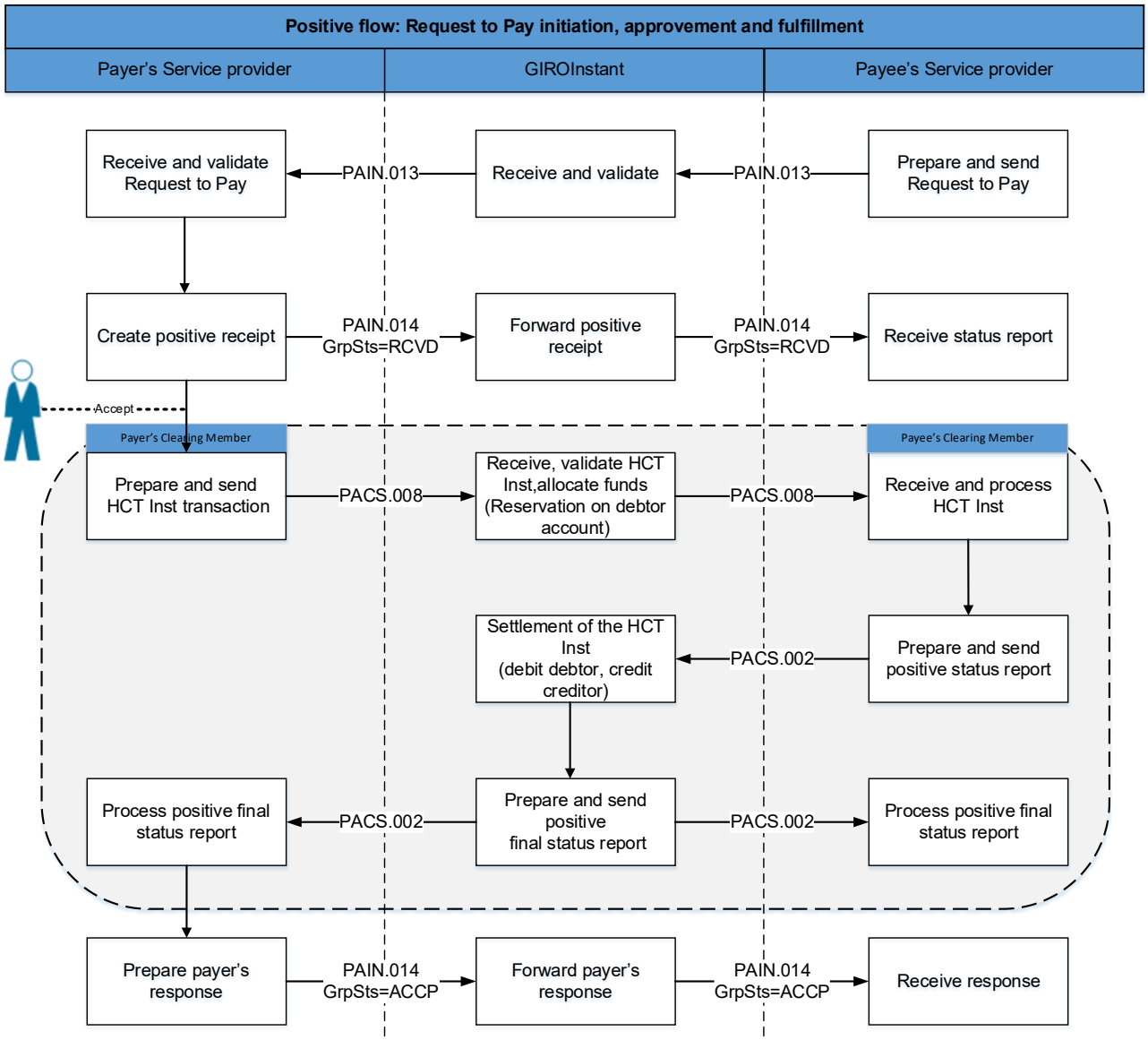
- ✓ GIRO forwards the verified (correct) message to the banking service provider of the Paying party.
- ✓ Paying party or its banking service provider confirms receipt and acceptance (code: RCVD) via GIRO within 5 seconds in pain.014 format and forwards the message to Paying party.
- ✓ If the response of the Paying Party's Clearing Member is found by GIRO Zrt. to be incorrect due to a formal error or non-compliance with business rules, the processing will be terminated and the request to pay will remain unanswered.

On Paying party's approval

- ✓ Banking service provider initiates instant payment via pacs.008 message if there is coverage on the related account.
- ✓ GIROInstant – as set out in HCT Inst Scheme – notifies the concerned parties (banking service providers of Requesting and Paying party) about the successful settlement of the transfer in a final status report (pacs.002 message).
- ✓ If the original pain.013 request allowed for the modification of the payable amount, the payment may be done with larger or smaller amount in pacs.008 messages.

- ➢ Paying party or its banking service provider notifies Requesting party or its banking service provider (with pain.014 message, code: ACCP) about the settlement of the Request after successful money transfer

Figure 2. – Request to Pay – initiation, approval and settlement in case of not just banking service providers



Steps in case of not just banking service providers:

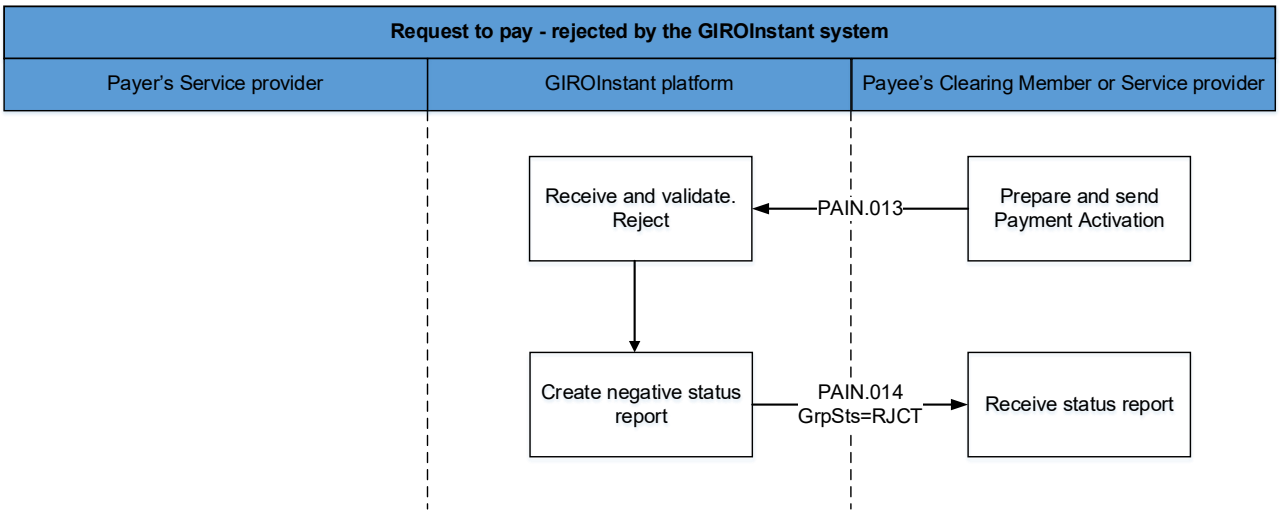
- ✓ Requesting party's non-banking service provider submits request to GIRO in pain.013 format (after substituting secondary account identifier with bank data if necessary).
- ✓ GIRO forwards the verified (correct) message to the non-banking service provider of the Paying party.
- ✓ Paying party's non-banking service provider confirms receipt and acceptance (code: RCVD) via GIRO within 5 seconds in pain.014 format to the Requesting party's non- banking service provider and forwards the request to Paying party.
- ✓ On Paying party's approval

- Paying party's banking service provider initiates instant payment via pacs.008 message if there is coverage on the related account.
- GIROInstant – as set out in HCT Inst Scheme – notifies the concerned parties (banking service providers of Requesting and Paying party) about the successful settlement of the transfer in a final status report (pacs.002 message).
- If the original pain.013 request allowed for the modification of the payable amount, the payment may be done with larger or smaller amount in pacs.008 messages.

✓ Paying party's non-banking service provider notifies Requesting party's non-banking service provider (with pain.014 message, code: ACCP) about the settlement of the request after successful money transfer. The notification contains all relevant status data received from Paying party's banking service provider.

3.2 Request to pay – rejected by GIRO

Figure 3. – Request to Pay – rejected by system



Steps:

✓ Requesting party or its service provider submits request to GIRO Zrt. in pain.013 format (after substituting secondary account identifier with bank data if necessary).

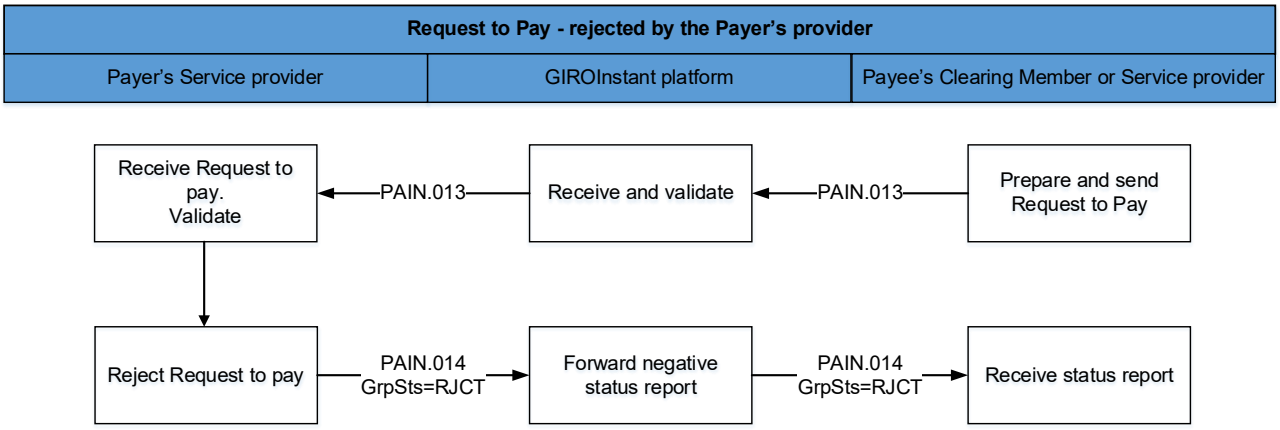
✓ GIRO rejects the message with pain. 014 message (code: RJCT, reason specified), if the submitted request does not fulfil the verification requirements set out in the standards. The data of the pain.013 messages rejected by GIRO Zrt. due to non-compliance with business rules can be found in the transaction level reconciliation reports (CTR and DTR) and can be queried in the GIROInstant Monitor Search Transaction (VAS) function.

If the pain.013 message is found by GIRO to be incorrect due to a formal error, processing will be completed and the request to pay message will not be transmitted. In the case of a formality error, a SOAP Fault message is sent to the VAS Fault endpoint in response, the

details of the pain.013 message rejected by GIRO can be viewed on the Parse Exception screen in the GIROInstant Monitor.

3.3 Request to pay – rejected by Paying Party's service provider

Figure 4. – Request to Pay – rejected by paying party`s service provider



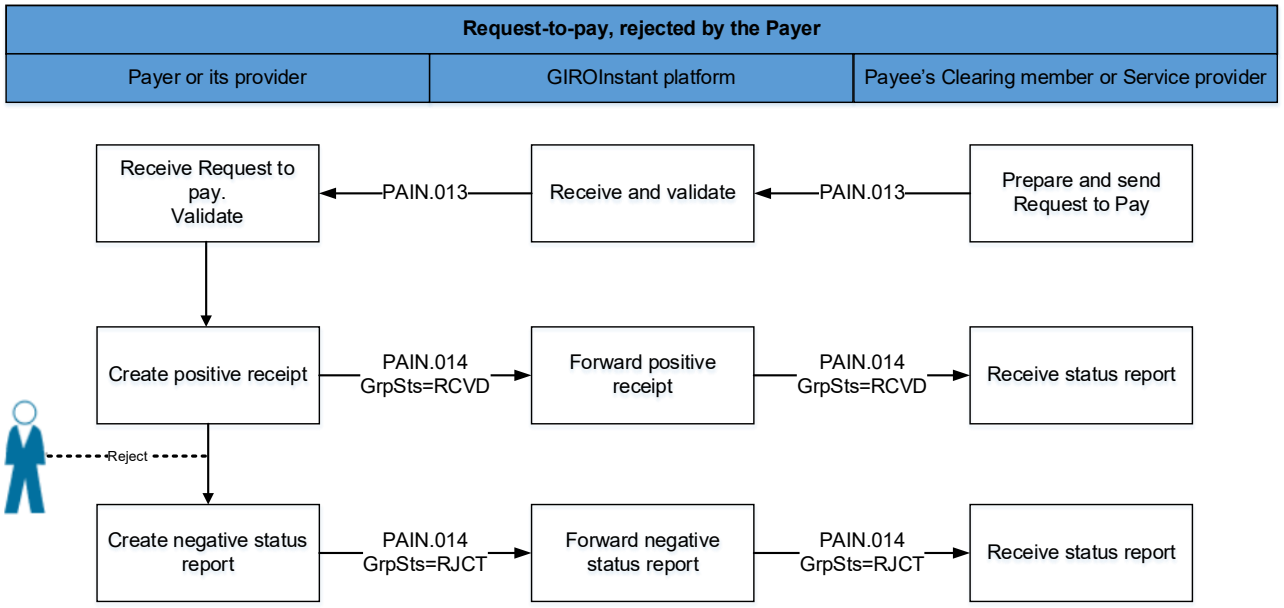
Steps:

- ✓ Requesting party or its service provider submits request to GIRO Zrt. in pain.013 format (after substituting secondary account identifier with bank data if necessary).
- ✓ GIRO forwards the verified message to the Paying party's service provider.
- ✓ Paying party's service provider replies with pain.014 message via GIRO to inform Sending party about reception and rejection (RJCT). Reason for rejection is specified in the message (e.g.: non-existent bank account).

- ➢ If the response of the Paying Party's Service Provider is found by GIRO Zrt. to be incorrect due to a formal error or non-compliance with business rules, the processing will be terminated and the request to pay will remain unanswered. In the case of a formal error, the response is a SOAP Fault message sent to the VAS Fault endpoint, the details of the pain.014 message rejected by GIRO can be viewed on the Parse Exception screen in the GIROInstant Monitor. The data of pain.014 messages rejected by GIRO due to non-compliance with business rules can be found in the transaction level reconciliation reports (CTR and DTR) and queried in the GIROInstant Monitor Search Transaction (VAS) function.

3.4 Request to pay – rejected by Payer

Figure 5. – Request to Pay – rejected by Payer

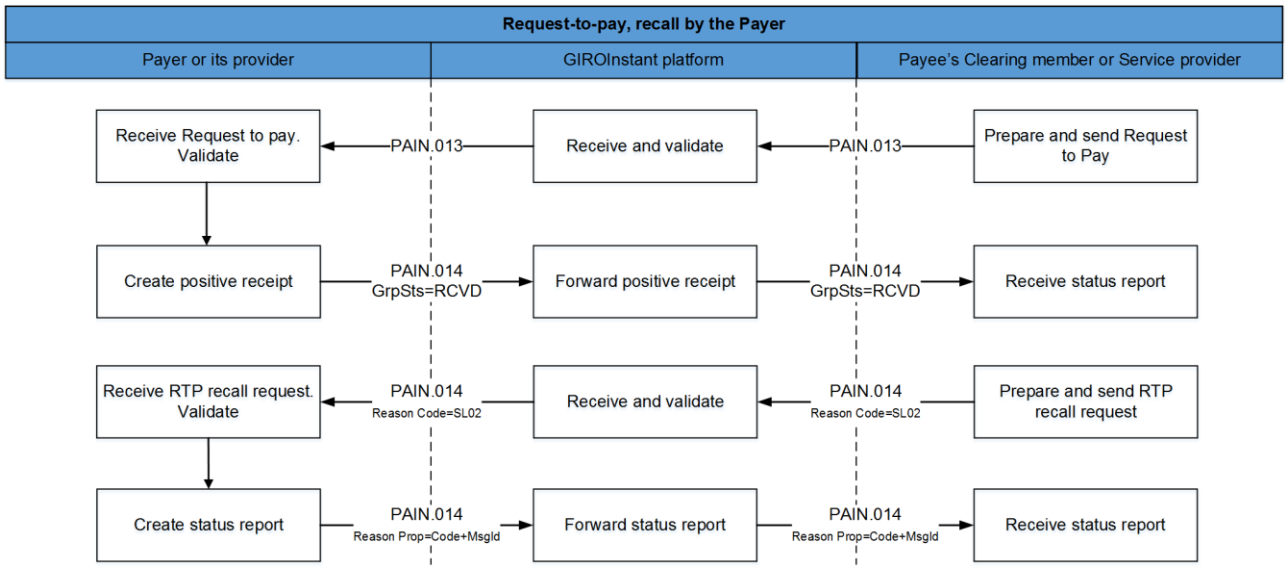


Steps:

- Requesting party or its service provider submits request to GIRO Zrt. in pain.013 format (after substituting secondary account identifier with bank data if necessary).
- GIRO forwards the verified message to the Paying party's service provider.
- Paying party's service provider replies with pain.014 message via GIRO to inform Submitting party about reception (RCVD), and forwards the request to Paying party.
- Paying party rejects request to pay.
- Paying party's service provider notifies Submitting party (via GIRO, using pain.014 message) about rejection (RJCT). The paying party's rejection must be indicated via standard ISO code "DS02" in message pain.014 below RJCT status. The message can also contain additional information / textual explanation on the reason of rejection.
- If the response of the Paying Party's Service Provider is found by GIRO Zrt. to be incorrect due to a formal error or non-compliance with business rules, the processing will be terminated and the request to pay will remain unanswered. In the case of a formal error, the response is a SOAP Fault message sent to the VAS Fault endpoint, the details of the pain.014 message rejected by GIRO can be viewed on the Parse Exception screen in the GIROInstant Monitor. The data of pain.014 messages rejected by GIRO due to non-compliance with business rules can be found in the transaction level reconciliation reports (CTR and DTR) and queried in the GIROInstant Monitor Search Transaction (VAS) function.

3.5 Request to pay – recall by the Requesting Party

Figure 6. – Request to Pay – Recall by the Requesting party



Steps:

- ✓ Requesting party's service provider submits request to GIRO in pain.013 format (after substituting secondary account identifier with bank data if necessary).
- ✓ GIRO forwards the verified (correct) message to the service provider of the Paying party.
- ✓ Paying party's service provider confirms receipt and acceptance (code: RCVD) via GIRO within 5 seconds in pain.014 format and forwards the message to Paying party.
- ✓ If the request to pay's is still waiting for the paying party's reply (approval or rejection), the Requesting party's service provider can initiate a recall via pain.014 message (code: RJCT), with reason code SL02 = Specific Service offered by Creditor Agent.
- ✓ In case of request to pay recall message to GIRO Zrt. if you find it incorrect due to a formal error or non-compliance with business rules, then the processing will be completed, the request to pay recall message will not be transmitted. In case of formal error SOAP Fault message the response sent to the vas Fault endpoint is the pain rejected by GIRO.014 message data can be viewed on the GIROInstant Monitor on the Parse Exception screen. Pain refused by GIRO for non-compliance with business rules.014 message data can be found in the transaction level reconstruction reports (CTR and DTR) and can be queried in the GIROInstant Monitor Search Transaction (VAS) function.
- ✓ The paying party's service provider informs – via GIRO – the Requesting party (with pain.014 message, code: RJCT) about the result of the recall request's processing. Reason Proprietary field contains the recall's acceptance (ACCP) or rejection (RJCT) together with the recall's message identifier (MsgId). The message can also contain additional information / textual explanation on the reason of rejection.

- ✓ If the response of the Paying Party's Service Provider is found by GIRO Zrt. to be incorrect due to a formal error or non-compliance with business rules, the processing will be terminated and the request to pay recall message will remain unanswered. In the case of a formal error, the SOAP Fault message is the response sent to the VAS Fault endpoint, the details of the pain.014 message rejected by GIRO can be viewed on the Parse Exception screen in the GIROInstant Monitor. The data of pain.014 messages rejected by GIRO due to non-compliance with business rules can be found in the transaction level reconciliation reports (CTR and DTR) and queried in the GIROInstant Monitor Search Transaction (VAS) function.

4 Confirmation codes of request to pay

Request to Pay service does not verify the (acceptance or rejection) codes specified by addressee (the service provider of Paying party) in the reply messages to request to pay or recall message.

Paying party may use the codes from the code list of ISO 20022 (to be found on the internet) or the codes agreed on previously in the bilateral agreement with Submitting party. In the latter case all consequences of using the codes must be borne by the parties concerned.

5 Hungarian specialities of request to pay

Character set – rejected if inappropriate

In the text fields of the request to pay messages, if they are not identifiers, only the Hungarian accented characters in the "extended" ASCII range above 128 may be used in addition to all the basic UTF-8 characters (in the range 32 to 126). If an incorrect character is used, the request to pay will be considered invalid and will be rejected by the system.

Structure of Message ID

(RTP-REF/1 rule, see Message Implementation Guideline)

Transactions must have unique IDs which cannot recur for 7 calendar days.

The length of the message ID (MsgId) of a request to pay is maximum 35 characters. The required setup is as follows:

Character 1. – 11.	Service provider of Requesting party (BIC / BEI) in the case of an 8-character BIC, characters 9 – 11.: 3 x underscore (_)
Character 12.	dash (-)
Character 13. –	date of processing/submission, year, month, day (*YYYYMMDD*)

20.	
Character 21.	dash (-)
Character 22. – 35.	unique serial number of transaction within the day of processing (max. 14 characters) E.g.: KEZDBIC8___-20180322-12345678ABCDE0 or KEZDBIC1111-20180322-ABCDE012345678

Note: if the setup of the message ID is not standardized, the message is rejected by the system (reason code: HU56).

Currency – rejected if inappropriate

The currency of the Request to Pay messages can only be Hungarian forint, HUF. The amount may only be specified as an integer, with two decimals allowed, where the last two digits (the ones after the comma) may only be zero. Should these conditions not prevail, the Request shall be rejected by the system.

Start of execution time

Sending party specifies the start of execution to milliseconds. The Request to Pay service is logging the processing of the messages from submission to reception by addressee.

Secondary account identifier (PROXY-REF rule, see Message Implementation Guideline)

It has to be specified in the request if identification of Paying party is done be secondary account identifier.

Specifying message ID from start point to end point (RTP-REF/2 rule, see Message Implementation Guideline)

The message ID used in the MsgId field needs to be repeated in the EndToEndId field as well. If the content of these 2 fields differ, the message shall be rejected by the system (with reason code HU57).

In the HCT Inst message fulfilling the RtP instruction, there are two fields unambiguously indicating that the credit transfer is a reply to RtP:

- ✓ EndToEndIdentification field of credit transfer must contain the value of the request to pay's EndToEndIdentification field thus granting the relation of the two transactions. (See Hungarian Guideline "RTP-IND" in Message Implementation Guideline.)

- ✓ PaymentIdentification / InstructionIdentification field of credit transfer must indicate – among others – that the credit transfer fulfills a request to pay. (See Hungarian Guideline "RTP-REF" in Message Implementation Guideline).

Specifying fee payer (FEE-PAYER rule, see Message Implementation Guideline)

The ability of the Paying Party to change the amount of the request to pay shall be indicated by the constant '-M'. Modification is allowed in both directions, i.e. both higher and lower financial settlements than the amount of the request are possible. However, it is not currently possible to initiate more than one transfer on the basis of a request to pay.

The modifiability of the amount and the maximum number of instalments (nn) can be indicated in the same field (PaymentInformation / CreditTransferTransaction / PaymentIdentification / InstructionIdentification). The display of instalment payments is not currently allowed in the system, the following is only a description of the principle use of this information.

The maximum length of the "InstructionIdentification" field is 35 characters:

[[RTP-MOD][RTP-PMAX]]

For example:

1. - M (the amount of the request to pay can be changed, currently only this is used)
2. - M3 (the amount of the request to pay can be modified and can be settled in a maximum of 3 installments)

Relation between the fields of the request to pay and the instant payment message

- ✓ The unique (MsgId) ID – generated according to the rule defined in Message Implementation Guidelines – needs to be repeated in the PmtInf / CdtTrfTx / PmtId / EndToEndId field of the pain.013 message. This grants that the value of EndToEndId of the instant request to pay will be the same.
- ✓ The pacs.008 message fulfilling the request to pay must also contain this information in the CdtTrfTxInf / PmtId / EndToEndId field - this will be an unambiguous reference to the request to pay.
- ✓ In the field Pacs.008 CdtTrfTxInf / PmtId / InstrId the constant "-R" must be entered, indicating that the instant transfer is in response to the corresponding request to pay, "-R-M" for a modifiable amount. If an instalment payment is introduced, the serial number of the instalment payment will also have to be entered here, e.g. "-R-M3" or "-R-MF" (last instalment payment), but this function is not yet enabled.

- ✓ In the Pacs.008 CdtTrfTxInf / RgltryRptg block, the H-DATA information in the request to pay shall be repeated.

Modifiability of the notice

If the Paying Party modifies the communication, the modified communication shall be included in the responses to the initiation of the request to pay and in the transfer initiated upon acceptance.

If the request to pay message has not been modified by the Paying Party, the original message shall be displayed in the replies to the request to pay and in the transfer initiated for an accepted request to pay.

Validity period and payment term

Two dates play a decisive role in the execution of a request to pay; the period of validity of the request to pay and the deadline for payment.

The validity period of the application for payment, according to the current regulations, can be up to 2 months. The maximum period of validity may be the end of the last calendar day of 2 months following the submission of the request to pay, or a shorter period may be specified. Its location in the message standard: the RegulatoryReporting/Details/Information/LatestDtTm field of the H-DATA rule in the message Implementation Guide for a request to pay. Accuracy in hundredths of a second.

In addition to the period of validity of the request to pay, it is mandatory to specify the period of payment, which must be within the period of validity. It is also displayed in the PaymentInformation/RequestedExecutionDate/DateTime field of the request to pay to display the payment term, with hundredths of a second accuracy according to the RTP-DLN rule of the message Implementation Guide. This value is mandatory.

The above two values are related: payment term ≤ validity period.

Both values above are passed between the system members with an accuracy of hundredths of a second.

Feedback on an expired request to pay

If the Paying Party has not initiated a transfer in response to a request to pay by the end of the validity period of the request to pay, the service provider receiving the request does not need to send a feedback to the originator of the request due to the expiry of the validity period.

Message flow between non-Clearing Members

In addition to the basic use case of a request to pay flow, i.e. the payee sending a request to pay via its own account-holding Clearing Member to the payer via its own account-holding Clearing Member, Other Clients that are not Clearing Members, but are payment service providers or electronic money

institutions (not providing payment services) as well as institutions that have entered into a contract for the GIROInstant Additional Service or the GIROFix Service before 1 November 2023 may also participate in the request to pay flow (see Figure 2). Other Clients are identified in the system by a BEI code. If the recipient of the request to pay is an Other Client, the response to the request to pay must be sent to this provider.

Request to pay of HUF 0

A Clearing Member or Service Provider of the Beneficiary Party may not send a request to pay with a value of HUF 0. If this happens, the request to pay initiated with HUF 0 must be rejected by the Paying Party's Service Provider (with error code AM01).

Request to pay over limit

The "GIROInstant transfer limit amount and request to pay register", maintained and published by GIRO, shows the current limits for sending and receiving instant transfers by each payment service provider. Payment service providers shall report their sending and receiving limits to the register on a voluntary basis.

Request to pay response message fields

The status report sent for a request to pay (message type pain.014) must contain all fields that were specified in the request to pay message (pain.013), regardless of whether they were optional or mandatory. In the standard, XML tag names starting with 'original' refer to these fields, fields that should be treated differently are described in detail in the RTP Message Implementation Guide.

BIC code of the beneficiary bank of the instant transfer transaction sent on the basis of the request to pay

The Beneficiary-side BIC code of an instant transfer transaction created on the basis of a request to pay may be different from the Beneficiary-side BIC code specified in the request to pay (e.g. if the request to pay is sent by a bank on behalf of a Beneficiary with an account with another bank), therefore, the Beneficiary BIC code for the instant transfer transaction must always be filled in by retrieving the corresponding BIC code from the Validation Table in force on the day the transfer is initiated for the IBAN account number of the Beneficiary indicated in the request to pay.

Addressing the parties to a request to pay

Participants in the Request to Pay service can be Clearing Members and Other Customer Participants without a BIC code. Participants in the service should be prepared to send/receive request to pay messages from both types of participants. Other Customer Participants are identified by the BEI codes published by GIRO. For a detailed description of the addressing of these actors, please refer to the Message Implementation Guide.

Request to pay purpose code

The Purpose Code field of the request to pay message can be used to specify the purpose code of the request to pay, which is used to typify the transaction and also helps to fraud prevention. The mandatory/optional nature of the Purpose Code field is governed by the applicable Request to Pay Message Implementation Guide. The purpose code is selected from the ISO External Code Set by the Payee's Clearing Member or Service Provider, but if the payee is a natural person, the code "MP2P" should always be used. If the Payee is a legal entity, a code other than the above shall be used.

INDICATION OF DATA CARRIER

Request to Pay has to contain (in Regulatory Reporting block) the code (H-DATA/1) and identifier

(H-DATA/2) of data carrier as follows:

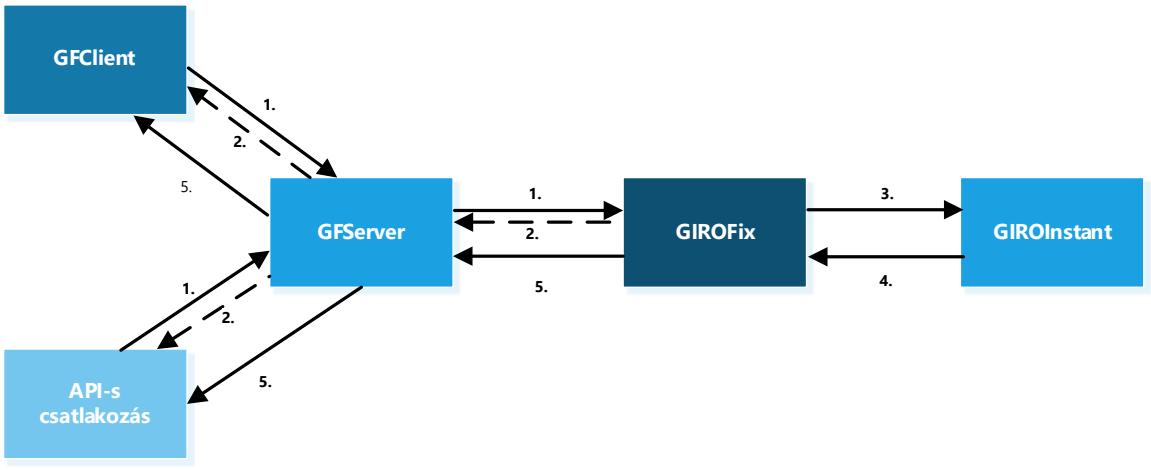
code	description
CustomerID	Customer identifier (at bill payment)
CredTranID	Beneficiary's internal transaction identifier
InvoiceID	Identifier of bill or invoice
LoyaltyID	Identifier of regular customer of discount system
MerchDevID	Identifier of commercial device (cash register, POS)
NAVCheckID	National Tax and Customs Office's Verification code
ShopID	Identifier of commercial unit, store
LatestDtTm	Validity period

6 GIROFix batch request to pay

GIRO Zrt. also receives GIROFix batch messages generated and submitted according to the GIROFix CSV message standard from client with a GIROFix service contract. A GIROFix batch message is a GIROFix standard message containing several individual request to pay or request to pay recall messages, from which GIRO Zrt. generates and submits individual request to pay (pain. 013) or request to pay recall (pain.014) messages to GIROInstant. The processing of individual request to pay generated from GIROFix batch request to pay in GIROInstant shall be carried out as described in Chapter 3.

GIROFix client subscribed to the GIROFix service are identified in the GIROFix system by one or more BEI code issued by GIRO Zrt. The purpose of this chapter is to describe the specific processing steps for GIROFix batch request to pay outside the GIROInstant system.

Figure 7. – GIROFix batch request to pay processing procedure



1. The Client contracted for the service sends request to pay or recall of request to pay messages generated in accordance with the GIROFix CSV message standard to GIRO Zrt. via GFClient application or API connection.
2. GIRO will perform a formal and business check of the submitted input batch as described in the GIROFix CSV message standard. The Client will be informed of the result of the input batch verification by two types of technical receipts:

    a. the GIROFix system will notify the submitter of the batch rejection with a negative technical acknowledgement,
    b. the successfully received batch will be opened and checked in batches, and any defective batches found during the check will be rejected. For request to pay submitted with a GIROFix secondary account identifier, GIRO Zrt. will perform a search in the secondary account identifier database. After the batch has been opened and all batch items have been processed, the GIROFix system will report back to the submitter on the success of the batch processing in the form of a positive technical receipt file, which will contain the number of requests to pays accepted and rejected and the reason for rejection.

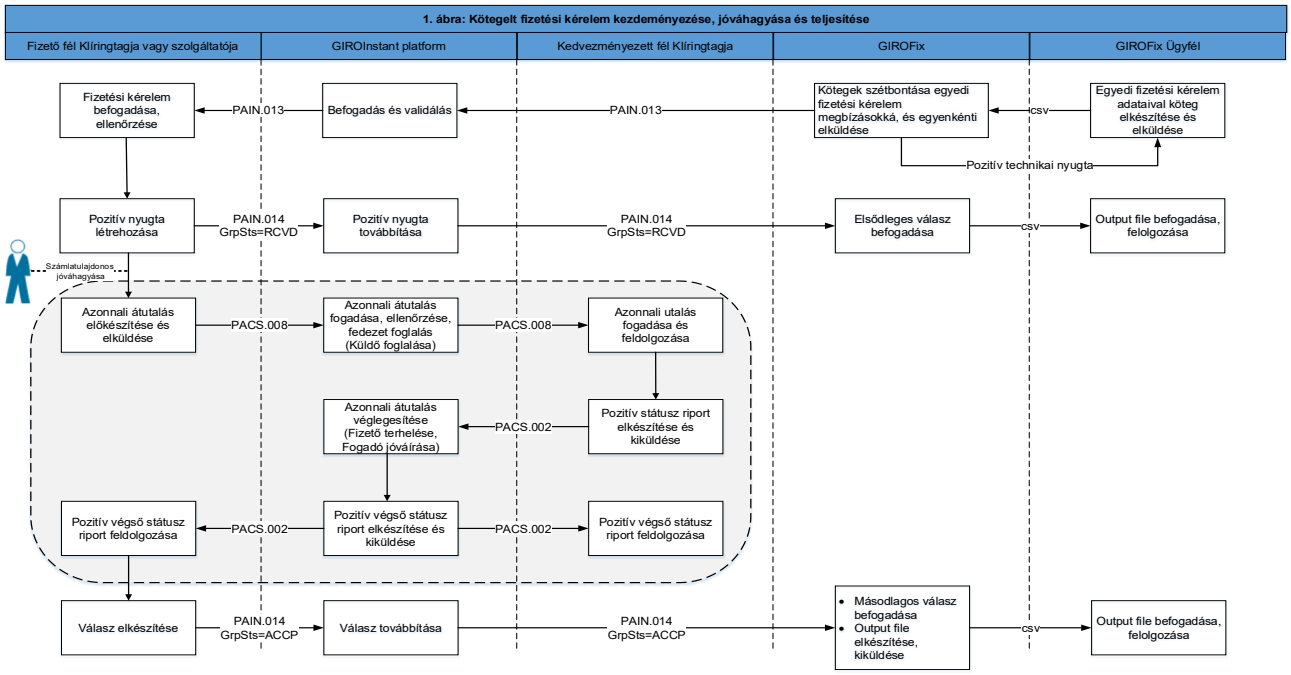
3. The GIROFix system converts the successfully received request to pay or recall of request to pay items in the order of receipt, under the Customer's BEI code, into standard request to pay (pain.013) and request to pay recall (pain.014) messages according to the Message Implementation Guide and sends the messages to the GIROInstant system on behalf of the sending Customer, signed, taking into account the request to pay received per second rate reported by the Payer's service provider.

Individual request to pay and request to pay recall messages generated from GIROFix batch messages and submitted to GIROInstant will be received by GIROFix in response to the payer's responses from GIROInstant.

4. The GIROFix system converts the response messages from the GIROInstant system into CSV format, grouped by type, with an hourly cyclical frequency, and sends them to the Customer. A Daily Activity Report is generated on the Customer's daily traffic.

6.1 GIROFix batch request to pay – positiv flow

Figure 8. – Initiation and execution of a GIROFix batch request to pay



Steps in the process:

- ✓ The Client contracted to the GIROFix service submits the request to pays to GIRO Zrt. in the GIROFix standard CSV file format. A GIROFix batch request to pay can be submit using a secondary account identifier instead of the Payer's account number and name.
- ✓ GIRO Zrt. will open the batches without errors and, after processing each batch, will provide the sender with a report containing aggregated data in a "Positive Technical Receipt" file, confirming the success of the batch processing.
- ✓ The error-free CSV items are converted into individual request to pay - pain.013 - messages and sent one by one to GIROInstant, which forwards them to the Payer's service provider. If the GIROFix batch request to pay was submitted with secondary account identifier, GIRO Zrt. first performs a search in the central secondary account identifier database and submit the request

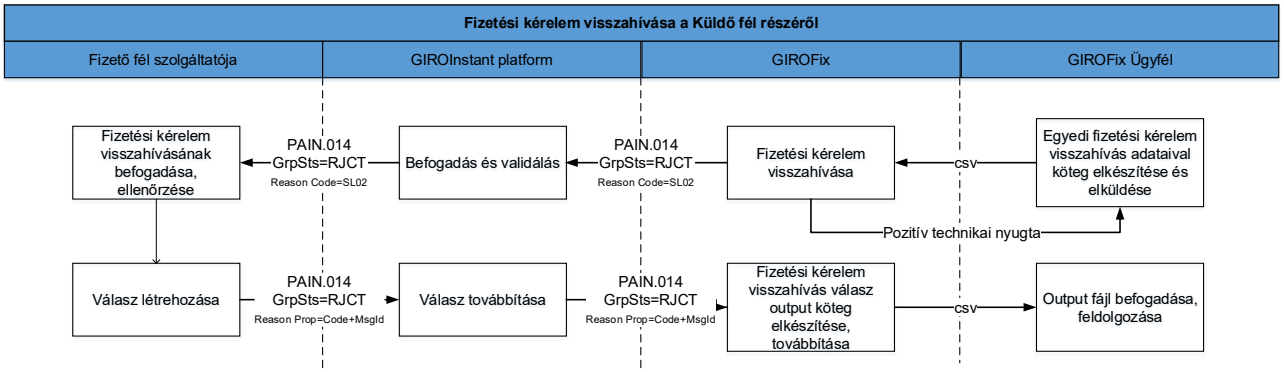
to pay (pain.013) to the GIROInstant system with the account number and account holder name received in response to the search.

- ✓ Within 5 seconds the Payer's service provider (via GIRO Zrt.) confirms the receipt of the request to GIRO Zrt. with a pain.014 message (code: RCVD), which is notified to the GIROFix customer by the GIROFix system in the output file containing the primary responses.
- ✓ If the response of the Paying Party's service provider is found by GIRO Zrt. to be incorrect due to a formal error or non-compliance with business rules, no primary response will be sent on the request to pay.
- ✓ Upon approval by the Paying Party, the Clearing Member of the Paying Party will initiate an instant transfer with message pacs.008, provided the Paying Party has sufficient funds. The process is carried out as described in Chapter 3.1.
- ✓ The Payer's service provider informs GIRO Zrt. (with a message pain.014, ACCP feedback code) about the execution of the request to pay by the Payer after the successful instant transfer, which is notified to the GIROFix client by the GIROFix system in the output file containing the secondary responses.

The GIRO Zrt. shall not return to the Client the IBAN account number and the name of the account holder associated with the secondary account identifier obtained as a result of the search.

6.2 GIROFix batch recall of request to pay – positive flow

Figure 9. – GIROFix batch request to pay recall



Steps in the process:

- ✓ The GIROFix Client submits the request to pay recalls to GIRO Zrt. in the GIROFix standard CSV file format. A GIROFix batch request to pay recall can be submit using a secondary account identifier instead of the Payer's account number and name.
- ✓ The GIRO Zrt. will open the batches without errors and, after processing each batch, will send a report containing aggregated data in a "Positive Technical Receipt" file to the submitter on the success of the batch processing. . If the GIROFix batch request to pay recall was submitted with secondary account identifier, GIRO Zrt. first performs a search in the central secondary

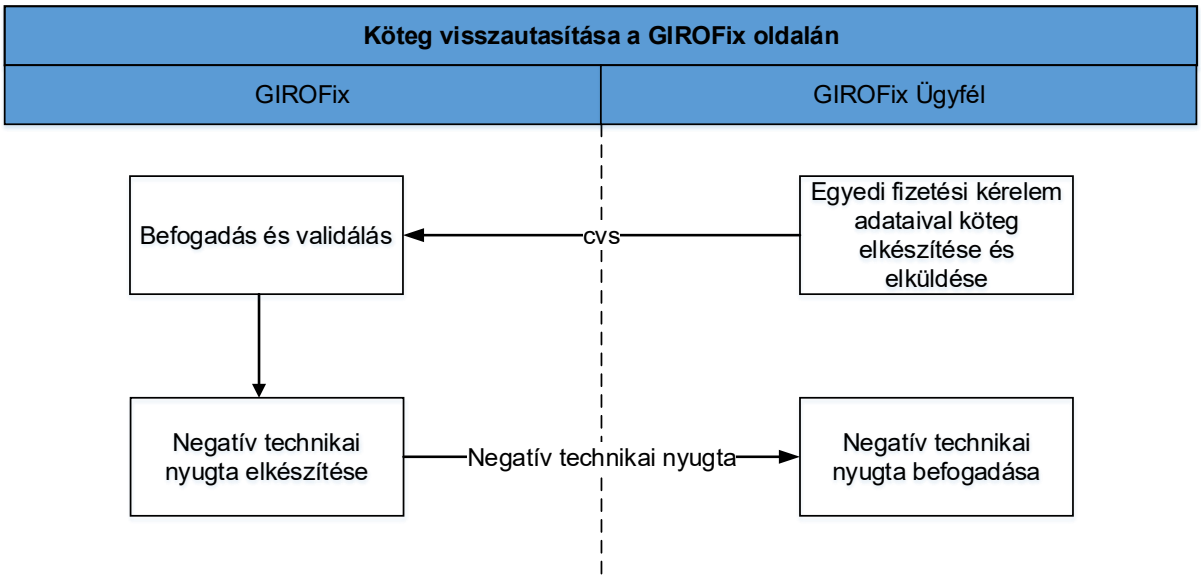
account identifier database and submit the request to pay (pain.013) to the GIROInstant system with the account number and account holder name received in response to the search.

- ✓ GIROFix converts the CSV error-free batches into individual request to pay recall - pain.014 - messages and sends them one by one to GIROInstant, which forwards them to the Payer's service provider.
- ✓ The Payer's service provider, via the GIRO S.p.A., notifies the GIRO S.p.A. of the result of the processing of the recall request by means of a pain.014 message (code RJCT), as described in Chapter 3.5. The Reason Proprietary field contains, in addition to the code indicating the acceptance (ACCP) or rejection of the recall, the identifier of the recall message (MsgId). The message may also contain a textual explanation of the reason for the rejection.
- ✓ The GIROFix system will notify the GIROFix Client of the feedback received on the result of the processing of the recall request in the output file containing the request to pay recall responses.

The GIRO Zrt. shall not return to the Client the IBAN account number and the name of the account holder associated with the secondary account identifier obtained as a result of the search.

6.3 Rejection in case of batch failure

Figure 10. – Reject a bundle on the GIROFix site



- ✓ The GIROFix Client submits the request to pays to GIRO Zrt. in the GIROFix standard CSV file format.
- ✓ The GIRO Zrt. checks the batches and if it finds any batch level errors (file consistency, file name, signature, certificate, submitter), the GIROFix system does not start processing the batches at batch level, but immediately returns an error message with a negative technical receipt to the client.

6.4 Feedback sent by GIROFix system

- Output batches: at specified intervals (every 1 hour), the primary and secondary responses received during the given time interval, as well as the request to pay recall responses, are sent in a CSV file generated by response type.

  The following types of response messages are distinguished:

  a) delivery response message (primary response),

  b) customer response to the request to pay (secondary response),

  c) request to pay recall response message.

- Positive technical receipt: generated and sent after the processing of the batch received has been completed.
- Negative technical receipt: generated and sent after the batch level check of the received batch in case of a batch level error.
- Daily Activity Report: a statement of the calendar day's turnover, containing the following data of the request to pay and withdrawal messages sent to GIROInstant for the calendar day in question:
  - identification by customer
  - Identifier by GIROFix
  - date of submission/receipt.

6.5 File name convention for message types received by GIROFix

- ✓ For request to pay batches: BEI + "INP13" + Date of submission + Batch number.csv (pl. GFIXHUH0000INP1320190424001.csv)
- ✓ Request to pay for recall batches: BEI + "INP14" + Date of submission + Batch number.csv (pl. GFIXHUH0000INP1420190424001.csv)

6.6 File name convention for message types sent by GIROFix to the Client

- ✓ Positive technical receipt for request to pay batches: BEI + ACK13 + original date + original serial number.csv
- ✓ (pl.: GFIXHUH0000ACK1320190424001.csv)
- ✓ Positive technical receipt request to pay for recall batches: BEI + ACK14 + original date + original serial number.csv
- ✓ (pl.: GFIXHUH0000ACK1420190424001.csv)
- ✓ Negative technical receipt request to pay for batches: BEI + NOTACK13 + original date.csv
- ✓ (pl.: GFIXHUH0000NOTACK1320190424.csv)

- ✓ Negative technical receipt request to pay for recall batches: BEI + NOTACK14 + original date.csv
- ✓ (pl.: GFIXHUH0000NOTACK1420190424.csv)
- ✓ Primary response: BEI + "PRI" + generation date + cycle number.csv
- ✓ (pl.: GFIXHUH0000PRI2019091801.csv)
- ✓ Secondary response: BEI + "SEC" + generation date + cycle number.csv
- ✓ (pl. GFIXHUH0000SEC2019091801.csv)
- ✓ Callback response: BEI + "RECA" + generation date + referencedBatchNumber.csv
- ✓ (pl. GFIXHUH0000RECA20190424001.csv)
- ✓ Day activity report: BEI+"REP "+yyymmdd.csv
- ✓ (pl. GFIXHUH0000REP20190424.csv)

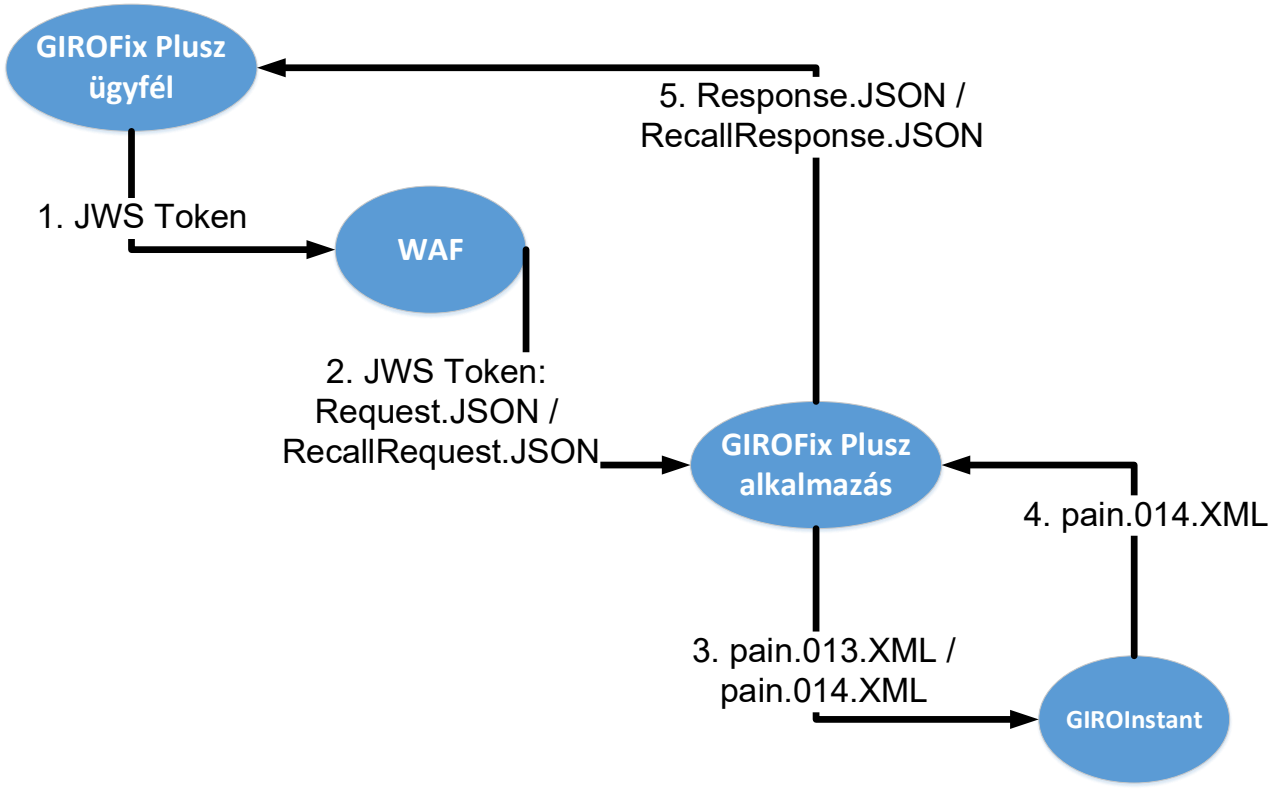
7 GIROFix Plusz standard message

GIRO Zrt. also receives request-to-pay or request to pay recall messages from Client with a GIROFix Plusz service contract in JSON format, generated and submitted according to the GIROFix Plusz message definition, from which GIRO Zrt. generates individual request to pay (pain. 013) or request to pay recall (pain.014) messages and submits to GIROInstant.

The processing of individual request to pay or request to pay recall generated from GIROFix Plusz standard message in GIROInstant shall be carried out as described in Chapter 3.

GIROFix Plusz Client subscribed to the GIROFix Plusz service are identified in the GIROFix Plusz system by one or more BEI code issued by GIRO Zrt. The purpose of this chapter is to describe GIROFix plusz standard message specific processing steps outside the GIROInstant system.

Figure 7. – GIROFix Plusz standard message process



1.-2. The Client contracted for the GIROFix Plusz service sends GIROFix Plusz standard message generated in accordance with the GIROFix Plusz message definition to GIRO Zrt. via web application firewall (WAF).
3. GIROFix Plusz system will perform a formal and business check of the submitted GIROFix Plusz standard message. GIRO Zrt. will perform a search in the central secondary account identifier database if the request to pay or request to pay recall was submitted with a secondary account identifier.

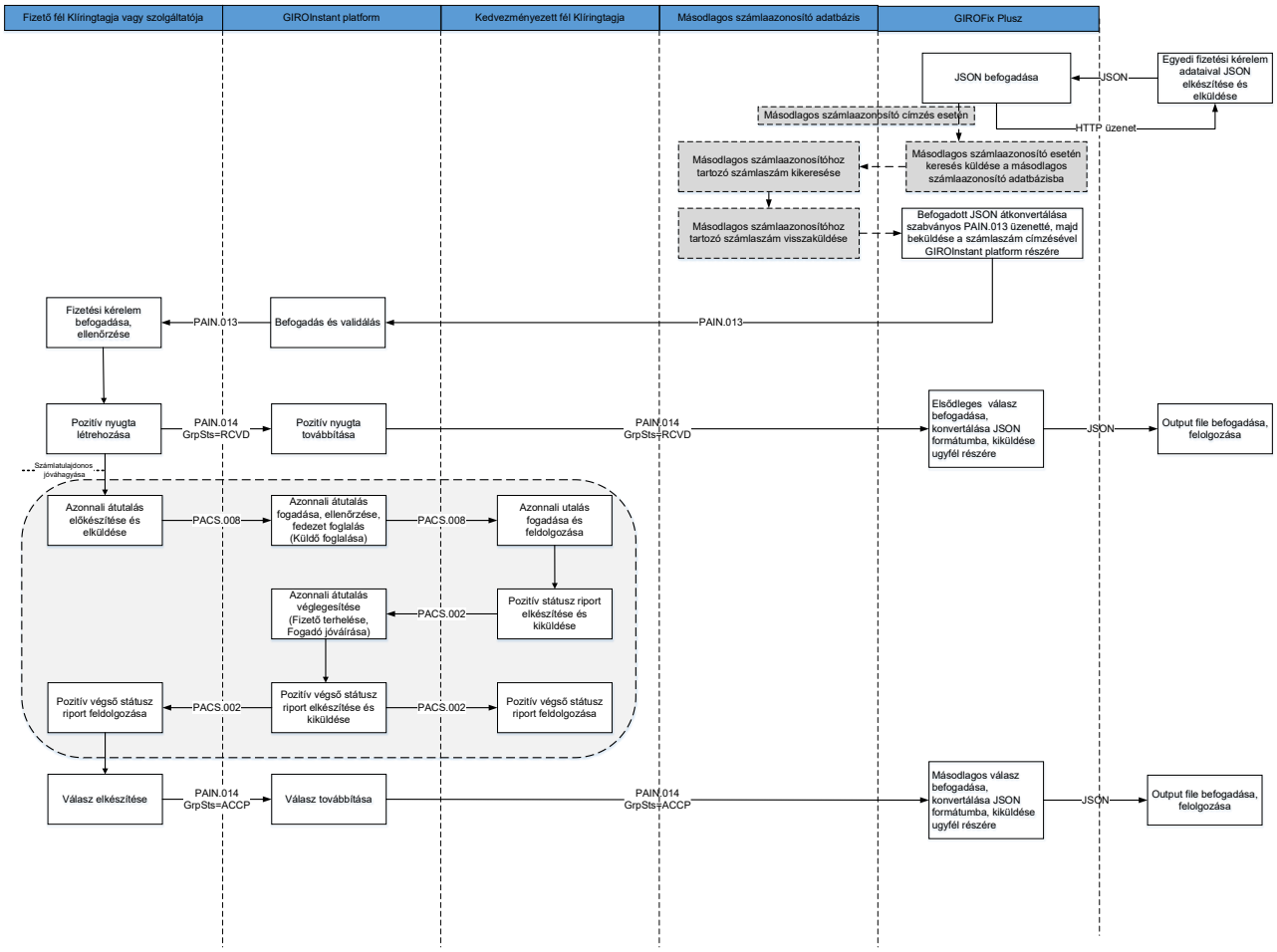
The GIROFix Plusz system converts the valid GIROFix Plusz standard message into xml format request to pay (pain.013) and request to pay recall (pain.014) messages and sends the messages to the GIROInstant system.

4. GIROInstant forwards the pain.014 xml format primary and secondary response messages sent by the Payer's service provider.

5. The GIROFix Plusz system converts the response messages into GIROFix Plusz message format and sends them to the Client.

7.1 GIROFix Plusz request to pay – positiv flow

Figure 8. – Initiation a GIROFix Plusz request to pay and settlement the instant credit transfer



2. ábra: Interneten benyújtott fizetési kérelem kezdeményezése, jóváhagyása és teljesítése

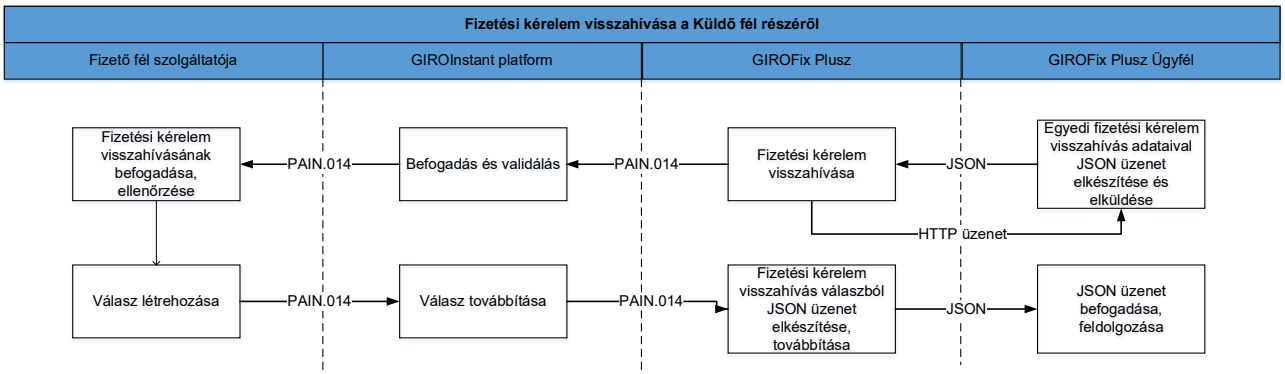
Steps in the process:

- ✓ The Client contracted to the GIROFix Plusz service submits the request to pay to GIRO Zrt. in the GIROFix Plusz standard JSON format. A GIROFix Plusz standard message can be submit using a secondary account identifier instead of the Payer's account number and name.
- ✓ GIRO Zrt. will notify the Client of the receipt of the message.
- ✓ The GIROFix Plusz system converts the GIROFix Plusz standard message into an individual request to pay message (pain.013) and sends it to the GIROInstant system, which forwards it to the Payer's Clearing Member or service provider. If the GIROFix Plusz standard message was submitted with secondary account identifier, GIRO Zrt. first performs a search in the central secondary account identifier database and submit the request to pay (pain.013) to the GIROInstant system with the account number and account holder name received in response to the search.
- ✓ Within 5 seconds the Payer's service provider (via GIRO Zrt.) confirms the receipt of the request to GIRO Zrt. with a pain.014 message (code: RCVD), which is notified to the GIROFix Plusz Client by the GIROFix Plusz system in the JSON file containing the primary response.
- ✓ If GIRO Zrt. determines that the response of the Payer's service provider is incorrect due to a formal error or non-compliance with business rules, no primary response to the request to pay will be sent.
- ✓ Upon approval by the Payer, the Payer's Clearing Member will initiate an instant credit transfer with the message pacs.008, provided the Payer has sufficient funds. The process is carried out as described in Chapter 3.1.
- ✓ The Payer's service provider informs GIRO Zrt. (with a message pain.014, ACCP feedback code) about the execution of the request to pay by the Payer after the successful instant transfer, which is reported by the GIROFix Plusz system to the GIROFix Plusz Client in the JSON file containing the secondary response.

The GIRO Zrt. shall not return to the Client the IBAN account number and the name of the account holder associated with the secondary account identifier obtained as a result of the search.

7.2 GIROFix Plusz recall of request to pay – positive flow

Figure 9. – GIROFix Plusz request to pay recall



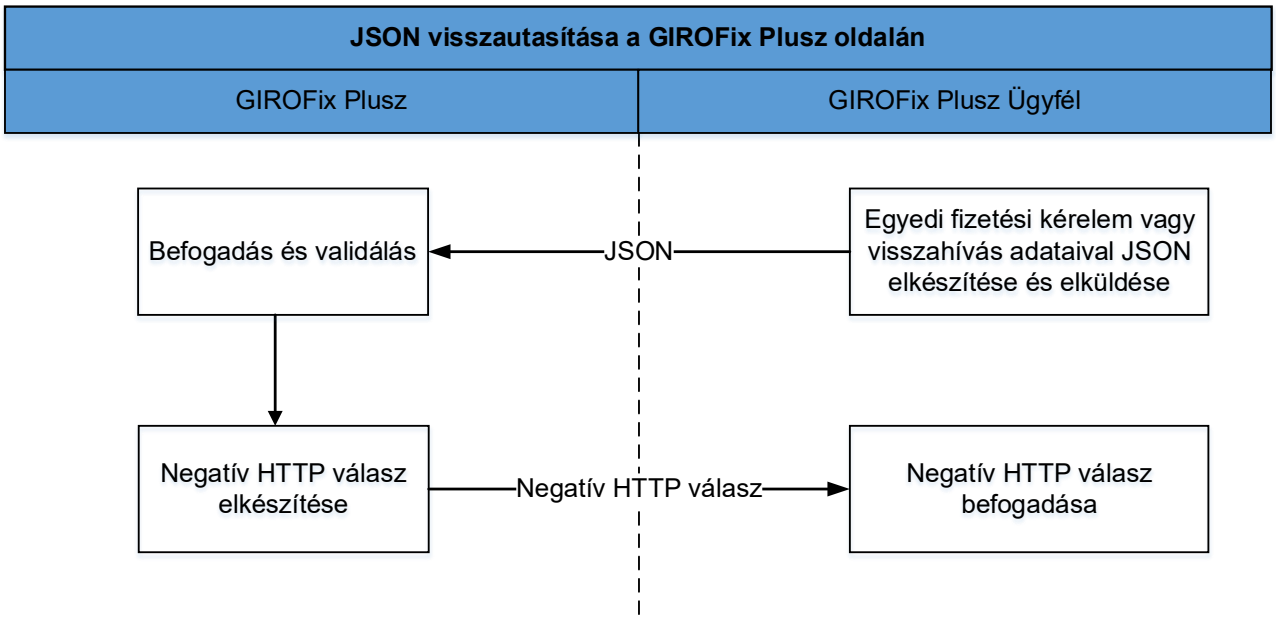
Steps in the process:

- ✓ The Client contracted to the GIROFix Plusz service submits the request to pay recall to GIRO Zrt. in the GIROFix Plusz standard JSON format. A GIROFix Plusz standard message can be submit using a secondary account identifier instead of the Payer's account number and name.
- ✓ GIRO Zrt. will notify the Client of the receipt of the message.
- ✓ The GIROFix Plusz system converts the GIROFix Plusz standard message into an individual request to pay recall message (pain.014) and sends it to the GIROInstant system, which forwards it to the Payer's Clearing Member or service provider. If the GIROFix Plusz standard message was submitted with secondary account identifier, GIRO Zrt. first performs a search in the central secondary account identifier database and submit the request to pay recall (pain.014) to the GIROInstant system with the account number and account holder name received in response to the search.
- ✓ The Payer's service provider notifies GIRO Zrt. with a message pain.014 as defined in Section 3.5 about the successful processing of the request to pay recall. The Reason Proprietary field contains the acceptance (ACC) or rejection of request to pay recall and the message identification (MsgId). The message can include an explanation of the rejection.
- ✓ The GIROFix Plusz system reports the GIROFix Plusz Client about the result of processing of the request to pay recall in the JSON file converted from the Payer's service provider response.

The GIRO Zrt. shall not return to the Client the IBAN account number and the name of the account holder associated with the secondary account identifier obtained as a result of the search.

7.3 Rejection in case of JSON failure

Figure 10. – Reject a bundle on the GIROFix site



- ✓ The GIROFix Plusz Client submits the request to pay or request to pay recall to GIRO Zrt. in the GIROFix Plusz standard message in JSON format.
- ✓ The GIRO Zrt. checks the JSON message and if it finds any formal or business error (structure, signature, certificate, submitter), the GIROFix Plusz system does not start converting the message, but returns the reason for rejection to the GIROFix Plusz Client.

7.4 Feedback sent by GIROFix Plusz system

- ➢ The following types of response messages are distinguished:

a) feedback of acceptance or rejection (http response),

b) delivery response message (primary response),

c) Payer's response to the request to pay (secondary response),

d) request to pay recall response message.

The system sent JSON response message from messages under b-d) to the GIROFix Plusz Client.

- ➢ Daily Activity Report: a statement of the calendar day's turnover, containing the following data of the request to pay and request to pay recall messages submitted to GIROInstant and its responses:
  - identification by GIROFix Plusz Client,
  - GIROInstant message ID (pain.013 or pain.014),

- amount,
- date of submission/receipt of GIROFix Plusz standard message,
- date of forward of pain.013 or pain.014,
- reason of rejection,
- status code and explanation in response message.

GIROINSTANT ELECTRONIC SIGNATURE GUIDE

BUSINESS TERMS AND CONDITIONS

ANNEX NO 28.

1 Introdcution

The GIROInstant Electronic Signature Guide describes the rules for electronic signatures and signature verification for GIROInstant customers.

The GIROInstant system uses the GIROLock PKI infrastructure and ruleset for electronic signatures. For issues and processes related to the GIROLock service and the Interbank Clearing System not covered in this document, the provisions of the Terms of Business of the service and their annexes shall prevail

1.1 Definitions

Basic concepts related to signatures are set out in the following table:

Expression	Description
PKI	Public Key Infrastructure
CA	Certificate Authority, Authentication Centre. The use of an authentication service for issuing, revoking and managing certificates.
GIROLock RootCA	GIROLock is a high-security primary authentication centre. It is identified by a self-signed RootCA certificate that does not change within its validity period. Several RootCAs can be held simultaneously by GIRO Zrt.
GIROLock CA	For GIROLock, certificates that can be used for signing are issued by an intermediary CA. It is identified by the CA certificate issued by the GIROLock RootCA. At the same time, GIRO may have several intermediate CAs, which may be under the same or different RootCAs.
Signature	The purpose of an electronic signature is to prove the authenticity (authenticity) and integrity (integrity) of the signed content. The signature verifier can verify that the signed content was signed by the intended sender and that it has reached him or her in unaltered form.
Certificate	An electronic certificate issued by GIRO Zrt. that links the signature verification data to the specified user or device.
Certificate for devices	A certificate for devices issued under the terms and conditions set out in the GIROLock Terms of Business, which can be used for electronic signatures.

Expression	Description
Certificate Chain	Certificate Chain, if the certificate in the signature is not issued directly by RootCA, a chain is formed. An intermediate certificate is trusted if it is vouched by the RootCA, i.e. the certificate of the intermediate CA was issued by the RootCA and has not been revoked in the meantime. The chain can theoretically have multiple elements, but in the case of GIROLock only one intermediate CA is currently possible.
DER	Distinguished Encoding Rules, X.509 PKI standard binary certificate format.
PKCS#7	An open key signature standard, RFC 2315 deals with version 1.5.
ASN.1	Formal descriptors of data types. (Abstract Syntax)
OID	Object identifier in the X.509 description language (Object IDentifier).
AIA	Authority Information Access field in the certificate

1.2 Referenced standards

Standard	Description
RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Defines the format of the X.509 (v3) compliant certificate and certificate revocation list. Replaces the previously used RFC 3280.
SHA2 algoritmus	For the purposes of GIROLock, as set out in the Code of Conduct, this means the SHA-512 algorithm.
Cryptographic Message Syntax (CMS) (electronically sign, digest, authenticate, or encryptarbitrary message content)	Defines the message signature and encryption format according to the CMS standard (based on PKCS#7). RFC 5652.

2 Purpose of the guide

The purpose of this guide is to set out the terms and conditions related to the GIROInstant services provided by GIRO Zrt,

- which provide uniformity and clarity in the generation and verification of electronic signatures used in the sending and receiving of authentic electronic messages between GIRO Zrt. and its customers,
- which, if fulfilled, allow electronic signatures to be considered valid between the parties that created the signature and the parties that verify the signature.

The requirements of the guidelines basically apply to the signatory and the verifying party, regulating the creation, interpretation, correct use and validation of electronic signatures, while specifying the technical and procedural requirements of the given business and transaction environment.

This guide only describes the rules for electronic signing and signature verification of messages and does not cover the TLS channel encryption used to use the GIROInstant service.

The certificates used for channel encryption (TLS) and signing (CMS) are different!

2.1 The principles used to develop the guide

1. The electronic signature can be created with the object authentication certificate issued to the GIROInstant service and its customers.
2. Renewal of certificates with the same key is not supported by GIRO Zrt.
3. The electronic signature does not need to be time-stamped.
4. The following cryptographic HASH function and encryption is used when generating electronic certificates for the PKI IT system used in the GIROInstant system:
    - o SHA-512 with RSA Encryption (SHA2RSA) SHA-512 (512 bits) HASH algorithm with 2048 or 4096 bit RSA keys.

3 Use of electronic signatures

3.1 Obligations and responsibilities for the creation and verification of electronic signatures

For technical messages distributed in the GIROInstant system and electronically signed, the signature shall be produced and verified by GIRO Zrt. and its customer in the manner described herein. For a detailed list of messages to be electronically signed, please refer to the chapter Electronic Signature of Message Types.

3.2 Signature creation rules

In message flows, electronic signatures must be created in accordance with and using the following rules:

1. The electronic signature should be created in the target hardware or software application that protects the keys appropriately, preferably at the point of data creation.
2. Only object authentication certificates issued by GIRO Zrt. for the GIROInstant service may be used for signature creation.
3. Messages signed with an invalid certificate (expired, revoked or suspended) or with a certificate not requested for the GIROInstant service are not considered authentic for the purposes of these guidelines and will not be accepted. The GIROInstant system will send an error message upon processing.
4. For signing, CMS and PKCS#7 standards must be used with the DER ASN.1 structure indicated below.
5. The signature shall use the SHA512 HASH algorithm (OID 2.16.840.1.101.3.4.2.3).
6. The SignedData and SignerInfo structures shall be imprinted (HASH) using the SHA-512 (OID 2.16.840.1.101.3.4.2.3) algorithm!
7. For the encryption of the SignerInfo structure footprint, use the RSA algorithm: rsaEncryption (OID 1.2.840.113549.1.1.1.1) or sha512WithRSAEncryption (OID 1.2.840.113549.1.1.13).
8. The RSA keys of the GIROLock certificates to be used for signing are 2048.
9. The SignedData structure must contain the original message to be signed (ContentInfo block), i.e. the use of the so-called attached format (OID 1.2.840.113549.1.7.1) is mandatory.
10. A SignedData structure may contain exactly one certificate (the signer) and one SignerInfo block.
11. The SignedAttributes block shall contain the following fields:

    - contentType (OID 1.2.840.113549.1.9.3)
    - signingTime (OID 1.2.840.113549.1.9.5)
    - cmsAlgorithmProtect (OID 1.2.840.113549.1.9.52)

- messageDigest (OID 1.2.840.113549.1.9.4)

12. Signed messages must be sent in Base64 encoding.

3.3 Verify of electronic signature

In message flows, electronic signatures should be verified by considering and applying the following rules:

1. By Base64 decoding the messages received, the DER ASN.1 structure is obtained.
2. Integrity and formal verification according to the signature scheme:
    a. Whether SHA-512 and RSA algorithms were used for signing.
    b. A SignerInfo and a certificate are attached.
    c. Whether the impressions were encrypted with the enclosed certificate using RSAEncryption or SHA-512 with RSA Encryption algorithm.
3. Verify the authenticity of the signing certificate:
    a. Whether the certificate is valid at the time of the inspection.
    b. Cryptographically verify that the issuer is one of the GIROLock CAs published by GIRO.
    c. Be prepared to expand/change the trusted CA list in the future.
4. Unlike other services and the GIROLock Code of Conduct, GIROInstant does not require full chain verification or CRL verification, as it requires the use of explicitly defined certificates.
5. It is necessary to check (against compromise) that the signing certificate belongs to the GIROInstant service (DN is identical to the one published by GIRO) and to be prepared for possible replacements that do not cause downtime (e.g. multiple accepted values, additions, deletions at runtime, etc.).

The following tables show the DN configuration of the signing certificates used by GIRO in GIROInstant:

GIROInstant banking test environment DN
GIRO test primary
CN = giroinst.signer.teszt.01
OU = GIROINSTANT
O = GIRO
C = HU
E = giroinst.signer.teszt.01@giroinstant.hu
GIRO test secondary (Reserve)
CN = giroinst.signer.teszt.02
OU = GIROINSTANT
O = GIRO
C = HU
E = giroinst.signer.teszt.02@giroinstant.hu

GIROInstant banking live environment DN
GIRO live primary
CN = giroinst.signer.eles.01
OU = GIROINSTANT
O = GIRO
C = HU
E = giroinst.signer.eles.01@giroinstant.hu
GIRO live secondary (Reserve)
CN = giroinst.signer.eles.02
OU = GIROINSTANT
O = GIRO
C = HU
E = giroinst.signer.eles.02@giroinstant.hu

6. 6. Live operational GIROLock CA certificates must be stored in a local certificate store (e.g. key store). The repository shall support the storage and acceptance of multiple operational CA certificates renewed with the same or different keys (with the same Subject, issued from the same Root CA) at the same time.

3.4 Managing certificates used for signing

In the case of a software key storage (file-less) certificate, it must be ensured that the key file cannot fall into unauthorised hands. Where possible, the certificate's private key should be password protected and the password should be protected in addition to the certificate file. The protection should be implemented in such a way that no person or application other than the application using the certificate has access to it.

4 The stucture of electronic signiture

The electronic signature format used is PKCS#7 (also known as CMS), for more information on PKCS standards see https://tools.ietf.org/html/rfc5652 or the URL http://www.pkiglobe.org/pkcs7.html.

For help with checking ASN structures, please visit http://lapo.it/asn1js/

According to the information received from the GIROInstant vendor, the Castle Crypto API (version 1.56) was used to implement the electronic signatures: https://www.bouncycastle.org/

The reference structure ASN1 of the GIROInstant message for SHA2 certificates and signatures is a GIROLock test certificate:

```
SEQUENCE {
  OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
  [0] {
    SEQUENCE {
      INTEGER 1
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER sha-512 (2 16 840 1 101 3 4 2 3)
          NULL
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)
        [0] {
          OCTET STRING
            64 69 72 0A 64 69 72 20 2F 6D 65 64 69 61 2F 6D
                    [ Another 15245 bytes skipped ]
          }
        }
      [0] {
        SEQUENCE {
          SEQUENCE {
            [0] {
              INTEGER 2
              }
            INTEGER 5015
            SEQUENCE {
              OBJECT IDENTIFIER
                sha512WithRSAEncryption (1 2 840 113549 1 1 13)
              NULL
              }
            SEQUENCE {
```

```
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER countryName (2 5 4 6)
        PrintableString 'HU'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationName (2 5 4 10)
        UTF8String 'GIRO'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER commonName (2 5 4 3)
        UTF8String 'GIROLock2_Test_CA'
        }
      }
    }
  SEQUENCE {
    UTCTime 18/06/2018 11:19:36 GMT
    UTCTime 18/07/2019 11:19:36 GMT
    }
  SEQUENCE {
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER countryName (2 5 4 6)
        PrintableString 'HU'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationName (2 5 4 10)
        UTF8String 'giro_zrt'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER
          organizationalUnitName (2 5 4 11)
        UTF8String 'People'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER
          emailAddress (1 2 840 113549 1 9 1)
        IA5String 'glapi-gl2-2048@mail.giro.hu'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER commonName (2 5 4 3)
        UTF8String 'glapi-gl2-2048'
        }
      }
    }
  SEQUENCE {
    SEQUENCE {
      OBJECT IDENTIFIER
        rsaEncryption (1 2 840 113549 1 1 1)
      NULL
      }
    BIT STRING, encapsulates {
      SEQUENCE {
        INTEGER
        00 AF 41 C1 AB 7A 48 A3 1E 8A E0 84 FC D5 02 7E
        BA BB 7F E8 C0 0A F7 B3 DD A6 55 C7 4E AC 8C 89
        15 FC 3E 0B 91 0D D8 4E A8 00 54 89 AD 8A E9 79
        70 3E 56 4B 18 7A C7 8D 08 6D 4D 9D 28 EC FF 1C
        B1 E0 26 4E 49 9B 58 6C A3 D9 6F 34 E4 84 67 28
        FA 91 75 6C EE D3 32 A9 01 14 89 82 2A 9D 46 22
        D3 2D C6 B6 D8 16 68 7B C5 A6 E5 33 FC 87 8F D1
        E7 D7 B1 44 68 E2 DB D8 87 5A A5 AC 14 F2 24 96
                [ Another 129 bytes skipped ]
        INTEGER 65537
        }
      }
    }
  [3] {
```

```
SEQUENCE {
  SEQUENCE {
    OBJECT IDENTIFIER basicConstraints (2 5 29 19)
    BOOLEAN TRUE
    OCTET STRING, encapsulates {
      SEQUENCE {}
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER subjectAltName (2 5 29 17)
    OCTET STRING, encapsulates {
      SEQUENCE {
        [1] 'glapi-gl2-2048@mail.giro.hu'
        }
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER
      authorityInfoAccess (1 3 6 1 5 5 7 1 1)
    OCTET STRING, encapsulates {
      SEQUENCE {
        SEQUENCE {
          OBJECT IDENTIFIER
            caIssuers (1 3 6 1 5 5 7 48 2)
          [6]
    'ldap://girolock.test.giro.hu/cn%3dgirolock2_test'
    '_ca_aia,o%3dgirolock2,c%3dhu?cACertificate?base?'
    '(objectClass=certificationAuthority)'
          }
        SEQUENCE {
          OBJECT IDENTIFIER
            caIssuers (1 3 6 1 5 5 7 48 2)
          [6]
    'ldap://girolock2.test.giro.hu/cn%3dgirolock2_tes'
    't_ca_aia,o%3dgirolock2,c%3dhu?cACertificate?base'
    '?(objectClass=certificationAuthority)'
          }
        SEQUENCE {
          OBJECT IDENTIFIER
            caIssuers (1 3 6 1 5 5 7 48 2)
          [6]
    'http://web.girolock.test.giro.hu/cert/gl2testca.'
    'p7c'
          }
        SEQUENCE {
          OBJECT IDENTIFIER
            caIssuers (1 3 6 1 5 5 7 48 2)
          [6]
    'http://web2.girolock.test.giro.hu/cert/gl2testca'
    '.p7c'
          }
        }
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER keyUsage (2 5 29 15)
    BOOLEAN TRUE
    OCTET STRING, encapsulates {
      BIT STRING 7 unused bits
        '1'B (bit 0)
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
    OCTET STRING, encapsulates {
      SEQUENCE {
        OBJECT IDENTIFIER
          clientAuth (1 3 6 1 5 5 7 3 2)
        }
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER
      authorityKeyIdentifier (2 5 29 35)
    OCTET STRING, encapsulates {
      SEQUENCE {
        [0]
    AE 1D AA 96 56 E1 90 D4 49 F2 B9 ED 9C 10 90 B7
    A7 AF 8A 77
        }
```

```
                }
              }
            SEQUENCE {
              OBJECT IDENTIFIER
                cRLDistributionPoints (2 5 29 31)
              OCTET STRING, encapsulates {
                SEQUENCE {
                  SEQUENCE {
                    [0] {
                      [0] {
                        [6]
              'ldap://girolock.test.giro.hu/cn%3dgirolock2_test'
              '_ca_cdp,o%3dgiro,c%3dhu?certificateRevocationLis'
              't?base?(objectClass=cRLDistributionPoint)'
                        }
                      }
                    }
                  SEQUENCE {
                    [0] {
                      [0] {
                        [6]
              'ldap://girolock2.test.giro.hu/cn%3dgirolock2_tes'
              't_ca_cdp,o%3dgiro,c%3dhu?certificateRevocationLi'
              'st?base?(objectClass=cRLDistributionPoint)'
                        }
                      }
                    }
                  SEQUENCE {
                    [0] {
                      [0] {
                        [6]
              'http://web.girolock.test.giro.hu/crl/gl2testca.c'
              'rl'
                        }
                      }
                    }
                  SEQUENCE {
                    [0] {
                      [0] {
                        [6]
              'http://web2.girolock.test.giro.hu/crl/gl2testca.'
              'crl'
                        }
                      }
                    }
                  }
                }
              SEQUENCE {
                OBJECT IDENTIFIER
                  subjectKeyIdentifier (2 5 29 14)
                OCTET STRING, encapsulates {
                  OCTET STRING
                0C 3C 4D E2 60 BE EE FE 7B A6 60 D3 62 7B A3 91
                1F 97 3C AA
                  }
                }
              }
            }
          }
        SEQUENCE {
          OBJECT IDENTIFIER
            sha512WithRSAEncryption (1 2 840 113549 1 1 13)
          NULL
          }
        BIT STRING
          66 3E 8C C6 C4 56 C2 C2 B3 5B 97 BF 83 1F 24 E7
          02 91 29 8B 2A EF 2E 74 E5 DC 24 5F BF EE EB E9
          47 AD 79 29 C2 6E D2 E7 5D 7D D4 D1 4C D7 56 3B
          92 E7 BF 26 9B 58 C7 FE 99 35 8A 66 EB 62 3E 57
          9D 27 9D 5B CA 90 E5 B7 96 26 8E 6B BA 80 C7 9D
          86 09 CA 19 FA 21 6D A5 FD 4E 91 EA 6C 34 B1 D6
          D3 15 CC D8 6F 2A 6D 41 56 23 C7 68 1C 85 50 A1
          83 AB 91 44 13 55 FD 99 4A C6 03 9D 59 9D EC 7B
                  [ Another 384 bytes skipped ]
        }
      }
    SET {
      SEQUENCE {
        INTEGER 1
```

```
SEQUENCE {
  SEQUENCE {
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER countryName (2 5 4 6)
        PrintableString 'HU'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationName (2 5 4 10)
        UTF8String 'GIRO'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER commonName (2 5 4 3)
        UTF8String 'GIROLock2_Test_CA'
        }
      }
    }
  INTEGER 5015
  }
SEQUENCE {
  OBJECT IDENTIFIER sha-512 (2 16 840 1 101 3 4 2 3)
  NULL
  }
[0] {
  SEQUENCE {
    OBJECT IDENTIFIER contentType (1 2 840 113549 1 9 3)
    SET {
      OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER signingTime (1 2 840 113549 1 9 5)
    SET {
      UTCTime 22/08/2018 15:22:29 GMT
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER '1 2 840 113549 1 9 52'
    SET {
      SEQUENCE {
        SEQUENCE {
          OBJECT IDENTIFIER
            sha-512 (2 16 840 1 101 3 4 2 3)
          NULL
          }
        [1] {
          OBJECT IDENTIFIER
            sha512WithRSAEncryption (1 2 840 113549 1 1 13)
          NULL
          }
        }
      }
    }
  SEQUENCE {
    OBJECT IDENTIFIER
      messageDigest (1 2 840 113549 1 9 4)
    SET {
      OCTET STRING
        D6 32 43 A3 A2 1B 0A 38 D9 3F 0F 73 3F E0 76 D2
        5A 6A F0 FF DD EA 13 21 46 EB 6E B4 70 AB 73 BE
        51 29 89 EF 98 38 64 A7 A8 86 9F 97 C2 EC 89 98
        A9 2C 11 44 FD 92 14 45 97 F9 A6 A0 48 74 20 0E
      }
    }
  }
SEQUENCE {
  OBJECT IDENTIFIER
    sha512WithRSAEncryption (1 2 840 113549 1 1 13)
  NULL
  }
OCTET STRING
  83 FF D1 A0 57 21 38 53 F3 8B 0E 98 4D 45 6C 69
  53 DF 1D 89 47 36 64 EB AD 28 CC C4 0C B0 E0 FB
  DC BC FF 1A E6 96 7A EF 00 D3 1A 46 C8 51 00 30
  AD 3C 83 63 59 CB BA ED 6D 1C 75 59 46 EC B9 3E
  4D 4D 19 71 C4 B2 A6 CD A2 FA 12 5A DF 65 02 E7
```

```
            F4 19 32 77 E9 4F 49 58 5A 6F C1 76 ED 07 E4 87
            91 30 0D D9 5C C8 92 9B E4 0E 83 58 FE 2F E3 9A
            75 AA C8 7A 7B 0D 77 E0 51 F2 D5 34 22 AD 4A 41
                    [ Another 128 bytes skipped ]
          }
        }
      }
    }
  }
```

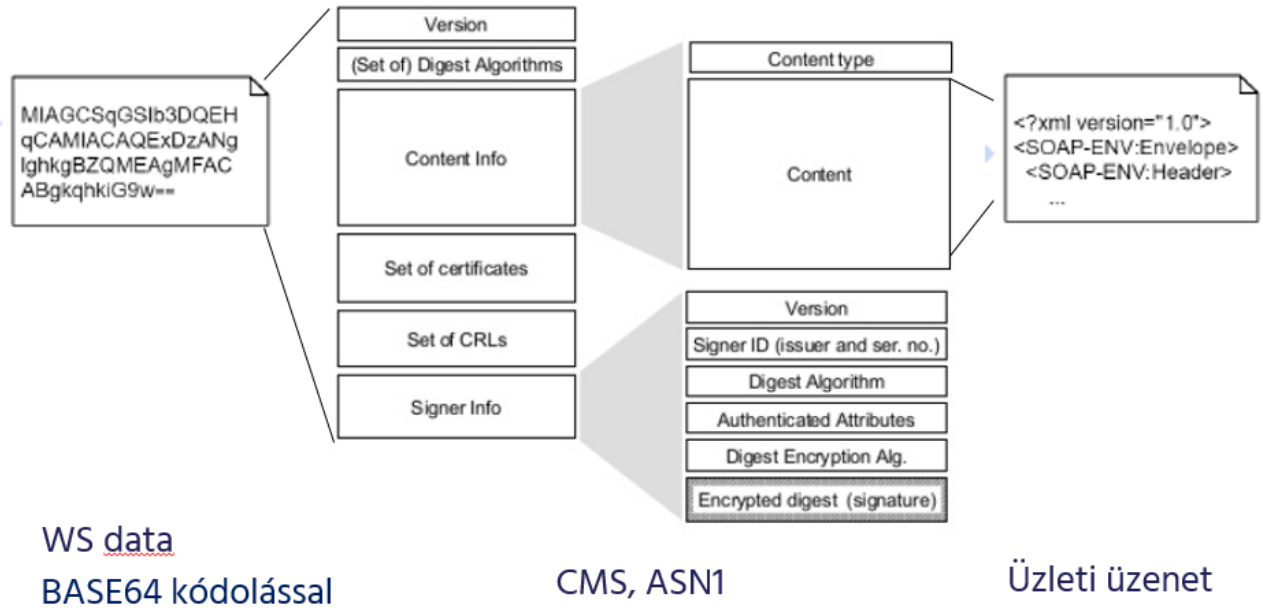
A further example is given in chapter 5.3.1 of this document.

5 Electronic signature of message types

The implementation of an electronic signature is required for messages related to the following services:

- HCT Inst - instant transfer
- NAS - Maintenance and retrieval of secondary account identifiers
- RTP - Request to pay service

The attached figure shows the steps of message generation for a SOAP message:



If the business message is a REST based WEB service (WS), then the REST response is embedded in the "Content" field, as appropriate.

The following chapters describe, by message type, which messages require a digital signature.

5.1 The method of sending the message, and its document

The way GIROInstant messages are exchanged on a webservice basis is described in the WSDL implementation guide (Participants and GIROInstant message exchange.pdf), available on GIROnline.

When sending a webservice message, the type of message sent must be defined in the HTTP header according to the following specification. The data must be passed to the webservice process in BASE64 encoded format.

The GIROInstant system checks the message content according to the type defined in the Accept header.

5.1.1 HCT Inst – Instant credit transfer

Message Type	HTTP header	HTTP header value
Unsigned	Accept	application/vnd.realtime247.**sct**-giro-v1+xml
	Content-Type	text/xml; charset="utf-8"
Signed	Accept	application/vnd.realtime247.**sct**-giro-v1+cms
	Content-Type	text/plain; charset="utf-8"

5.1.2 NAS – maintenance and retrieval of secondary account identifiers

Üzenet típusa	HTTP header	HTTP header value
Unsigned	Accept	application/vnd.realtime247.**nas**-giro-v1+xml
	Content-Type	text/xml; charset="utf-8"
Signed	Accept	application/vnd.realtime247.**nas**-giro-v1+cms
	Content-Type	text/plain; charset="utf-8"

5.1.3 RTP – Request to pay

Message type	HTTP header	HTTP header value
Unsigned	Accept	application/vnd.realtime247.**vas**-giro-v1+xml
	Content-Type	text/xml; charset="utf-8"
Signed	Accept	application/vnd.realtime247.**vas**-giro-v1+cms
	Content-Type	text/plain; charset="utf-8"

5.2 Fault management

5.2.1 TLS Channel error codes

The GIROInstant system sends a 401 status code and a "CMS Signing Error" message to the client in the TLS channel in case of an error during the electronic signature verification.

HTTP code	Description	HTTP header value
401	Unauthorised access	The verification of the message received by the GIROInstant system failed.

5.2.2 "Processingfault" error codes after error-free processing of CMS package

In the case of asynchronous communication, XML error codes after a successful CMS packet (http202) are also electronically signed and returned on a new communication channel.

5.3 List of message types

5.3.1 HCT Inst – Instant credit transfer

The HCT Inst interface provides the implementation of the instant transfer service via HTTPS based asynchronous webservice communication. Server- and client-side webservices need to be built by the connecting system member.

The method for sending messages is described in Chapter 4 of the WSDL Implementation Guide (Participants and GIROInstant message exchange.pdf).

The table below lists the messages to be electronically signed during an instant transfer:

Message	Direction of the Message	Signatory Party
pacs.008	initiator -> GIROInstant	initiator
pacs.008 (forwarded)	GIROInstant -> beneficiary	GIROInstant
pacs.004	initiator party -> GIROInstant	initiator
pacs.004 (forwarded)	GIROInstant -> beneficiary	GIROInstant
pacs.002	GIROInstant -> beneficiary	GIROInstant

pacs.002	GIROInstant -> initiator	GIROInstant
pacs.002	beneficiary -> GIROInstant	beneficiary
pacs.028	initiator -> GIROInstant	initiator
camt.056	initiator -> GIROInstant	initiator
camt.056 (forwarded)	GIROInstant -> beneficiary	GIROInstant
camt.029	beneficiary -> GIROInstant	beneficiary
camt.029 (forwarded)	GIROInstant -> initiator	GIROInstant

Signature example files for SCT messages in GIROInstant (RT24/7):

P0838488_P8000_standard_ACCP_pacs008.xml - XML-formatted message sent by GIRAHUH0 (by GIRO test bank).

P0838488_P8000_st
andard_ACCP_pacs0

P0838488_P8000_standard_ACCP_pacs008_signed.txt - Previous message in signed form

P0838488_P8000_st
andard_ACCP_pacs0

P0838488_RTP24720181113000000000000001_pacs002_signed.txt - RT24/7 reply to previous message signed (rejected with timeout)

P0838488_RTP24720
18111300000000000

P0838488_RTP24720181113000000000000001_pacs002.xml - Previous message restored to XML format

P0838488_RTP24720
18111300000000000

5.3.2 NAS – maintenance and retrieval of secondary account identifiers

The NAS interface provides the implementation of the secondary identity management service via REST-based HTTPS synchronous webservice communication. Server- and client-side web services must be built by the connecting system member.

The method of sending messages is described in Chapter 6 of the WSDL Implementation Guide (Participants and GIROInstant message exchange.pdf).

The table below lists the messages to be electronically signed during the maintenance and retrieval of secondary identifiers:

Message	Direction of the Message	Signatory party
Registration message	account holder -> GIROInstant	account holder
Registration reply	GIROInstant -> account holder	GIROInstant
Search	szolgáltató -> GIROInstant	*not signed*
Search reply	GIROInstant -> Service Provider	GIROInstant
Query	account holder -> GIROInstant	*not signed*
Query reply	GIROInstant -> account holder	GIROInstant
Cancel	the account holder initiating the cancellation -> GIROInstant	account holder
Cancel reply	GIROInstant -> the account holder initiating the cancellation	GIROInstant
Cancellation information	GIROInstant -> the account manager initiating the original registration	GIROInstant

5.3.3 RTP - Request to pay service

The RTP interface provides the implementation of the request to pay service via HTTPS based asynchronous webservice communication. Server- and client-side web services must be established by the connecting system member.

The method for sending messages is described in Chapter 5 of the WSDL Implementation Guide (Participants and GIROInstant message exchange.pdf).

The table below lists the messages to be electronically signed when using the request to pay service:

Message	Directon of the Message	Signatory Party
pain.013	initiator -> GIROInstant	initiator
pain.013 (forwarded)	GIROInstant -> paying party	GIROInstant
pain.014	paying party -> GIROInstant	paying party
pain.014 (forwarded)	GIROInstant -> initiator	GIROInstant
pain.014 (GIROInstant)	GIROInstant -> initiator	GIROInstant

6 Testing electronic signatures and CMS packages

A JavaScript file for testing electronic signatures has been provided as part of the electronic signature guide and testing aids package. In addition to the script, the package contains the raw and signed example messages, the certificates required to verify the messages, the signing, intermediate and root certificates required to sign any message, and the default key store used by the script.

The script can be used to verify pre-signed test pacs.002 and pacs.008 messages, or to sign and base64 encode your own messages according to specification and then verify them.

6.1 Restrictions

The use of test scripts is subject to the following constraints, unlike in live operation:

1. The script is designed for the needs and purposes of this testing, and is not intended for use in a live operational environment.
2. The test script does not provide valid results for performance measurements.
3. The "byte-buffer" solution used is not suitable for checking large packets - the use of streams is recommended instead.
4. Verification of the authenticity of the embedded certificate can only be done by checking the contents of the keystore ("-ct" option).

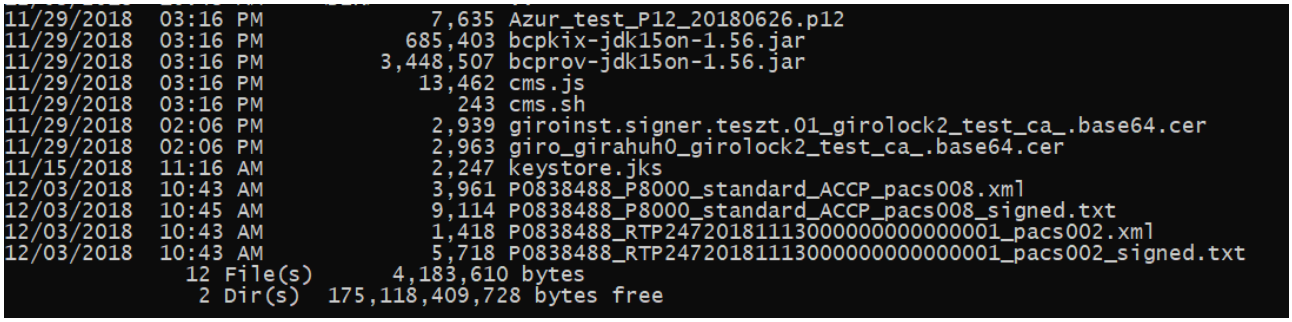
5. When checking messages, it is necessary to ensure that line breaks in base64 encoded bement files correspond to unix end of line characters ("CR LF" instead of "LF" control characters).

6.2 Test package content

The delivered CMS.zip test package contains the following items:

cms.js	Test JavaScript for signature and signature verification. Requires JDK 1.8+ (Nashorn engine) to run.
cms.sh	Unix shell script calling cms.js (for ease of Unix use)
keystore.jks	Default keyring used by the test script (password: "changeit").
bcpkix-jdk15on-1.56.jar	Files containing the cryptolib needed for the script to work.
bcprov-jdk15on-1.56.jar	
Azur_test_P12_20180626.p12	Key store file containing test signing keys and certificates (password: "Azur.test.P12").
giro_girahuh0_girolock2_test_ca_.base64.cer	certificate to be used to verify pacs.002 test message.
giroinst.signer.teszt.01_girolock2_test_ca_.base64.cer	certificate to be used to verify pacs.008 test message.
P0838488_RTP24720181113000000000000001_pacs002.xml	Test pacs.002 message raw version.
P0838488_P8000_standard_ACCP_pacs008.xml	Test pacs.008 raw version of message.
P0838488_RTP24720181113000000000000001_pacs002_signed.txt	Test pacs.002 message signed and encoded version.

P0838488_P8000_standard_ACCP_pacs008_signed.txt	Test signed and encoded version of message pacs.008.



6.3 Use of the package

To run the script, you need JDK 1.8+ and the included Bouncy Castle Crypto API (1.56). The script can be executed with the jjs command with the following parameters:

Usage:

*$JAVA_HOME/bin/jjs *

*-cp "bcpkix-jdk15on-1.56.jar:bcprov-jdk15on-1.56.jar" *

cms.js -- [options...] [data]

Options:

-s, --sign	*Sign the message. Either -s or -u option must be specified.*
-u, --unsign	*Verify the signed message and extract the signed contents. Either -s or -u option must be specified.*
-ct	*Upon verifying a signed message, check that the embedded public key certificate is trusted.*
-z	*GZIP-compress the message before signing. GZIP-Decompress the message after unsigning.*
-a <algorithm>	*The signature algorithm. Defaults to 'SHA512withRSA'.*
-f <file>	*File with content to (un)sign. Alternative to specifying data as last argument.*
-o <file>	*Write result to file instead of stdout.*
-ks <keystore>	*KeyStore file. Defaults to 'keystore.jks'.*

-kspwd <password> KeyStore password. Defaults to 'changeit'.

-ska <alias> Alias of the signing key in the KeyStore. Defaults to 'signtest'.

-skpwd <password> Private signing key password. Defaults to 'changeit'.

-v, --verbose Make the operation more talkative.

-h, --help Print usage.

Data: The actual data to (un)sign. Not specified when -f is used.

```
Usage:
  $JAVA_HOME/bin/jjs -cp bcpkix-jdk15on-1.56.jar:bcprov-jdk15on-1.56.jar cms.js -- [options...] [data]
Options:
-s, --sign         Sign the message. Either -s or -u option must be specified.
-u, --unsign       Verify the signed message and extract the signed contents. Either -s or -u option must be specified.
-ct                When verifying a signed message, also check that the embedded public key certificate is trusted.
-z                 GZIP-compress the message before signing. GZIP-Decompress the message after unsigning.
-a <algorithm>     The signature algorithm. Defaults to 'SHA512withRSA'.
-f <file>          File with content to (un)sign. Alternative to specifying data as last argument.
-o <file>          Write result to file instead of stdout.
-ks <keystore>     Keystore file. Defaults to 'keystore.jks'.
-kspwd <password> Keystore password. Defaults to 'changeit'.
-ska <alias>       Alias of the (private) signing key in the keystore. Defaults to 'signtest'.
-skpwd <password> Private signing key password. Defaults to 'changeit'.
-v, --verbose      Make the operation more talkative.
-h, --help         Print usage.
Data: The actual data to (un)sign. Not specified when -f is used.
```

6.4 Checking signed messages

The sample messages pacs.002 (P0838488_RTP24720181113000000000000000001_pacs002_signed.txt) and pacs.008 (P0838488_P8000_standard_ACCP_pacs008_signed.txt) included in the package can be checked for signature as follows.

6.4.1 Import cerfificate to be used for verification

The first step is to import the certificates (giroinst.signer.test.01_girolock2_test_ca_.base64.cer and giro_girahuh0_girolock2_test_ca_.base64.cer) containing the public part of the key pair used to sign the pacs.002 and pacs.008 messages into the key store:

pacs.002:

```
keytool -v -import -alias giroinst.signer.teszt.01_girolock2_test_ca -file
giroinst.signer.teszt.01_girolock2_test_ca_.base64.cer -keystore
keystore.jks
```

```
C:\cms>keytool -v -import -alias giroinst.signer.teszt.01_girolock2_test_ca -file giroinst.signer.teszt.01_girolock2_test_ca_.base64.cer -keystore keystore.jks
Enter keystore password:
Owner: CN=giroinst.signer.teszt.01, EMAILADDRESS=giroinst.signer.teszt.01@giroinstant.hu, OU=GIROINSTANT, O=GIRO, C=HU
Issuer: CN=GIROLock2_Test_CA, O=GIRO, C=HU
Serial number: 19de
Valid from: Tue Oct 09 22:28:19 CEST 2018 until: Fri Nov 08 21:28:19 CET 2019
Certificate fingerprints:
         MD5:  2A:1D:D2:72:54:DF:48:E7:03:A6:F5:F6:ED:6C:85:7B
         SHA1: AF:A8:E6:76:A8:C0:6C:83:8B:25:77:26:26:AA:C4:13:88:97:67:F3
         SHA256: 6B:3B:86:9D:AB:1A:73:C1:44:51:3C:25:E7:E2:35:EF:62:E7:6D:98:5F:17:8E:8B:56:A4:53:A6:B8:A6:A9:F7
Signature algorithm name: SHA512withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
   accessMethod: caIssuers
   accessLocation: URIName: ldap://girolock.test.giro.hu/cn%3dgirolock2_test_ca_aia,o%3dgirolock2,c%3dhu?cACertificate?base?(objectClass=certificationAuthority)

,
   accessMethod: caIssuers
   accessLocation: URIName: ldap://girolock2.test.giro.hu/cn%3dgirolock2_test_ca_aia,o%3dgirolock2,c%3dhu?cACertificate?base?(objectClass=certificationAuthority)

,
   accessMethod: caIssuers
   accessLocation: URIName: http://web.girolock.test.giro.hu/cert/gl2testca.p7c

,
   accessMethod: caIssuers
   accessLocation: URIName: http://web2.girolock.test.giro.hu/cert/gl2testca.p7c
]
]


#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: AE 1D AA 96 56 E1 90 D4   49 F2 B9 ED 9C 10 90 B7  ....V...I.......
0010: A7 AF 8A 77                                        ...w
]
]

#3: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#4: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
     [URIName: ldap://girolock.test.giro.hu/cn%3dgirolock2_test_ca_cdp,o%3dgiro,c%3dhu?certificateRevocationList?base?(objectClass=cRLDistributionPoint)]
  DistributionPoint:
     [URIName: ldap://girolock2.test.giro.hu/cn%3dgirolock2_test_ca_cdp,o%3dgiro,c%3dhu?certificateRevocationList?base?(objectClass=cRLDistributionPoint)]
, DistributionPoint:
     [URIName: http://web.girolock.test.giro.hu/crl/gl2testca.crl]
, DistributionPoint:
     [URIName: http://web2.girolock.test.giro.hu/crl/gl2testca.crl]
]]

#5: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
]

#6: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  RFC822Name: giroinst.signer.teszt.01@giroinstant.hu
]

#7: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 87 FF A4 F3 C0 49 0C 11   FD D4 F1 80 B3 B1 46 BE  .....I........F.
0010: EF 49 A8 9A                                        .I..
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing keystore.jks]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore keystore.jks -destkeystore keystore.jks -deststoretype pkcs12".

C:\cms>
```

pacs.008:

```
keytool -v -import -alias giro_girahuh0_girolock2_test_ca -file
giro_girahuh0_girolock2_test_ca_.base64.cer -keystore keystore.jks
```

```
C:\cms>keytool -v -import -alias giro_girahuh0_girolock2_test_ca -file giro_girahuh0_girolock2_test_ca_.base64.cer -keystore keystore.jks
Enter keystore password:
Owner: CN=GIRO-GIRAHUH0, EMAILADDRESS=GIRO-GIRAHUH0@giro.hu, OU=GIROINSTANT, O=GIRO, C=HU
Issuer: CN=GIROLock2_Test_CA, O=GIRO, C=HU
Serial number: 1865
Valid from: Fri Sep 21 12:35:28 CEST 2018 until: Mon Oct 21 12:35:28 CEST 2019
Certificate fingerprints:
         MD5:  86:FC:2B:B1:40:DA:46:EA:84:07:CF:31:75:45:11:02
         SHA1: 71:51:3F:44:F5:CA:B0:DA:45:E2:93:87:E0:E5:F2:D9:4C:AC:59:20
         SHA256: 45:B0:28:4A:F4:EE:15:F8:6E:1E:E6:36:D3:30:61:EF:53:C4:BF:46:62:10:24:B5:80:F5:C7:3F:DA:C8:C5:DE
Signature algorithm name: SHA512withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
   accessMethod: caIssuers
   accessLocation: URIName: ldap://girolock.test.giro.hu/cn%3dgirolock2_test_ca_aia,o%3dgirolock2,c%3dhu?cACertificate?base?(objectClass=certificationAuthority)

,
   accessMethod: caIssuers
   accessLocation: URIName: ldap://girolock2.test.giro.hu/cn%3dgirolock2_test_ca_aia,o%3dgirolock2,c%3dhu?cACertificate?base?(objectClass=certificationAuthority)

,
   accessMethod: caIssuers
   accessLocation: URIName: http://web.girolock.test.giro.hu/cert/gl2testca.p7c

,
   accessMethod: caIssuers
   accessLocation: URIName: http://web2.girolock.test.giro.hu/cert/gl2testca.p7c
]
]


#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: AE 1D AA 96 56 E1 90 D4   49 F2 B9 ED 9C 10 90 B7  ....V...I.......
0010: A7 AF 8A 77                                        ...w
]
]

#3: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#4: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
     [URIName: ldap://girolock.test.giro.hu/cn%3dgirolock2_test_ca_cdp,o%3dgiro,c%3dhu?certificateRevocationList?base?(objectClass=cRLDistributionPoint)]
  DistributionPoint:
     [URIName: ldap://girolock2.test.giro.hu/cn%3dgirolock2_test_ca_cdp,o%3dgiro,c%3dhu?certificateRevocationList?base?(objectClass=cRLDistributionPoint)]
, DistributionPoint:
     [URIName: http://web.girolock.test.giro.hu/crl/gl2testca.crl]
, DistributionPoint:
     [URIName: http://web2.girolock.test.giro.hu/crl/gl2testca.crl]
]]

#5: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#6: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
]

#7: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL client
   SSL server
]

#8: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: GIRO-GIRAHUH0
  RFC822Name: GIRO-GIRAHUH0@giro.hu
]

#9: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E9 6A 73 97 C5 54 9A BF   8C DE 4C 3A EA 96 4A D9  .js..T....L:..J.
0010: 27 1E 1D 78                                        '..x
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing keystore.jks]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore keystore.jks -destkeystore keystore.jks -deststoretype pkcs12".
```

6.5 Message checking

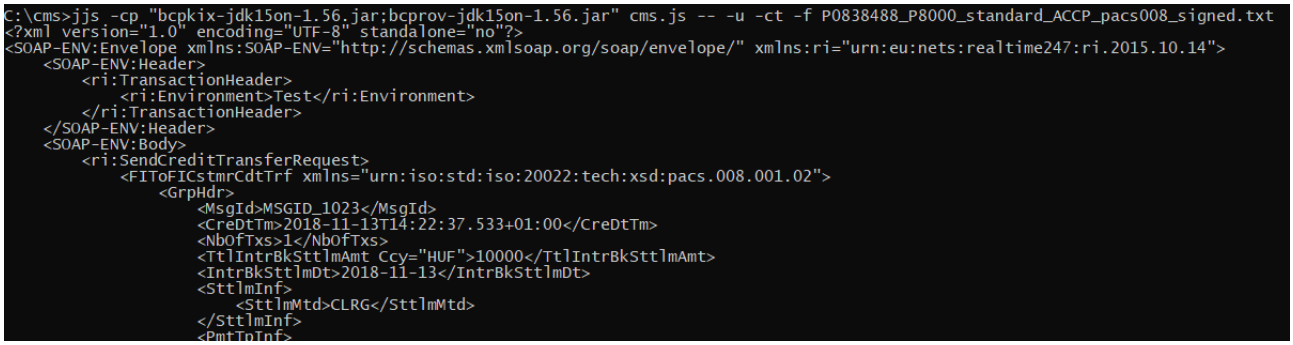
Once imported, verification and unpacking of messages can be performed using the imported certificates along the following commands (it is worth checking that the messages contain the correct line breaks):

pacs.002:

```
jjs -cp "bcpkix-jdk15on-1.56.jar;bcprov-jdk15on-1.56.jar" cms.js --
-u -ct -f P0838488_RTP24720181113000000000000001_pacs002_signed.txt
```

pacs.008:

```
jjs -cp "bcpkix-jdk15on-1.56.jar;bcprov-jdk15on-1.56.jar" cms.js --
-u -ct -f P0838488_P8000_standard_ACCP_pacs008_signed.txt
```



If the check and unpacking is successful, the original message will be displayed. The content of the messages must match the content of P0838488_RTP24720181113000000000000000001_pacs002.xml and P0838488_P8000_standard_ACCP_pacs008.xml in the package.

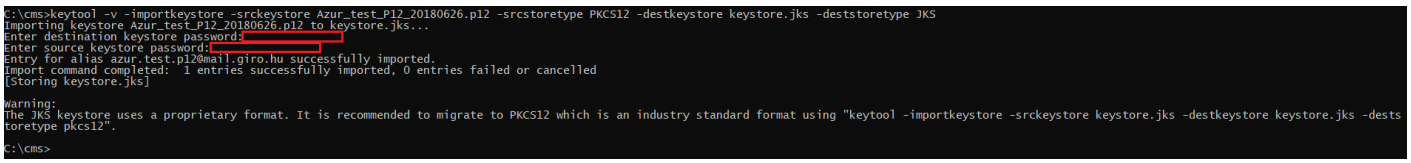
6.6 Production of signed message packets

The script also allows you to sign and verify your own "to be sent" messages, as follows.

6.6.1 Import a cerfificate to be used for signing and verification

The first step is to import the keystore (keystore.jks) containing the certificates and keys to be used for signing and verifying the message to be sent (Azur_test_P12_2018.0626.p12, password: "Azur.test.P12") into the keystore used by the script:

```
keytool -v -importkeystore -srckeystore Azur_test_P12_20180626.p12 -
srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS
```

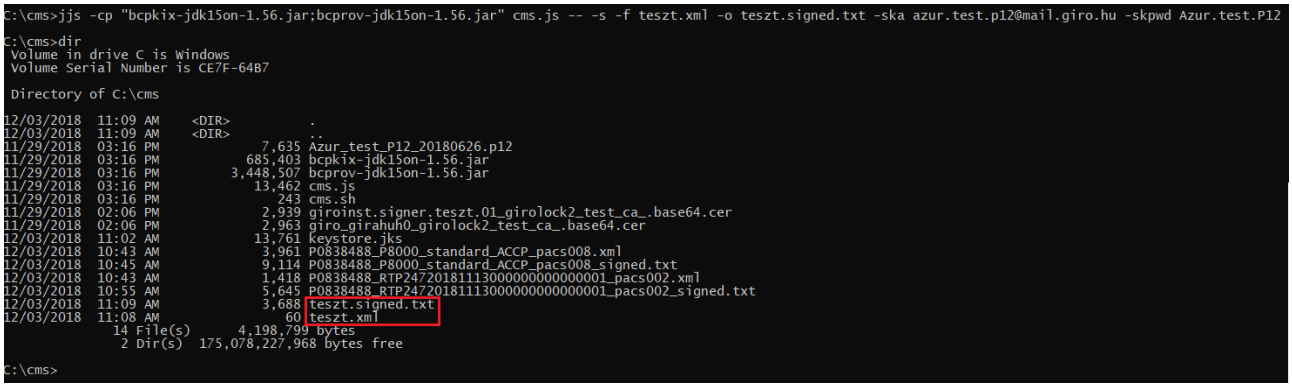


6.6.2 Generation of message packet

After importing, the test packet to be submitted from any test message can be signed and base64 encoded as follows (with azur.test.p12@mail.giro.hu alias and "Azur.test.P12" password):

For arbitrary test.xml file:

```
jjs -cp "bcpkix-jdk15on-1.56.jar;bcprov-jdk15on-1.56.jar" cms.js -- -s -f teszt.xml -o teszt.signed.txt -ska azur.test.p12@mail.giro.hu -skpwd Azur.test.P12
```

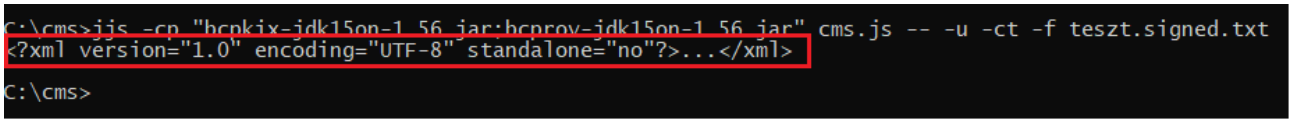


If the generation is successful, the signed message is saved in the file test.signed.txt.

6.6.3 Message Checking

Finally, the verification of the message packet and the extraction of the original message can be done as follows (at the same time, the existence of the public key embedded in the message in the keystore for verification is checked):

```
jjs -cp "bcpkix-jdk15on-1.56.jar;bcprov-jdk15on-1.56.jar" cms.js -- -u -ct -f teszt.signed.txt
```



If the check and unpacking is successful, the original message is displayed on the screen.

LIQUIDITY MANAGEMENT GUIDE

BUSINESS TERMS AND CONDITIONS

ANNEX NO 29.

1 Collective account and instant settlement account

Under the GIROInstant service, clearing and settlement is carried out on a pre-funded basis, continuously, every day of the year, in real time, on a payment transaction by payment transaction basis, to the debit/credit of the the instant settlement accounts in GIROInstant, by funding the collective account held with the MNB and jointly owned by the Clearing Members. The balance of the instant settlement account shall not fall below 0.

The ownership of the balance on the collective account among the Clearing Members shall be determined by the current balance on the instant settlement accounts.

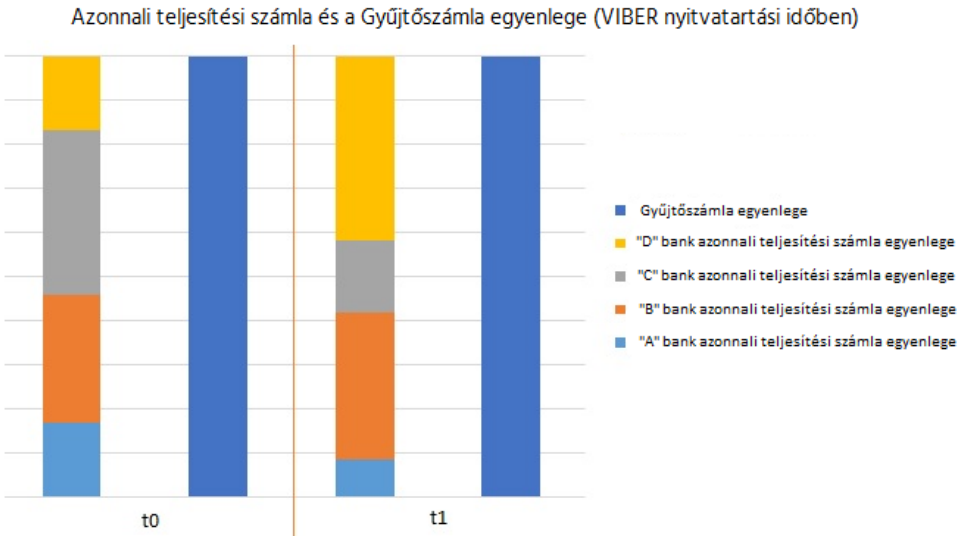
The clearing and settlement of instant transactions on the instant settlement accounts is continuous and the balance of the collective account does not change as a result of the cleared and settled transactions.

Transfers to the collective account may only be initiated via the GIROInstant platform by Clearing Members with an instant settlement account.

The balance of the Clearing Member instant settlement account will be adjusted in the same way as the transfer settled on the collective account. It follows from this, and from the closed nature of the GIROInstant platform, that the sum of the balances of the instant settlement accounts - at VIBER opening time - is equal to the balance of the collective account. The figure below shows the balances of the instant settlement accounts at t^0 and t^1. The balance on the collective account is unchanged, i.e. the same at t^0 and t^1:

	t^0 Date	**t^1 Date**
"A" bank instant settlement account balance	20	10
"B" bank instant settlement account balance	35	40
"C" bank instant settlement account balance	45	20
"D" bank instant settlement account balance	20	50
Collective account balance	120	120

Figure 1. - - Instant Settlement Account and Collective Account balance (during VIBER opening hours)



The balance of the instant settlement accounts may change during the transfer of funds or the settlement of instant transactions.

The available balance of an instant settlement account consists of 2 factors:

Available balance = Credit Line + settled net turnover (net positon)

Net cleared turnover is the difference between cleared credits (amounts received) and cleared debits (amounts sent) related to the instant settlement account. At the close of each reconciliation cycle (every hour), the value of the net cleared turnover is transferred to the Credit Line and reset to zero (so that the available balance of the instant settlement account and the Credit Line at close will be equal, but the available balance of the instant settlement account will not change at the close of the reconciliation cycle).

Funds transfers in favour of the collective account increase the value of the Credit Line, while funds transfers against the collective account decrease the value of the Credit Line. Funds transfers cannot reduce the value of the Credit Line below 0, i.e. only transfers that do not exceed the current value of the Credit Line can be executed. Transfers that would reduce the value of the Credit Line below 0 will be rejected.

As a result, the total amount that may be transferred from the collective account to the Clearing Member's bank account within a Reconciliation Cycle shall not exceed the balance of the Clearing Member's Instant Settlement Account at the beginning of the Reconciliation Cycle, adjusted by the amount of the transfers made by the Clearing Member to the collective account. In other words, since the settled incoming instant transactions executed during a given

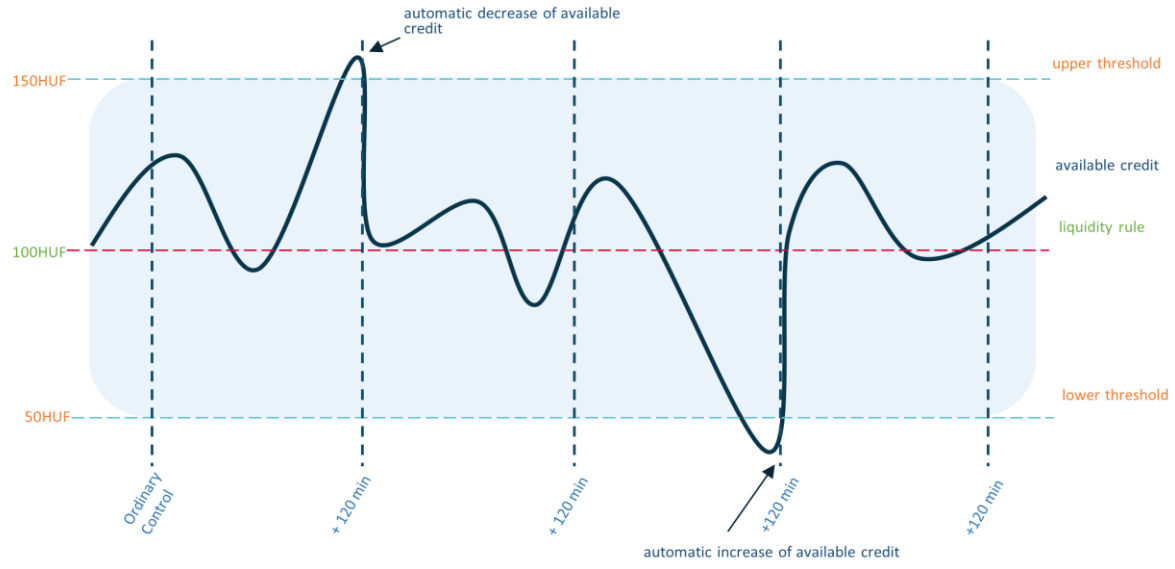
hour first adjust the net position (and not the Credit Line, from which funds may be transferred, if applicable), no funds in excess of the Credit Line may be transferred until the next reconciliation cycle. (Of course, as the settled net turnover is transferred to the Credit Line at the end of the reconciliation cycle, this amount will also be transferable during VIBER operating hours, provided the above limit is not exceeded.)

If the funds transfer request is rejected in VIBER for any reason, the actual cover adjustment of the Clearing Member will not be made in the GIROInstant platform. The GIROInstant platform ensures that only one valid transfer request should be in progress for a given Clearing Member at a time.

2 GIROINSTANT'S AUTOMATIC LIQUIDITY MANAGEMENT PROCESS

The GIROInstant platform has an automatic liquidity management function: following an ordinary control or extraordinary control, it automatically initiates a funds transfer if thresholds are exceeded.

Figure 2. – Change in Instant settlement account balance



2.1 LIQUIDITY PARAMETERS

Clearing members can use the following parameters and functions to customise liquidity management:

- Setting the reference level value (Liquidity rule)

- Setting Lower threshold/Upper threshold
- Automatic check on/off
- Start manual control (Extraordinary control) (fee required)
- Specify minimum liquidity control level (Minimum liquidity)
- Query the balance of the instant settlement account at any frequency

The logic of the automatic liquidity management function from the perspective of a given Clearing Member is as follows:

- In order to determine the need for a transfer of cover, a Lower and Upper Threshold has been defined in the GIROInstant platform.
  - If the available credit of the Instant Settlement Account is below the Lower Threshold at the time of the ordinary or extraordinary control, i.e. the Instant Settlement Account balance < Lower Threshold, the GIROInstant platform will initiate a transfer in favour of the collective account in VIBER.
  - If the available credit of the Instant Settlement Account is above the Upper Threshold at the time of the ordinary or extraordinary contro, i.e. Instant Settlement Account Balance > Upper Threshold, the GIROInstant platform will initiate a transfer against the collective account in VIBER during opening hours.
  - The Lower and Upper thresholds are set by each Clearing Member itself, in HUF.

- Liquidity rule is used to determine the amount to be transferred to or from the collective account.
  - During the ordinary or extraordinary control, the GIROInstant platform will attempt to set the Clearing Member's instant settlement account balance to the current Liqudity rule level, so the amount included in the funds transfer request to VIBER may be determined as follows:
    The amount to be transferred is equal to

    a) in case of a transfer in favour of the collective account: the difference between the Liqudity rule and the available credit of the Clearing member's instant settlement account at the time of ordinary or extraordinary control.

    b) in case of a transfer against the collective account: the difference between the available credit of the Clearing member's instant settlement account and the Liqudity rule at the time of ordinary or extraordinary control. The amount of the transfer against the collective account may not exceed the value of the current Credit Line.

- On the GIROInstant platform, each Clearing Member can set the Liquidity rule parameter in HUF, with no technical limit to the frequency of change.

2.2 Funding

In case of a transfer in favour of the collective account from the Clearing Member's bank account, the GIROInstant platform will perform the following steps:

1. If the instant settlement account on the GIROInstant platform requires additional liqudity, the platform generates a transfer request for a specified amount in favour of the collective account, which is forwarded to VIBER.
2. When the request is processed in VIBER, the funds are transferred from the Clearing Member's bank account to the collective account according to the specified amount, and VIBER sends a confirmation to the GIROInstant platform, and a debit notification to the Clearing Member that the transfer has been successfully completed.
3. The GIROInstant platform will credit the specified amount to the relevant Clearing Member's Instant Settlement Account.

No partial execution is possible during VIBER operating hours due to the rules of VIBER. Outside the VIBER operating hours, requests for cover are forwarded to the Credit Limit Register (CLR). The operation of the CLR also allows for partial settlement, whereby the partial amount sent and confirmed by the CLR is credited to the clearing member's instant settlement account.

2.3 Defunding

In the case of a transfer from the collective account in favour of the Clearing Member's bank account, the following steps will be taken:

1. In the event that a liquidity transfer is required from the instant settlement account, the GIROInstant platform first blocks the amount of the transfer request in the Clearing Member's instant settlement account, thus ensuring that the amount to be transferred is reserved until the transfer between the collective account and the clearing member's bank account is completed.

2. At the same time, the GIROInstant platform will generate a transfer against to the collective account and forward it to VIBER.

3. In VIBER, when the request is processed, the funds are transferred between the VIBER accounts (debited from the Collective Account to the Clearing Member's bank account) according to the specific amount, and VIBER sends a confirmation to the GIROInstant

platform, and VIBER also sends a credit notification to the Clearing Member that the transfer has been successfully completed.

4. The GIROInstant platform will debit the Clearing Member's Instant Settlement Account with the amount transferred at the same time as the block is released.

There is no possibility to allocate cover outside VIBER operating hours.

2.4 Ordinary control

The verification of the balances of instant settlement accounts against the Lower and Upper Thresholds is not performed during the settlement and clearing of each transaction, but by default at regular intervals, scheduled in advance, during the execution of the so-called Automatic Verification process.

- A Fund Transfer request will be sent to VIBER if the available credit of the instant settlement account is below the Lower Threshold or above the Upper Threshold when the Automatic Check is executed.
- No automatic cover transfer request is sent to VIBER between Automatic Checks. Clearing Members may use the Manual Check feature of the platform during the periods between automatic checks, as they wish. (The details of the Manual Check are explained in the next chapter.)
- The frequency of the Automatic Checks is set by GIRO Zrt. as the System Operator, in prior consultation with Clearing Members. Automatic Checks shall run at the same intervals for the entire duration of the Settlement Day
- The Clearing Member may switch the execution of the Automatic Checks on or off at its own discretion. If the Automatic Check is switched off, the platform shall not automatically generate a margin transfer request to VIBER. In such a case, the Clearing Member shall itself ensure that the available credit of its Instant Settlement Account is checked by either deactivating the Automatic Check or by initiating the Manual Check.

2.5 Extraordinary control

Regardless of whether Automatic Check is on or off, the Clearing Member can also perform a Manual Check. A Manual Check may be carried out up to 4 times a day without any additional charge, provided that at least 120 minutes elapse between two Manual Checks. Otherwise, the manual check will be charged at the BKR Fee Schedule. The functionality of the Manual Check is

the same as for the Automatic Check, but it is not started automatically and on a scheduled basis, but manually.

- During the Manual Check, the available credit of the Clearing Member's Instant Settlement Account is checked and if it is below the Lower Threshold or above the Upper Threshold, a margin transfer request is initiated to VIBER.
- If an Automatic or another Manual Check is already in progress when the Manual Check is initiated, the newly initiated Manual Check will no longer be executed.
- GIRO Zrt. as System Operator may also initiate a Manual Control in case of an incident or upon request of a Clearing Member, which will be executed for all Clearing Members simultaneously, regardless of the deactivated state of the Automatic Control.
- A new check cannot be initiated while a previous Automatic or Manual check is running.
- No Manual Check shall be started at the end of the reconciliation cycle. The GIROInstant platform shall reject the execution of a Manual Check started during this period and inform the Clearing Member accordingly. The request to perform a Manual Check shall be repeated after the closure.
- The purpose of the Manual Check is to provide the possibility to execute margin calls in case of urgency between two runs of the 15-minute Automatic Check. It is recommended to execute it after the available credit has been retrieved, if the liquidity situation so warrants. This function is not intended to check the liquidity situation on a regular basis.

2.6 GIROINSTANT MINIMUM LIQUIDITY CHECK

The GIROInstant platform has a security feature called Minimum Liquidity Check. The Minimum Liquidity Check checks the available credit of the Clearing Member's instant settlement account at regular intervals, independently of the Automatic Check, in a pre-scheduled manner.

- If the available credit of the Clearing Member's Instant Settlement Account is below the GIROInstant Minimum Balance level at the Minimum Liquidity Check, i.e. the Available Credit of the Instant Settlement Account < GIROInstant Minimum Balance, the GIROInstant platform will send a warning via the GIROInstant Monitor or API to the Clearing Member.
- The GIROInstant Minimum Balance value is set by each Clearing Member for itself in HUF.

- The frequency of the GIROInstant Minimum Balance Checks is set by GIRO Zrt. as System Operator, in accordance with prior agreement with Clearing Members. The GIROInsant Minimum Liquidity Checks shall run at the same intervals throughout the settlement day

2.7 SYSTEM OPERATOR TASKS

The automatic liquidity management function of the GIROInstant platform can be tailored to the needs of Clearing Members at the platform level, by GIRO Zrt. as the System Operator, according to the following parameters:

- Determine the frequency of automatic checks (to the nearest minute)
- Determine the frequency of minimum liquidity checks (to the nearest minute)

In special cases, GIRO Zrt. as the System Operator has the possibility to access the following platform functions:

- Launching a manual check for all Clearing Members simultaneously and simultaneously, if required to resolve a GIROInstant incident or in case of a Clearing Member's GIROInstant Monitor access problem. GIRO Zrt. will inform the Clearing Members about the execution of the manual check afterwards.
- Changes to the Reference Levels, Lower and Upper Thresholds and Minimum Liquidity Control Levels per Clearing Member,
- Determination of the minimum Reference Level value that may be provided by Clearing Members.

3 LIQUIDITY MANAGEMENT FOR INDIRECT PARTICIPANTS

The previously mentioned Automatic Liquidity Management process describes the margin adjustments of the instant settlement accounts related to the clearing members of the GIROInstant platform. The Indirect Participants do not have their own Instant Settlement Account within the GIROInstant platform and therefore use the Instant Settlement Account of their associated Clearing Member and thus the liquidity of their associated Clearing Member.

Clearing Members have the possibility to limit the liquidity that can be used by their Indirect Participants in order to prevent an Indirect Participant from draining the liquidity of the Clearing Member (and thereby the other Indirect Participants), if applicable.

The Clearing Member may set a limit on each of its Indirect Participants in the GIROInstant Monitor

- called CAP - to set a maximum limit on the value of the transactions sent by an Intermediary Participant above the value of the transactions received by that Intermediary Participant. In other words, a CAP specifies the maximum amount by which the settled net turnover of an Intermediate Participant can go below 0.

The CAP is used to calculate the available credit of the Intermediate Participant:

Available credit = CAP + cleared net turnover

When sending a transaction to an Indirect Participant, the GIROInstant platform checks, on the one hand, whether the Indirect Participant has sufficient Available Credit and, on the other hand, whether the corresponding Clearing Member has sufficient funds in its Clearing Member's Instant Settlement Account (i.e. sufficient Available Credit). If either condition is not met, the Indirect Participant's transaction will be rejected.

The settled net turnover of an Intermediate Participant shall be reset to zero at the end of each settlement day, so that at the start of each settlement day the Intermediate Participant's Available Credit is equal to the value of its CAP.

4 Funding outside VIBER operating hours

During VIBER opening hours, liquidity transfer requests will be forwarded to VIBER and, when executed, will be transferred between the Clearing Member's bank account and the collective account. Outside VIBER opening hours, margin transfer requests automatically constitute central bank borrowing. These requests, central bank borrowings, are forwarded to the Credit Limit Register (CRR). Transfer requests to the collective account which have not been processed by VIBER during VIBER's opening hours are rejected and are not forwarded to the CCBM.

It is not possible to allocate cover outside VIBER operating hours.

It is important to underline that the ICSD does not become operational immediately after the closure of VIBER, but according to the schedule of the MNB SIF, prior to the sending of the BKR Framework. During this period, no cover transfer request will be executed. Similarly, there is a period (from 06:15 to 07:00 on each VIBER opening day until the scheduled VIBER opening) before the opening of the VIBER when no margin transfer requests are executed.

Outside the VIBER operating hours, the details of collateral transfer requests - i.e. central bank borrowings - and the operation of the ICSD are as follows:

- The MNB will send the GIROInstant credit line information for all Clearing Members to the HCNB.

- The MNB has the possibility, outside the VIBER operating hours, to make additional extra credit limit adjustments (increase or decrease of existing limits).

- The GIROInstant credit lines are only a contingency reserve for Clearing Members. Drawdowns from the GIROInstant credit line may only be used as a form of financing in exceptional situations. It is the responsibility of Clearing Members to ensure that sufficient funds are available in their Instant Settlement Account prior to VIBER closure for their expected overnight or working day operations.

- Upon receipt of a request for margin call, HKNY will reduce the credit limit of the relevant Clearing Member by the amount requested and send a response message to the GIROInstant platform.

- The HKNY allows for a partial drawdown of the requested amount, i.e. if the available credit limit does not cover the requested amount, the remaining available credit limit will be drawn down in full.

- During the HKNY operating period, no reduction of cover and thus no GIROInstant loan repayment is possible.

- The drawn credit lines and the related fees will be booked at the next VIBER opening according to the MNB's AML. At 6:15 on each VIBER opening day, the operation of the ICSD is stopped and the value of the GIROInstant credit limits recorded therein is reset to zero.

- Collateral entries made during HKNY operating hours are notified to the MNB by the HKNY, broken down into pre-midnight and post-midnight, and the central bank loans and related fees are recorded in the MNB systems. For the opening of the VIBER, the withdrawals of collateral prior to the opening of the VIBER are booked to the collective account in accordance with the MNB SFA.

- Once the VIBER opening process has been completed, the collateral transfer requests are again forwarded to VIBER.

5 GIROInstant monitor – Liquidity management

The GIROInstant platform includes the GIROInstant Monitor, through which Clearing Members can monitor their own and their Indirect Participants' transactions in GIROInstant. Clearing Members can customise the parameters of the Automatic Liquidity Management, monitor their liquidity and download their own reconciliation reports.

With GIROInstant Monitor, Clearing Members can therefore

- can set their own Reference Level, Lower and Upper Thresholds and Minimum Liquidity Control Level.
- switch the Automatic Check function on and off for themselves.
- Set up a manual check for themselves (fee required).
- query the current balance of your instant settlement account.
- set the CAPs of your indirect participants.
- check the margin transfer requests and their results (the GIROInstant platform does not send a separate notification of margin transfers to Clearing Members).

GIROInstant Monitor supports the activities of Clearing Members with additional historical data retrieval and data analysis solutions.

GIROInstant Monitor is also available with automated data connectivity and data retrieval solutions between Clearing Members and the GIROInstant platform, however, certain technical limitations may apply. Operations that compromise the operation of the GIROInstant system may be sanctioned by GIRO Zrt.

6 CALCULATION EXAMPLES

6.1 First funding

The right and possibility to market a Clearing Member joining the GIROInstant system will be granted upon the entry into force of the registration in the Verfication Table and after the first cover has been provided. The Clearing Member is required to set the parameters for liquidity management in the GIROInstant Monitor based on the expected turnover after the entry into force of the Lending Table. The initial margining shall be carried out at a level equal to the reference level set. The parameters in the example are:

- Reference level (liquidity rule) = 100 mFt
- Upper threshold = 150 mFt
- Lower threshold = 50 mFt

Instant settlement account	Description
• Credit line = 0 • Net position = 0 • Available credit = 0	• The transfer of funds is executed in the first ordinary control or extraordinary control following the settings of the parameters. During the control process, the balance of the instant settlement account is cross checked against the lower/upper threshold. As in this case available credit 0, lower threshold 50 mFt, therefore a funds transfer is made. • Calculation: Liquidity rule (100) -available credit (0) =100 mFt • After funds transfer carried out in VIBER, Credit line will be increased by 100mFt: • Credit line (before)=0 • New credit line = 100 mFt • New available credit= 100 mFt = credit line (100)+net position (0)

6.2 Funding

The clearing member's cleared net turnover is -51 mFt at the time of the next automatic or manual check, the parameters remain as follows:

- Reference level (liquidity rule) = 100 mFt
- Upper threshold = 150 mFt
- Lower threshold = 50 mFt
- Available credit = 49 mFt

Instant settlement account	Description
• Credit line = 100 mFt • Net position = -51 mFt • Available credit = 49 mFt	• At the time of running the control available credit (49) is below the lower threshold (50), therefore a funds transfer is made. • Calculation: Liquidity rule (100) -available credit (49) =51 mFt • After funds transfer carried out in VIBER, Credit line will be increased by 51mFt: • Credit line (before)=100 • New credit line = 151 mFt • New available credit= 100 mFt = credit line (151)+net position (-51)

6.3 Defunding

The clearing member's cleared net turnover is +7 mFt at the time of the next automatic or manual check, the parameters remain as follows:

- Reference level (liquidity rule) = 100 mFt

- Upper threshold = 150 mFt
- Lower threshold = 50 mFt
- Available credit = HUF 158 million

Instant settlement account	Description
• Credit line = 151 mFt • Net position = 7 mFt • Available credit = 158 mFt	• At the time of running the control available credit (158) is above the upper threshold (150), therefore a funds transfer is made. • Calculation: Available credit (158) - Liquidity rule (100) =58 mFt • Defunding is only possible if the amount to be withdrawn does not exceed the current credit line, so Credit line - amount to be withdrawn >= 0 • After funds transfer carried out in VIBER, Credit line will be decreased by 58mFt: • Credit line (before)=151 mFt • New credit line = 93 mFt • New available credit= 100 mFt = credit line (93)+net position (7)

6.4 Closing the reconciliation cycle

At the end of the Reconciliation Cycle the Clearing member's net position will be reset. Here the Net Position is reset and the Credit Line is either decreased if the net position is negative or increased if the net position is positive accordingly. Available credit remains unchanged and the available credit and the credit line are equal at the end cycle.

Instant settlement account before resetting of net position	Instant settlement account after resetting of net position
• Credit line = 93 mFt • Net position = 7 mFt • Available credit = 100 mFt	• Credit line = 100 mFt • Net position = 0 mFt • Available credit = 100 mFt

6.5 Unsuccessful defunding

The clearing member's cleared net turnover is +300 mFt at the time of the next ordinary or extraordinary control, the parameters remain as follows:

- Reference level (liquidity rule) = 100 mFt
- Upper threshold = 150 mFt
- Lower threshold = 50 mFt
- Available credit = HUF 400 million

Instant settlement account	Description
•Credit line = 100 mFt •Net position = 300 mFt •Available credit = 400 mFt	•At the time of running the control available credit (400) is above the upper threshold (150), therefore a funds transfer is made. •Calculation: Available credit (400) - Liquidity rule (100) =300 mFt •Defunding is only possible if the amount to be withdrawn does not exceed the current credit line, so Credit line - amount to be withdrawn >= 0 •In this case this condition is not met, so defunding is unsuccesful: Credit line (100) < Amount to be withdrawn (300)

It is suggested to increase the value of the liqudity rule in case of regular unsuccessful adjustments of funds.