EAM ADDITIONAL SERVICES GUIDE

BUSINESS TERMS AND CONDITIONS

ANNEX NO 20.

Content

List of figures

List of tables

1 Introduction

1.1 Purpose of the document

The purpose of this document is to provide a summary of the process for instant credit transfers initiated through the Unified Data Entry Solution (hereinafter referred to as "EAM"), approved in the application installed on a portable multifunctional device, and the additional processes required to carry out this process.

1.2 Scope of the document

This document covers the following tasks performed by GIRO Zrt. as system operator:

- Clearing and settlement of instant credit transfers initiated via EAM,
- The transmission (outsourced to the Aggregator) of a feedback message sent by the Payer's Clearing Member on the execution or rejection of an instant credit transfer initiated via EAM (hereinafter referred to as "Confirmation Message"),
- the central register of cash substitute payment instruments made available on a portable multifunctional device enabling the initiation of instant credit transfer orders via EAM (hereinafter "central register of mobile banking applications").

This document also describes the additional tasks performed by GIRO Zrt. on the basis of statutory obligations:

- Placing the security code in the EAM to be created (outsourced to the Aggregator),
- Maintaining a certificate store to verify the security code.

This document applies to both interbank and intrabank credit transfers initiated via EAM.

The tasks, rights and obligations of the Sub-aggregators and the conditions for carrying out the Sub-aggregator activity are set out in a separate contract and business rules. To facilitate understanding, the flowcharts also indicate the Sub-aggregators and their tasks.

1.3 Content of the document

This document contains

- instant credit transfers initiated via EAM, such as QR code, deep link and NFC-based data entry solutions (as a payment scheme),
- the registration and deletion of mobile banking applications in the central register, and
- the operation of the Certificate Storage

rules, process descriptions, practical information and information on message handling and processing.

1.4 References, documents used

Identifier	Address
Relevant legal regulations	
Decree of the Governor of the Magyar Nemzeti Bank	Decree No 35/2017 (XII. 14.) on Execution of Payment Transactions (hereinafter MNBr.)
Message Implementation Guide	
GIRO Message Implementation Guides [1]	ISO 20022 pain.002 Message Implementation Guide (MIG) HCT Inst MIG
EAM Certificate Storage Development and Management Guide	
EAM Certificate Storage Development and Management Guide	

1.5 Change tracking

Date of entry into force	Content, change
1 September 2024.	Publication of the document.

2 General overview

The EAM data entry methods and use cases for initiating an instant credit transfer are as follows:

1. Two types of instant credit transfers initiated by QR code:

- using the mobile banking app to scan the QR code

- provided by the technical service provider or the factory camera software of the portable multifunctional device (smartphone, tablet, etc.) is used to scan the QR code, which launches the pre-installed mobile banking application. This requires that the mobile banking application has been previously registered in the central register of mobile banking applications kept by GIRO Zrt. as described in Chapter 8.

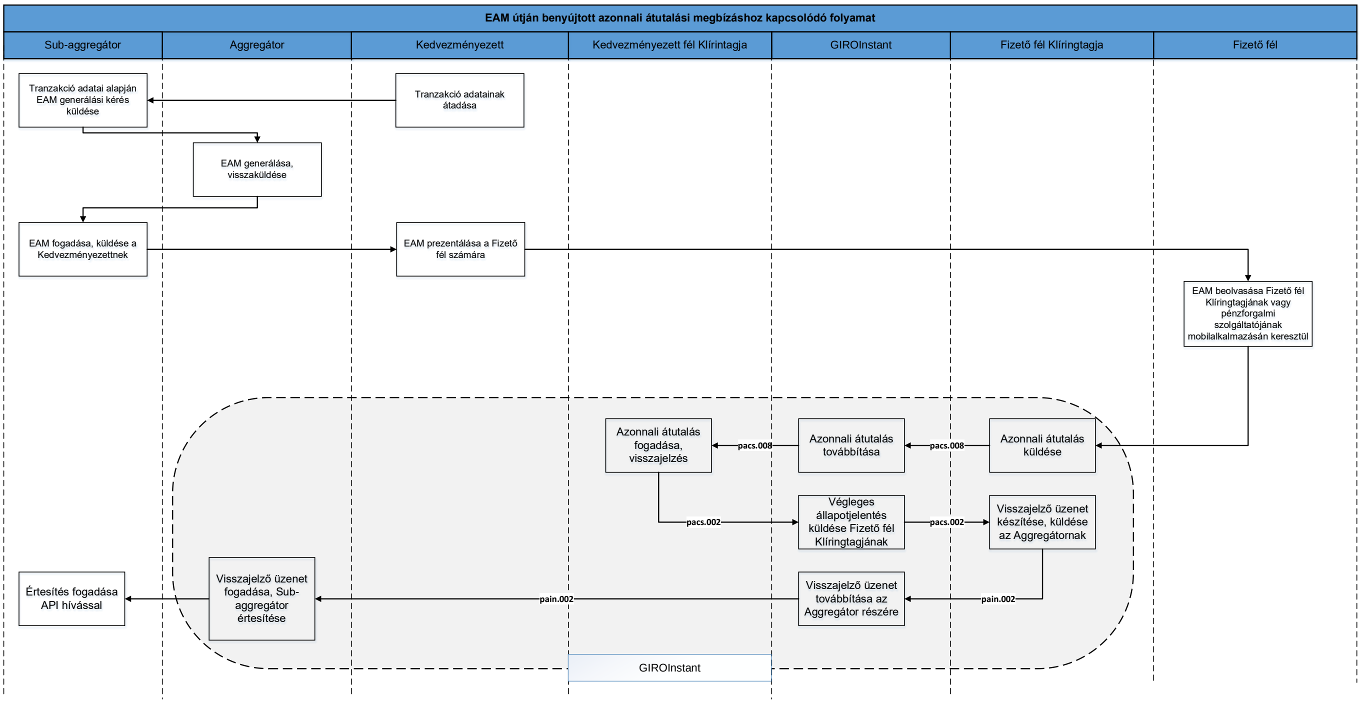
2. Instant credit transfer initiated by deep link: no camera scan is required, because the deep link(deep link based data entry procedure) launches the mobile banking application and the prepared instant credit transfer only needs to be approved by the Payer.

3. Instant credit transfer initiated via NFC: short-range communication technology based on RFID (Radio Frequency Identification) standards, as described in ISO/IEC 14443. The active communication mode defined in the standard can be used to issue a code to support the submission of an instant credit transfer order. Following the NFC-based data transmission, the mobile multifunctional device launches the pre-installed mobile banking application previously registered in the central register of mobile banking applications maintained by GIRO Zrt.

[1] Available at www.giro.hu, after logging in.

The term EAM refers to all three data entry methods (QR code, NFC, deep link).

1. ábra Process related to an instant credit transfer submitted via EAM


EAM útján benyújtott azonnali átutalási megbízáshoz kapcsolódó folyamat
Sub-aggregátor
Aggregátor
Kedvezményezett
Kedvezményezett fél Klírintagja
GIROInstant
Fizető fél Klíringtagja
Fizető fél
Tranzakció adatai alapján EAM generálási kérés küldése
Tranzakció adatainak átadása
EAM generálása, visszaküldése
EAM fogadása, küldése a Kedvezményezettnek
EAM prezentálása a Fizető fél számára
EAM beolvasása Fizető fél Klíringtagjának vagy pénzforgalmi szolgáltatójának mobilalkalmazásán keresztül
Azonnali átutalás fogadása, visszajelzés
pacs.008
Azonnali átutalás továbbítása
pacs.008
Azonnali átutalás küldése
pacs.002
Végleges állapotjelentés küldése Fizető fél Klíringtagjának
pacs.002
Visszajelző üzenet készítése, küldése az Aggregátornak
Értesítés fogadása API hívással
Visszajelző üzenet fogadása, Sub-aggregátor értesítése
pain.002
Visszajelző üzenet továbbítása az Aggregátor részére
pain.002
GIROInstant

Steps in the process:

1. If the Payer chooses the instant credit transfer payment method, the Beneficiary will electronically transmit the current purchase data to the Sub-aggregator, who will forward them to the Aggregator.
2. The Aggregator will create the EAM according to the standard defined in Chapter 6 of this document, which will include the details of the purchase and the beneficiary, and will provide the data with a validation code and send it to the Beneficiary via the Sub-aggregator.
3. The Beneficiary shall display and make available the EAM to the Payer. For example. In case of a web shop purchase, it is also possible to generate a link (deep link) for a purchase on a portable multifunctional device, which is clicked to open the mobile banking application of the Payer Clearing Member or payment service provider. In the case of NFC, the Beneficiary's device transmits the data.
4. The Payer scans the EAM using its portable multifunction device. The scanning of the EAM launches the pre-installed mobile banking application on the Payer's mobile multifunction device, as the names of the mobile banking applications that can be activated by the scanning of the EAM on the respective mobile multifunction device are stored in the central register of mobile banking applications. Otherwise, the Payer will already have accessed the mobile banking application in advance and will scan the EAM there.
5. The Payer's payment service provider shall ensure that the checks referred to in Section 3.3.1.1 are carried out in the Mobile Banking application. If the checks are found to be correct, the Payer shall then have the option to approve the instant credit transfer, reject the EAM or save it for later approval. Upon receipt of the instant credit transfer, the process continues as specified by the Payer Clearing Member.

6. The Payer Clearing Member shall ensure that the checks under Section 3.3.1.2 are carried out and shall then execute the instant credit transfer. If the Payer and the Beneficiary Clearing Member are the same, an intra-bank transfer will be made. The Payer Clearing Member shall submit the interbank instant credit transfer order to the GIROInstant platform for settlement. The settlement and execution of the instant credit transfer shall be carried out in accordance with Annex 25 of the BKR Rules.
7. The Payer Clearing Member shall send a confirmation message on the execution of the instant credit transfer initiated via EAM to the payment service provider having a contractual relationship with the Beneficiary, as defined below as a Sub-aggregator. The Payer Clearing Member shall perform this task by submitting a pain.002 message to the Aggregator on the GIROInstant platform. At the same time, the Payer Clearing Member shall notify the Payer of the debit on its portable multifunctional device, who shall thereby ascertain the final status of the transaction.
8. GIROInstant will send the confirmation message to the Aggregator.
9. The Sub-aggregator receives the confirmation message from the Aggregator via an API call and notifies the Beneficiary that the settlement has been made.

3 Instant credit transfer initiated via EAM

3.1 The actors in the process

Beneficiary (merchants, service providers)

The beneficiary of an instant credit transfer initiated via EAM. The actor who instructs the sub-aggregator to set up an EAM.

Aggregator

Behalf of the sub-aggregator, and as specified in a separate set of business rules, ensure the production and control of the EAM for the instant credit transfer initiated via EAM in a closed system.

On behalf of GIRO Zrt. and under its responsibility, it performs the following tasks in the framework of outsourced activities:

- placing a security code in the EAM.

- ensure the transmission of the confirmation message initiated by the Payer Clearing Member to the Sub-aggregator.

Sub-aggregator

The payment service provider providing the Beneficiary with the production of the EAM and the transmission of the confirmation message on the execution or rejection of the instant credit transfer initiated via the EAM. It may maintain a collective account for the Beneficiary, from which it will arrange for the onward transfer of the funds in the collective account, based on a contract with the Beneficiary.

Payer

The operator who scans or receives the EAM using the mobile banking application of the payment service provider providing the payment initiation or payment account management service. The Payer may approve an instant credit transfer initiated via EAM, save the EAM for later approval, reject it or disregard it.

Payer's payment service provider

A payment service provider providing a payment initiation or payment account management service to the Payer, which provides a mobile banking application to the Payer and has pre-registered the mobile banking application in the central register of mobile banking applications maintained by GIRO.

Payer Clearing Member

The payment service provider holding the Payer's payment account. It shall perform its duties in relation to the execution of an instant credit transfer initiated via the EAM, as defined by law and in these Terms and Conditions. It shall send a confirmation message on the execution or rejection of an instant credit transfer initiated via EAM to the payment service provider having a contractual relationship with the payee, i.e. the sub-aggregator.

Beneficiary Clearing Member

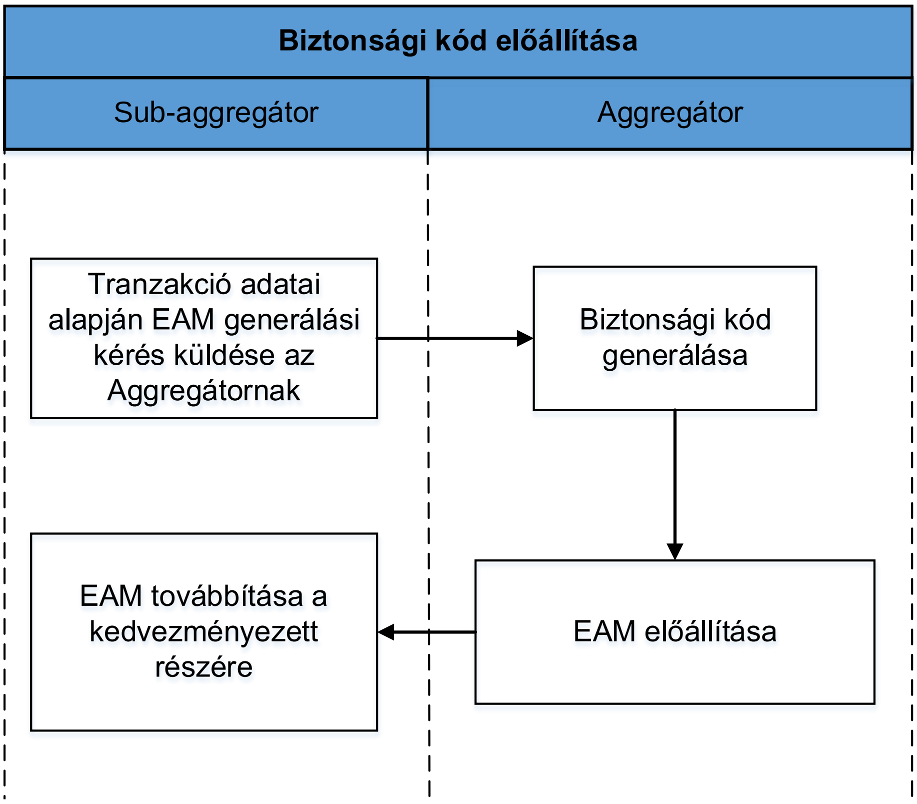
The payment service provider holding the Beneficiary's payment account or the sub-aggregator's collection account, who is a direct participant in the BKR.

GIRO Zrt. as

- the operator of the GIROInstant platform, settles instant credit transfers;
- the certificate storage operator;
- Head of the central register of mobile banking applications;
- the transmitter of the confirmation message;

3.2 Security code generation

2. ábra Security code generation

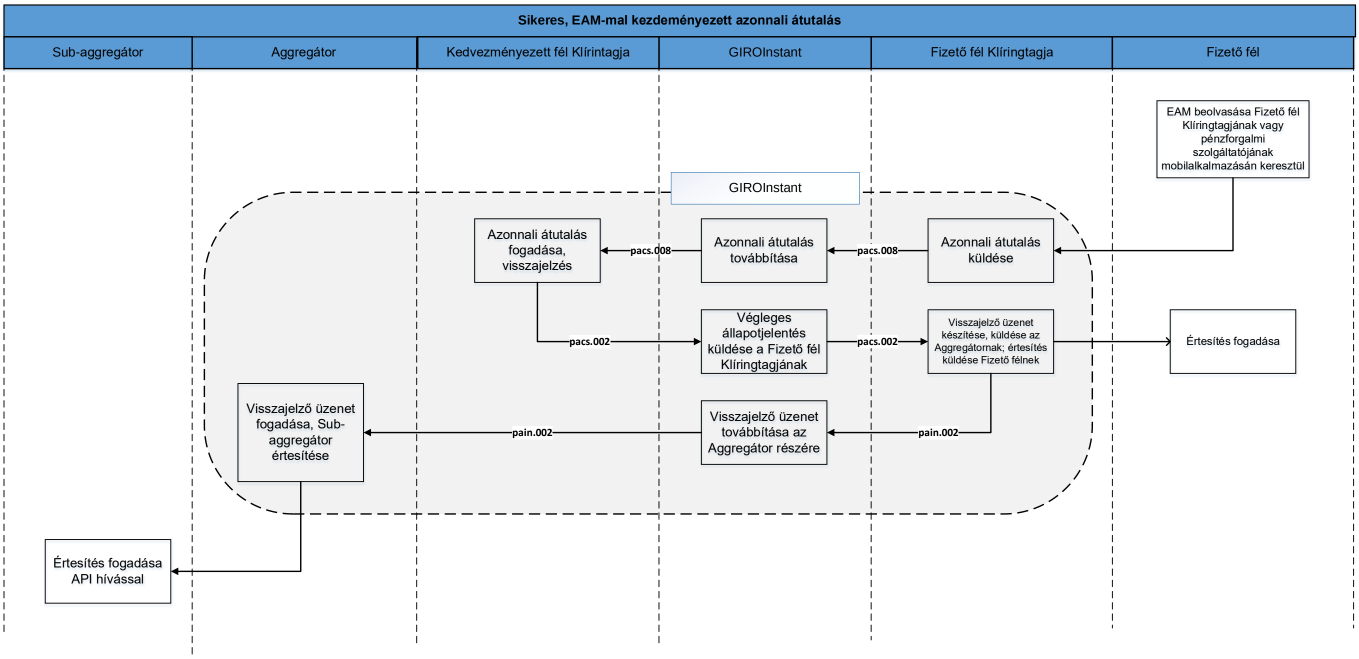

Biztonsági kód előállítása
Sub-aggregátor
Aggregátor
Tranzakció adatai alapján EAM generálási kérés küldése az Aggregátornak
Biztonsági kód generálása
EAM előállítása
EAM továbbítása a kedvezményezett részére

1. The Sub-Aggregator submits to the Aggregator an EAM generation request (hereinafter referred to as "Authentication Request") based on the transaction data received from the Beneficiary via electronic channel, the rules of which are set out in a separate contract and business rules. In the Authentication Request, the Sub-Aggregator instructs GIRO Zrt. to generate a uniquely generated PKI-based security code to be used for the generation and verification of the EAM and to include it in the EAM authentication code. The Aggregator shall perform the tasks related to the generation and verification of the GIRO security code through an outsourcing contract with GIRO.
2. The Aggregator will generate on behalf of GIRO Zrt. the uniquely generated security code according to Chapter 6 of this document.
3. The Aggregator shall produce the EAM according to the standard defined in Chapter 6 of this document.
4. The Aggregator sends the generated EAM to the Sub-aggregator, which forwards it to the Beneficiary.

3.3 Flowcharts for instant credit transfers initiated via EAM

3.3.1 Successful instant credit transfer initiated via EAM

3. ábra Instant credit transfer initiated on a schema-based portable multifunction device - Logical flowchart of successful message flow


Sikeres, EAM-mal kezdeményezett azonnali átutalás
Sub-aggregátor
Aggregátor
Kedvezményezett fél Klírintagja
GIROInstant
Fizető fél Klíringtagja
Fizető fél
EAM beolvasása Fizető fél Klíringtagjának vagy pénzforgalmi szolgáltatójának mobilalkalmazásán keresztül
GIROInstant
Azonnali átutalás fogadása, visszajelzés
pacs.008
Azonnali átutalás továbbítása
pacs.008
Azonnali átutalás küldése
pacs.002
Végleges állapotjelentés küldése a Fizető fél Klíringtagjának
pacs.002
Visszajelző üzenet készítése, küldése az Aggregátornak; értesítés küldése Fizető félnek
Értesítés fogadása
Visszajelző üzenet fogadása, Sub-aggregátor értesítése
pain.002
Visszajelző üzenet továbbítása az Aggregátor részére
pain.002
Értesítés fogadása API hívással

Steps in the process:

1. The Payer scans the EAM using its portable multifunction device. The Payer payment service provider shall check the formality of the EAM, its validity period, and the authentication code in the mobile banking application to ensure that no changes have been made to the information contained in the EAM. The verification of the authentication code shall be carried out in accordance with the procedure detailed in the Certificate Price section. If the verification finds everything correct, the Payer then has the option to approve the transfer instantly, reject the EAM or save it for later approval. Upon receipt of the instant credit transfer, the process continues as defined by the Payer Clearing Member.

2. It is the Payer Clearing Member's responsibility to ensure that the following checks are carried out in relation to the instant credit transfer:
   - Checking the validity period of the EAM before executing an instant credit transfer,
   - duplication control,
   - checking the coverage of the payer,
   - checking all other formal, business, and legal requirements for any instant credit transfer initiated through the EAM.

   After verification, the data content of the instant credit transfer and the additional data will be transmitted via the GIROInstant platform. If the Payer Clearing Member and the Beneficiary Clearing Member are the same, an intra-bank transfer will be made.

3. The GIROInstant platform sends a final status report on the execution of the instant credit transfer submitted via EAM. The steps of the message exchange between the Payer Clearing Member and the Beneficiary Clearing Member are the same as the message exchange for the instant credit transfer scheme (pacs.008pacs.002: beneficiary feedback pacs.002: final status report). In the case of an intra-bank instant credit transfer, the transaction does not pass through the GIROInstant platform, by analogy, and therefore no final status report is generated.

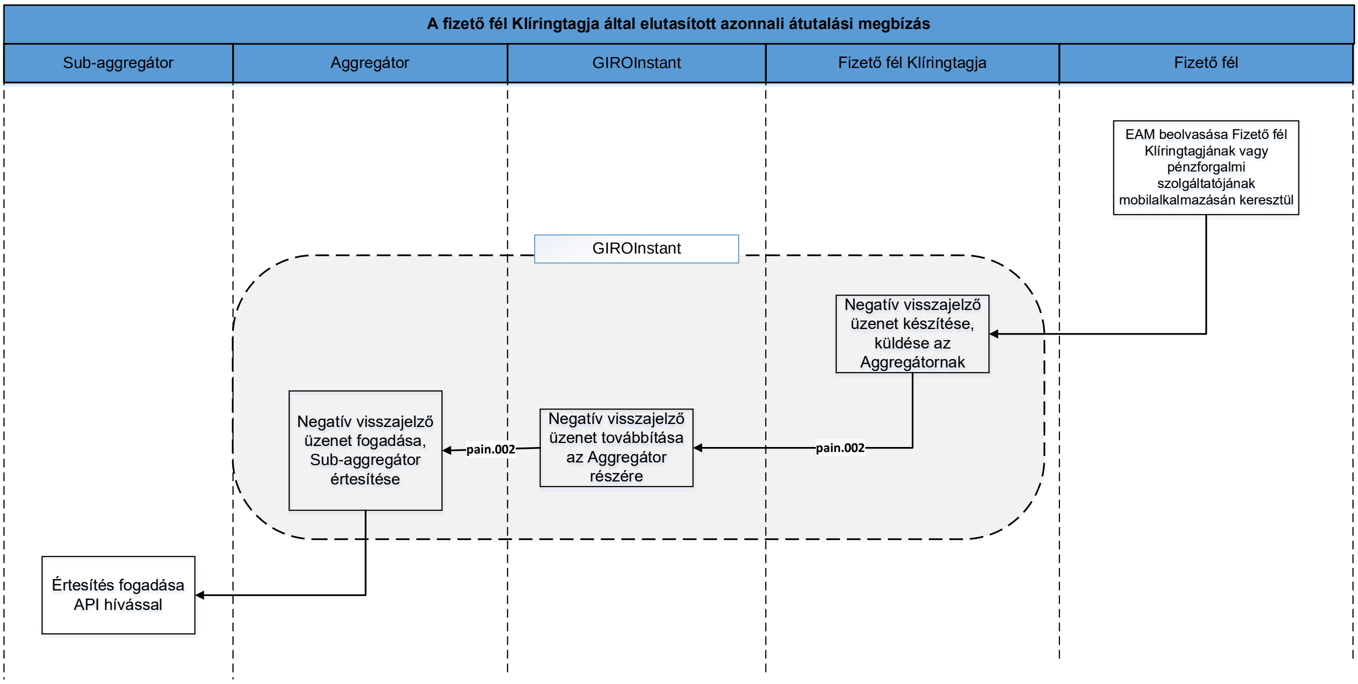
4. The Payer Clearing Member sends a confirmation message via the GIROInstant platform on the successful execution of both the intra-bank and interbank instant credit transfer in the form of a pain.002 confirmation message. The message shall be generated in accordance with the ISO 20022 pain.002 Message Application Guide (MIG). At the same time, the Payer Clearing Member shall notify the Payer of the debiting of the payment account, who shall thereby be satisfied that the instant credit transfer initiated via EAM has been completed.

5. GIROInstant will send the confirmation message to the Aggregator.

6. The Sub-aggregator receives the confirmation message via an API call and notifies the Beneficiary that the settlement has been made.

3.3.2 Issue 1: Instant credit transfer rejected by the Payer Clearing Member

4. ábra Instant credit transfer initiated under the scheme: negative feedback from the Payer Clearing Member


A fizető fél Klíringtagja által elutasított azonnali átutalási megbízás
Sub-aggregátor
Aggregátor
GIROInstant
Fizető fél Klíringtagja
Fizető fél
EAM beolvasása Fizető fél Klíringtagjának vagy pénzforgalmi szolgáltatójának mobilalkalmazásán keresztül
GIROInstant
Negatív visszajelző üzenet készítése, küldése az Aggregátornak
pain.002
Negatív visszajelző üzenet továbbítása az Aggregátor részére
pain.002
Negatív visszajelző üzenet fogadása, Sub-aggregátor értesítése
Értesítés fogadása API hívással

1. If the Payer Clearing Member rejects to execute an intra-bank or inter-bank instant credit transfer, a negative pain.002 confirmation message will be sent via the GIROInstant platform as follows. The message must be generated in accordance with the relevant MIG standard.

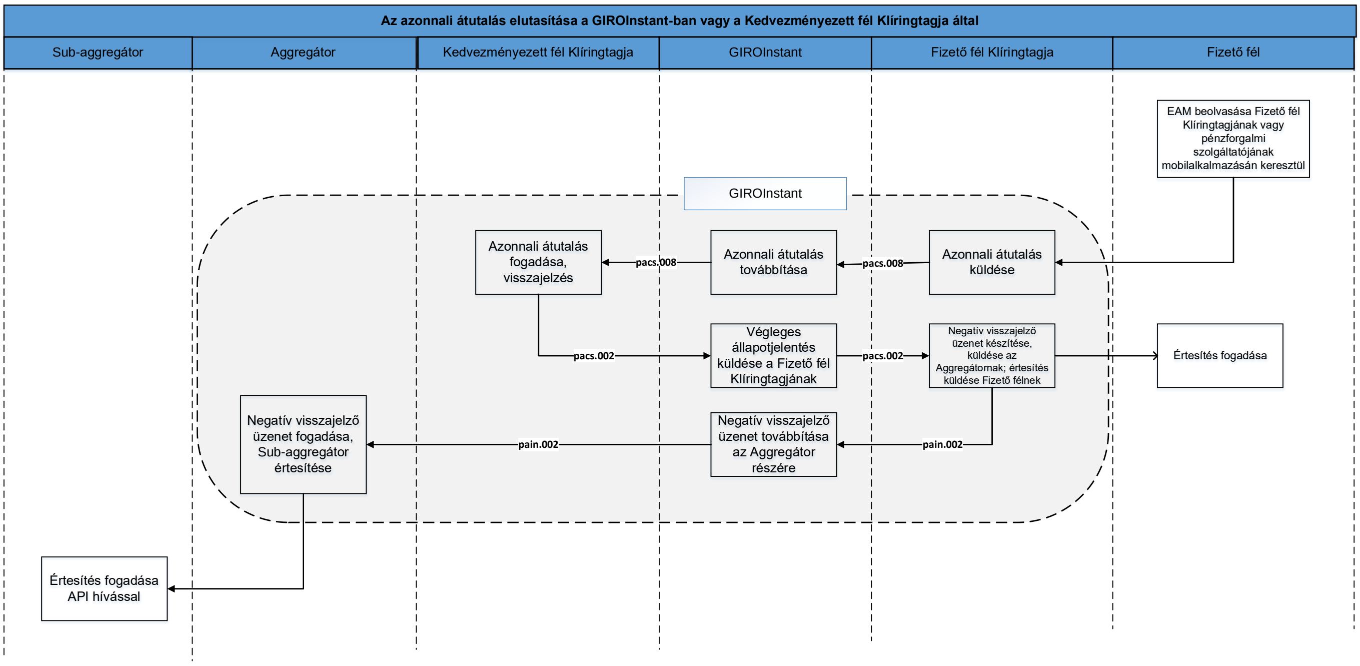
- Payer's coverage check: in case of insufficient funds, it is mandatory to send the confirmation message with error code MS03.
- verification of the authentication code: if the verification by the Payer payment service provider fails, a confirmation message shall be sent with the MIG standard error code (DS0D, DS0E, DS17).
- Duplication check: if an instant credit transfer has already been executed on the basis of an EAM, the Payer Clearing Member will fill in the confirmation message with error code AM05 to indicate the duplicate initiative.
- checking all other formal, legal, and business requirements for all instant credit transfers initiated via EAM: if the check fails, a confirmation message with the relevant error code will be sent.

2. GIROInstant forwards the negative confirmation message to the Aggregator.
3. The Sub-aggregator receives the confirmation message via an API call and notifies the Beneficiary of the rejection of the instant credit transfer.

If the Payer Clearing Member is unable to generate a pain.002 confirmation message due to a formal deficiency in the EAM (e.g. mandatory data is missing), it is recommended that GIRO Zrt. be notified of the reason for the failure to send pain.002 in the JIRA error reporting interface. The GIRO Helpdesk is able to investigate the incident based on this report and notify the Aggregator to detect possible errors.

3.3.3 Error 2: The instant transfer was rejected by GIROInstant or the Beneficiary Clearing Member

5. ábra Instant credit transfer initiated under the scheme: negative feedback from the Payer Clearing Member


Az azonnali átutalás elutasítása a GIROInstant-ban vagy a Kedvezményezett fél Klíringtagja által
Sub-aggregátor
Aggregátor
Kedvezményezett fél Klíringtagja
GIROInstant
Fizető fél Klíringtagja
Fizető fél
EAM beolvasása Fizető fél Klíringtagjának vagy pénzforgalmi szolgáltatójának mobilalkalmazásán keresztül
GIROInstant
Azonnali átutalás fogadása, visszajelzés
pacs.008
Azonnali átutalás továbbítása
pacs.008
Azonnali átutalás küldése
pacs.002
Végleges állapotjelentés küldése a Fizető fél Klíringtagjának
pacs.002
Negatív visszajelző üzenet készítése, küldése az Aggregátornak; értesítés küldése Fizető félnek
Értesítés fogadása
Negatív visszajelző üzenet fogadása, Sub-aggregátor értesítése
pain.002
Negatív visszajelző üzenet továbbítása az Aggregátor részére
pain.002
Értesítés fogadása API hívással

1. The Payer scans the EAM using its portable multifunction device. The Payer payment service provider shall check the formality of the EAM, its expiry date, and the authentication code in its mobile banking application to ensure that no changes have been made to the information

contained in the EAM. The verification of the authentication code shall be carried out in accordance with the procedure detailed in the Certificate Storage chapter. If the verification finds everything correct, the Payer then has the option to approve the transfer instantly, reject the EAM or save it for later approval. Upon receipt of the instant credit transfer, the process continues as defined by the Payer Clearing Member.

2. It is the Payer Clearing Member's responsibility to ensure that the following checks are carried out in relation to the instant credit transfer:
   - Checking the validity period of the EAM before executing an instant credit transfer order,
   - duplication control,
   - Checking the coverage of the payer,
   - checking all other formal, legal, and business requirements for any instant credit transfer initiated via EAM.

   After the verification, the Payer Clearing Member shall transmit the data content of the instant credit transfer to the Beneficiary Clearing Member via the GIROInstant platform.
3. The GIROInstant platform sends a final status message on the rejection of an interbank instant credit transfer by the GIROInstant platform or the Beneficiary Clearing. The steps of the message exchange are the same as the message exchange for the instant credit transfer scheme.
4. The Payer Clearing Member will send a confirmation message via the GIROInstant platform in the form of a pain.002 confirmation message on the failed transfer. The message is addressed to the Aggregator. At the same time, the Payer Clearing Member shall also notify the Payer of the refusal to execute the instant credit transfer.
5. The GIROInstant platform sends the negative confirmation message to the Aggregator.
6. The Sub-aggregator receives the confirmation message via an API call and notifies the Beneficiary of the rejection of the instant credit transfer.

4 Features of the EAM

Title code of the EAM

The EAM is required to include the transaction title code to identify the payment situation, which must be indicated in the instant credit transfer initiated via EAM (in the Purpose Code field of the ISO20022 message). The title code is used to type the transaction. Claim codes can be freely chosen from the list of ISO External Code Set, but if the beneficiary is a natural person, the code "MP2P" should always be used. If the payee is a legal person or an individual entrepreneur, a different code than the one above should be used.

Register of sub-aggregators

The current list of sub-aggregators is contained in the "GIROInstant Send/Receive Limit and Payment Request Service Send/Receive Register and Single Data Entry Mode Service Sub-aggregator Register", which is published monthly by GIRO Zrt. This list contains the names and identifiers of the sub-aggregators. The structure of the Sub-aggregator identifier consists of 4 alphanumeric characters, the first three digits identifying the Sub-aggregator itself, the last character identifying its technical service provider, if any. The register will contain the identifier consisting of the first three digits.

Trade name management

If the Beneficiary's company name and the trade name used by the Beneficiary in the market differ, the trade name used by the brand may be more informative for the Payer, and therefore, in line with international trends, the trade name is also stored in the EAM, allowing it to be displayed on statements and cash substitute payment instruments.

Timeout for sending a confirmation message

In case of execution or rejection of both inter-bank and intra-bank payment transactions, the Payer Clearing Member has 5 seconds to prepare, send and deliver a confirmation message in ISO20022 pain.002 format to the Sub-aggregator via the Aggregator.

According to the MNBr., the five seconds are counted from the receipt of the final status report generated by GIROInstant in the case of an interbank instant credit transfer, and from the execution or rejection of the payment transaction in the case of an intra-bank instant credit transfer. The scheme does not include a system-wide timeout check for the transmission of the confirmation message.

Duplication check

The Payer Clearing Member must verify any previous use of the EAM for a period of 180 days to avoid multiple sending. The verification process is set up by the Payer Clearing Member, for which a check of the Beneficiary's internal transaction ID field is recommended. This field is globally unique identifier. If an instant credit transfer has been previously completed under an EAM, the Payer Clearing Member shall complete the confirmation message with error code AM05 to indicate the duplicate initiative.

Expired EAM

In the case of an EAM with an expired validity period, the Payer Clearing Member is not allowed to send a confirmation message due to the risk of compromising the performance of the system.

Rejection by the payer, re-use of EAM

If the Payer rejects the scanned EAM in the Mobile Banking application, this does not constitute a use of the EAM. In this case, no instant credit transfer is initiated and no confirmation message (in the form pain.002) is generated by the Payer payment service provider. It is therefore possible to reuse the EAM.

5 Reconciliation, reports

The hourly and daily reports generated by the GIROInstant platform include the confirmation messages as set out in Annex 25 of the BKR Rules of Procedure.

In case of non-receipt of the http response confirming the delivery of the pain.002 confirmation message, the Payer Clearing Member will resend the confirmation message according to the Participant and

GIROInstant Message Exchange[2] . The retransmission shall be repeated until the http reply confirming successful delivery is received.

It is not possible to send an investigation message to the confirmation message.

6 EAM input standard

Technical characteristics of EAMs that can be used to submit an instant credit transfer order

1. The EAMs that may be used for the submission of an instant credit transfer order are:
a) QR code-based data entry solution,
b) NFC-based data entry solution,
(c) a deep link-based data entry solution using a single resource locator (hereinafter referred to as 'URL') (hereinafter referred to as ' deep link-based data entry solution').

2. Physical design of a QR code-based data entry solution
2.1 QR code: code defined according to ISO/IEC 18004.
2.2 The QR code-based data entry solution shall be designed with the following technical content:
(a) the maximum size of the code is 24, i.e. 113 × 113 units, with 4 units of empty space around it;
b) the QR code has a minimum error correction capability of M level (15 percent loss recovery capability).

3. Physical design of an NFC-based data entry solution
NFC-based data entry solution: a short-range communication technology based on RFID (Radio Frequency Identification) standards, communicating at 13.56 MHz, as described in the ISO/IEC 14443 technology standard. The active communication mode defined in the standard can be used to issue a code to support the submission of an instant credit transfer order.

4. Deep link-based data entry solution
A deep link is a link that points directly to content within a mobile banking application instead of a web page. The purpose of a is to direct the user to the right place to perform a specific task, in this case to initiate a payment transaction in the bank's mobile banking application.

5. Data content
The data entry solutions defined in point 1 shall be designed with the following technical content:

5.1 The character set used in the code shall be encoded according to the UTF-8 standard. In addition to all the basic UTF-8 characters (in the range 32-126), only Hungarian accented characters (in the "extended" ASCII range above 128) may be used. The contents of the fields must be URL encoded. The maximum field lengths specified in the table in subsection 5.3 are after URL encoding.

5.2 All fields must be terminated with the character "/", regardless of whether the field contains data. The character '/' shall not be used either before the field with the zero-row number or after the last field. Data fields shall be displayed strictly in the order indicated in the table in subsection 5.3. The code

[2] Available at www.giro.hu after logging into GIROnline.

shall contain 20 data fields (even empty, zero characters long) and 19 '/' characters, regardless of the data content. Separator characters do not need to be URL coded.

5.3 The following data fields shall be used in the design of each data entry solution.

Field name	Serial number	Field length (after URL encoding)	Mandatory? (I/N)	Fixed length? (I/N)	Set of values, content
Mobile application URL	0	64	I	N	https://azonnalifizetes.hu
Identification code	1	3	I	I	ID registered by GIRO: "HCT"
Version number	2	3	I	N	ID registered by GIRO: "3"
Character set	3	1	I	I	"1"
Beneficiary BIC	4	11	N	N	BIC code of the Clearing Member of the Beneficiary (Sub-aggregator in case of an omnibus account) (Not filled in by the Beneficiary, to be determined from the Creditor table)
Name of beneficiary	5	70	I	N	The name of the Beneficiary (Sub-aggregator in case of an omnibus account), i.e. the name of the owner of the account number in the EAM
Trade name	6	35	N	N	Trade name of the Beneficiary (e.g. a trader)
Beneficiary IBAN	7	34	I	N	Beneficiary (sub-aggregator in case of omnibus account) account number

Field name	Serial number	Field length (after URL encoding)	Mandatory? (I/N)	Fixed length? (I/N)	Set of values, content
Total	8	15	N	N	HUF+12 num
Validity period	9	26	I	N	YYYYMMDDhhmmss+Z-OOOOOOOO Where YYYYMMDDhhmmss+Z is the time of code generation OOOOOO is the validity in minutes from the time of generation (offset, fixed length, padded with zeros from the left.) Z: time zone offset at the time of generation (winter: 1, summer: 2)
Payment status identifier	10	4	I	N	Id. EAM title code paragraph
Press release	11	70	N	N	Free text, unstructured message field of ISO messages
Shop identifier	12	35	I	N	Content: <bolt no. Sub-aggregator prefix.EAM type.tax number.platform identifier> see. Shop identifier paragraph
Merchant device (POS, cash register) ID	13	35	N	N	Cash machine or terminal ID. Identical to the beneficiary device.
Invoice or receipt identifier	14	35	N	N	
Client ID	15	35	N	N	
Beneficiary's internal transaction ID	16	35	I	N	Unique operation identifier See Beneficiary's internal transaction ID paragraph.

Field name	Serial number	Field length (after URL encoding)	Mandatory? (I/N)	Fixed length? (I/N)	Set of values, content
CallbackURL	17	230	N	N	It contains a URL or deep link that navigates the payer back to the status page of the payment interface that initiated the payment. The payer's mobile banking application shall, at the end of the payment, provide an option to open the URL in this field. The field URL shall be in encrypted format.
Field protection	18	3	I	I	See paragraph on field protection
Authentication code	-	136	I	N	See authentication code paragraph
Space requirements for separators		19	I	I	hyphenation instead of "/" sign for separator character

6. Field protection

The field protection data element indicates the so-called authentication code generated by the application of EAMs from which data fields values have been generated, thus prohibiting the modification of which fields. At maximum protection, all 18 data fields are protected by the validation code. Minimum protection means the data fields that must be protected at all costs. The Sub-aggregator indicates its need for field protection in the authentication request. The Payer Clearing Member shall take into account the value of the field protection, and shall consider for the validation those data fields with a field protection value of 1 as shown in the table below.

Serial number	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Maximum protection	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Maximum protection URL_SAFE_BASE64 without padding	-						-						-					

Minimum protection	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	1	1	1
Minimum protection URL_SAFE_BASE64 without padding	code value: "7"						code value: "t"						-					

Mobile banking applications must ensure that the "amount" and "message" fields can be modified if they were not protected fields. The Customer ID field on the Payer's page cannot be modified even if it was modifiable in EAM.

The field protection field is binary content in URL_SAFE BASE64 without padding characters on 3 characters. If the local value is 1, the field is protected, if it is 0, it is not. Fields that are not protected shall be omitted from the check with the separator character. Unprotected fields are free to change until the payment is started.

7. Domain name
Mobile banking applications must be registered to the central domain (in the central register of mobile banking applications) as described in Chapter 8.

8. Authentication code
The following authentication code structure shall be used in the EAM.

8.1. Serial number of the certificate containing the key used to generate the security code, given in hexadecimal, up to a maximum of 7 lengths.
8.2. Separating point.
8.3 Security code, maximum length 128 characters, in URL_SAFE BASE64 without padding characters. The trust model of the security code is based on a public key infrastructure (PKI). Security code shall be generated and managed in an ISO/IEC 9594-8 elliptic curve scheme using a P-384 type key. The security code shall be provided in P1363 format (only the two integer values from ASN.1 sequences are transmitted) and SHA-384 hash algorithm shall be used.

9. Shop ID (ShopID)

The structure of the ShopID field consists of the following 5 mandatory fields:

1. **Shop serial number** - max 10 characters (to be provided by the Beneficiary)

Separator character" ."

2. **Prefix identifying the sub-aggregator** - 4 characters (identifier defined by GIRO)

Separator character" ."

3. **EAM type:** 1-7 - Q-D-N combination - max 1 character (1: QR, 2: DL, 3: NFC4:QR+DL, 5: QR+NFC, 6: DL+NFC, 7: QR+DL+NFC, only 1,2,3 codes can be used for now)

Separator character" ."

4. First 8 characters of the **beneficiary's tax** number/if no tax number, a unique identifier generated by the Sub-Aggregator, starting with the character "E". The other identifier may be used by Sub-Aggregators to indicate groups of customers (however, they must ensure that the shop numbers within the customer group are unique).

Separator character" ."

5. **Platform ID**: BEI - Max 8 characters

példa1: 1234567890.SUBA.1.12345678.INNOHUH0

10. Beneficiary's internal transaction ID
The structure of the Creditor's internal transaction ID (CredTranID) field is as follows: an internal transaction ID of up to 17 characters, provided by the Creditor, followed by a separator "_", followed by a unique transaction ID (UTI) of up to 17 characters generated by the aggregator. With this training rule, each EAM becomes globally unique.

példa1 „12345678912345678_12345678912345678"

If the beneficiary does not provide an identifier, only the UTI identifier of the aggregator is provided.
example2 "_12345678912345678"

7 Rejection codes

The Payer Clearing Member may communicate the reason for rejecting an instant credit transfer order initiated via EAM by providing the reasons listed in the ISO20022 pain.002 Message Application Guide.

8 Central register of mobile banking applications

8.1 General overview

This chapter describes the process of registration and deletion in the central register of mobile banking applications. An instant transfer order initiated via EAM may only be initiated using a mobile banking application that has been previously registered by the Payer's payment service provider in the central register of mobile banking applications maintained by GIRO Zrt.

In relation to the central register of mobile banking applications, the following components are distinguished:

- A file (JSON) containing registered mobile banking applications, available on a static web page, which is used to keep a current register of registered mobile banking applications. **GIRO Zrt. maintains a test and live mobile banking register, which is** placed in a folder corresponding to the operating system (Android or iOS) on the static website designed for this purpose.
    - Landing page: in case the payment is initiated from a device that does not have a mobile banking application listed in the central register of mobile banking applications, the Payer will be directed to this page. This page provides instructions on the list of mobile banking applications included in the central register of mobile banking applications, installation options and information.
- Customer Interface (hereinafter referred to as JIRA): payment service providers of Payers(hereinafter referred to as the "Customer Side") can initiate the registration or deletion of their mobile banking application in JIRA by submitting a form to the test or live registry in the JIRA interface. From JIRA, the submitted data will be automatically transferred to the register available on the static website. The Payer payment service provider will arrange for the necessary authorisations to be ordered by the users.

In the document, the term mobile operating systems (iOS, Android) refers not only to operating systems used on mobile phones, but also to operating systems available on other portable multifunctional devices as defined in the MNBr.

8.2 Technical overview

If the mobile operating system finds an installed mobile banking application, it will open it and pass the parameters. Multiple applications can be subscribed to a domain, so when using a shared domain, it is not necessary to know in advance which mobile banking application is on the payer's portable multifunction device, using a shared domain will launch the mobile banking application that is on the payer's device.

- For iOS, the last installed app (among the banking apps on the user's device) is launched by the device based on the domain.
- In the case of Android, the user chooses from a list of banking applications installed on the device, so that he or she can decide which application receives the necessary parameters. It is also possible for the user to set a default from a list, which will then be opened instead of a list.

8.3 The actors in the process

Payer's payment service provider

Register your current mobile banking application in use in the central register of mobile banking applications via JIRA, in order to enable the Payer to submit the instant credit transfer initiated via EAM on his device. The mobile banking applications that are no longer current and no longer in use are deleted from the central register of mobile banking applications via JIRA.

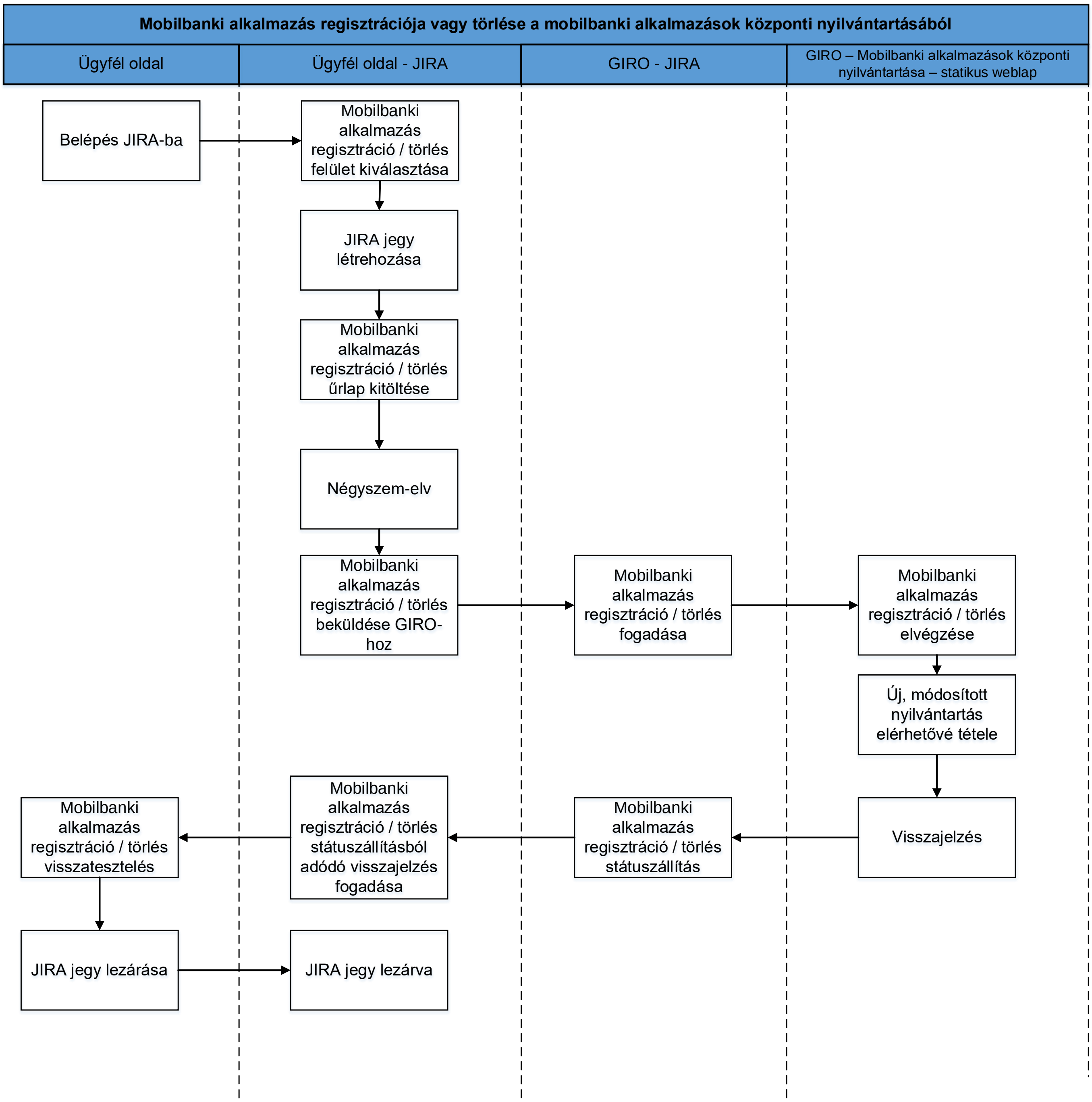
GIRO Zrt. as the central registry for mobile banking applications

GIRO Zrt. maintains the central register of mobile banking applications, which contains the list of mobile banking applications running on the portable multifunctional device, which is necessary to automatically launch the mobile banking application after the EAM is read/scanned.

8.4 Mobile banking application registration flowcharts

8.4.1 Successful registration/cancellation process

6. ábra Successful registration or cancellation flowchart


Mobilbanki alkalmazás regisztrációja vagy törlése a mobilbanki alkalmazások központi nyilvántartásából
Ügyfél oldal
Ügyfél oldal - JIRA
GIRO - JIRA
GIRO – Mobilbanki alkalmazások központi nyilvántartása – statikus weblap
Belépés JIRA-ba
Mobilbanki alkalmazás regisztráció / törlés felület kiválasztása
JIRA jegy létrehozása
Mobilbanki alkalmazás regisztráció / törlés űrlap kitöltése
Négyszem-elv
Mobilbanki alkalmazás regisztráció / törlés beküldése GIRO-hoz
Mobilbanki alkalmazás regisztráció / törlés fogadása
Mobilbanki alkalmazás regisztráció / törlés elvégzése
Új, módosított nyilvántartás elérhetővé tétele
Visszajelzés
Mobilbanki alkalmazás regisztráció / törlés státuszállítás
Mobilbanki alkalmazás regisztráció / törlés státuszállításból adódó visszajelzés fogadása
Mobilbanki alkalmazás regisztráció / törlés visszatesztelés
JIRA jegy lezárása
JIRA jegy lezárva

Steps in the process:

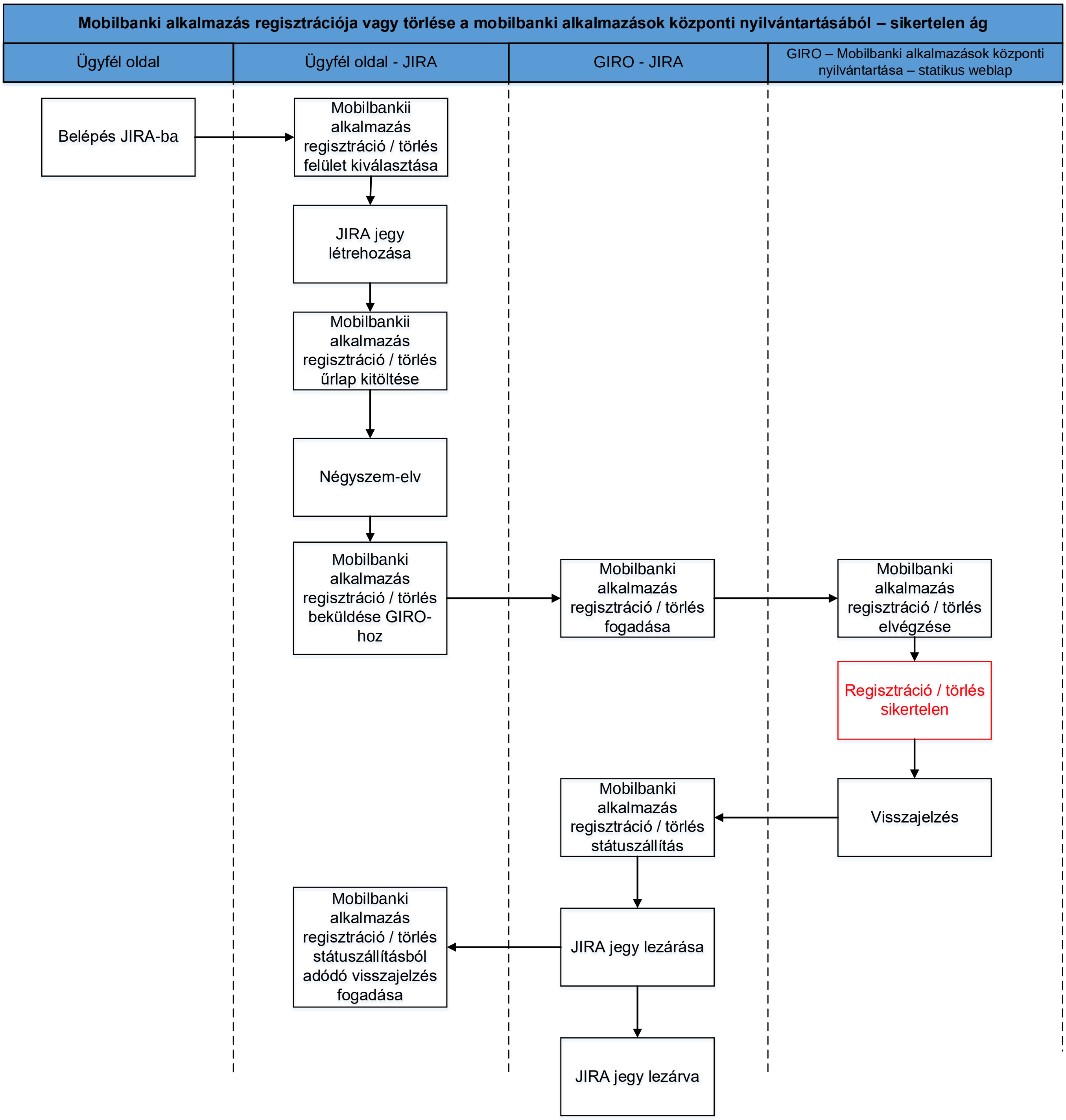
1. Login to JIRA: the client-side user logs into JIRA.
2. Mobile banking application registration/cancellation selection: if the logged in user has the appropriate authorisation, he/she clicks on the JIRA project.
3. Mobile banking application registration/cancellation form completion: after completing the form for the selected operating system, JIRA automatically sends a notification of the **ticket with** "**NEW"**

status to the client-side users who are authorized to record the four-eyes principle validation. (The statuses and JIRA workflow are described later in this document.)

4. Four-eyes principle: client-side user with appropriate authorization approves the mobile banking application registration / cancellation JIRA ticket.
5. Automatic status setting and e-mail notification: after the four-eyes principle is approved, the JIRA ticket is automatically set to "SENT TO GIRO" status, and the system sends a notification to GIRO.
6. Once received by the GIRO, the ticket will automatically be set to "PROGRESS" status.
7. Registration / cancellation -no intervention required- branch: if the mobile banking application to be registered is already in the register or the mobile banking application to be cancelled is not in the register, GIRO will consider this as a successful branch, no intervention is required and will automatically set the status of the process to "APPROVED" and record the information on the ticket.
8. Reload updated JSON file: after successful validation, GIRO generates the updated JSON file according to the given JIRA ticket (adds the mobile banking application to the register in case of registration, deletes the mobile banking application from the register in case of deletion) and reloads it back to the static web page.
9. Update JSON file: after receiving the JSON file, the next action is to "sharpen" the new file.
10. JIRA ticket status setting: in case of successful "arming", GIRO will automatically set the JIRA ticket to "APPROVED" status. In case of "APPROVED" status, JIRA will automatically send a notification to the client-side user who will close the JIRA ticket after the client-side back-check.

8.4.2 Unsuccessful registration/cancellation process

7. ábra Register or delete mobile apps


Mobilbanki alkalmazás regisztrációja vagy törlése a mobilbanki alkalmazások központi nyilvántartásából – sikertelen ág
Ügyfél oldal
Ügyfél oldal - JIRA
GIRO - JIRA
GIRO – Mobilbanki alkalmazások központi nyilvántartása – statikus weblap
Belépés JIRA-ba
Mobilbankii alkalmazás regisztráció / törlés felület kiválasztása
JIRA jegy létrehozása
Mobilbankii alkalmazás regisztráció / törlés űrlap kitöltése
Négyszem-elv
Mobilbanki alkalmazás regisztráció / törlés beküldése GIRO-hoz
Mobilbanki alkalmazás regisztráció / törlés fogadása
Mobilbanki alkalmazás regisztráció / törlés elvégzése
Regisztráció / törlés sikertelen
Visszajelzés
Mobilbanki alkalmazás regisztráció / törlés státuszállítás
Mobilbanki alkalmazás regisztráció / törlés státuszállításból adódó visszajelzés fogadása
JIRA jegy lezárása
JIRA jegy lezárva

Steps in the process:

1. Login to JIRA: a client-side user with the appropriate authorization and privileges logs into JIRA.
2. Mobile banking application registration / deletion selection: if the logged in user has the appropriate authorisation, he/she clicks on the JIRA project.
3. Mobile banking application registration/cancellation form completion: after completing the form for the selected operating system, JIRA automatically sends a notification of the **ticket with "NEW"**

status to the client-side users who are authorized to record the four-eyes principle validation. (The statuses and JIRA workflow are described later in this document.)

4. Four-eyes principle: client-side user with appropriate authorization approves the mobile banking application registration / cancellation JIRA ticket.
5. Automatic status setting and e-mail notification: after the four-eyes principle is approved, the JIRA ticket is automatically set to "SENT TO GIRO" status, and the system sends a notification to GIRO.
6. Once received by the GIRO, the ticket will automatically be set to "PROGRESS" status.
7. The update fails for some reason (e.g. the client has submitted data that cannot be registered).
8. JIRA ticket status setting: in case of unsuccessful "arming", GIRO will automatically set the JIRA ticket to "FAILED" status. From "FAILED" status, GIRO can set the ticket to "CLOSE" status, in which case JIRA will send an automatic notification to the client-side user.

8.5 Mobile banking application registration and cancellation features

The interface for registering and deleting mobile banking applications for instant credit transfers initiated via EAM in JIRA is only available to payment service providers contracted for the EAM add-on service. Users of the Payer Payment Service Provider (including the Payment Initiation Service Provider) with the appropriate authorisation will be able to see this interface, users without such authorisation will not. All authorised users will only see the JIRA tickets and associated information in which they are involved.

8.5.1 JIRA forms field description ai

The forms available in the JIRA interface (which can be filled in to submit a registration/cancellation change request) are described in the tables below.

Within the EAM Domain registration project, forms are available after selecting the operating system (iOS or Android).

1. táblázat - Form field description for iOS operating system

Field name	Mandatory / Optional	Description
Summary	Required	Mandatory field in JIRA by default, blank by default, to be filled in by the payment service employee, name of the ticket containing the change request.
Registration / Delete	Required	The type of change request can be selected in this field by the payment service employee: **registration or cancellation**. If registered, the mobile banking application is added to the

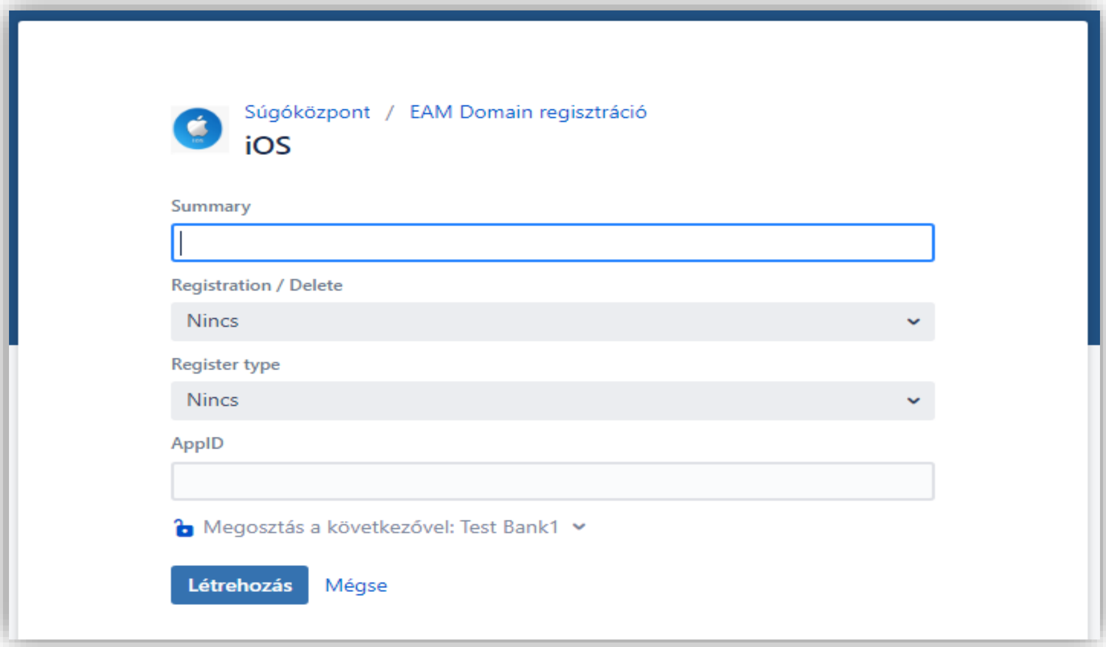
		register, if deleted, the mobile banking application is removed from the register.
Register type	Required	The type of record can be selected in this field by the payment service employee: **test or live environment.** If the test environment is selected, the operation is performed in the test register, if the live environment is selected, the operation is performed in the live environment.
AppID	Required	The mobile banking application ID (appID) of the application to be registered or deleted.

2. táblázat - Field description of a form for Android operating system

Field name	Mandatory / Optional	Description
Summary	Required	Mandatory field in JIRA by default, blank by default, to be filled in by the payment service employee, name of the ticket containing the change request.
Registration / Delete	Required	The type of change request can be selected in this field by the payment service employee: **registration or cancellation**. If registered, the mobile banking application is added to the register, if deleted, the mobile banking application is removed from the register.
Register type	Required	The type of record can be selected in this field by the payment service employee: **test or live environment.** If the test environment is selected, the operation is performed in the test register, if the live environment is selected, the operation is performed in the live environment.
package_name	Required	Identifier of the mobile banking application to be registered or deleted (package_name).
SHA-256 Cert. Fingerprint	Required	The fingerprint ID (SHA-256) of the mobile banking application to be registered or deleted, which is mandatory for Android applications.

8.5.2 JIRA form screenshots

8. ábra JIRA Screenshot - iOS



Súgóközpont / EAM Domain regisztráció

iOS

Summary

Registration / Delete

Nincs

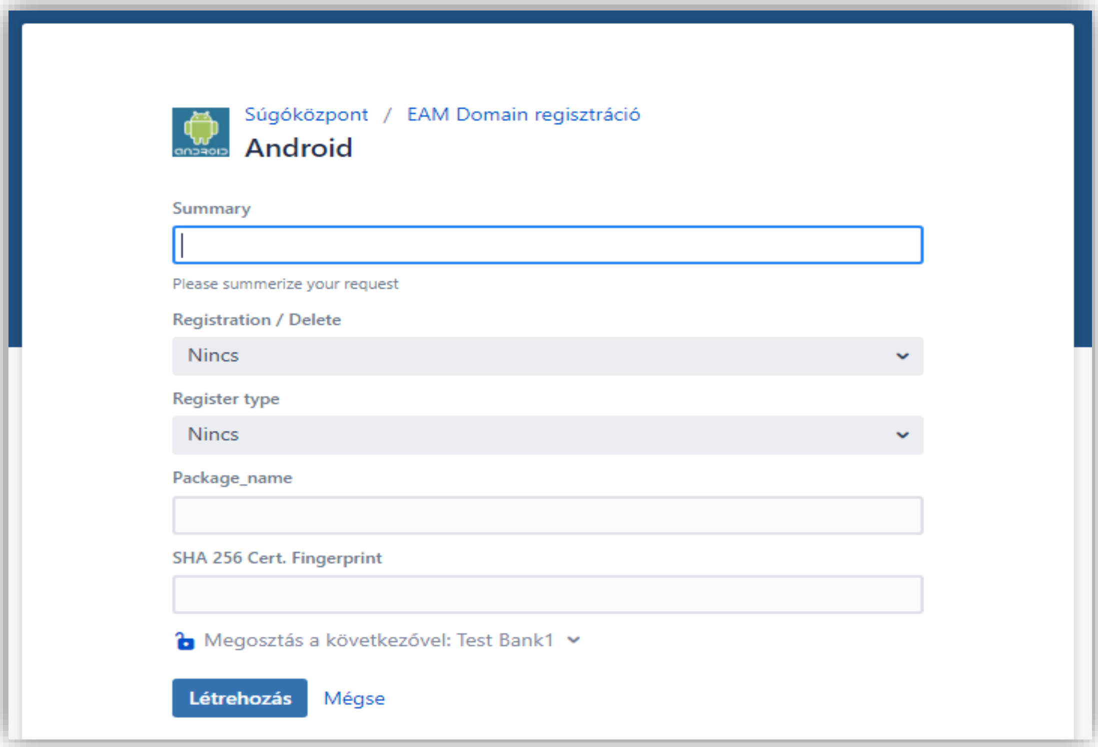
Register type

Nincs

AppID

Megosztás a következővel: Test Bank1

9. ábra JIRA screenshot - Android



Súgóközpont / EAM Domain regisztráció

Android

Summary

Please summerize your request

Registration / Delete

Nincs

Register type

Nincs

Package_name

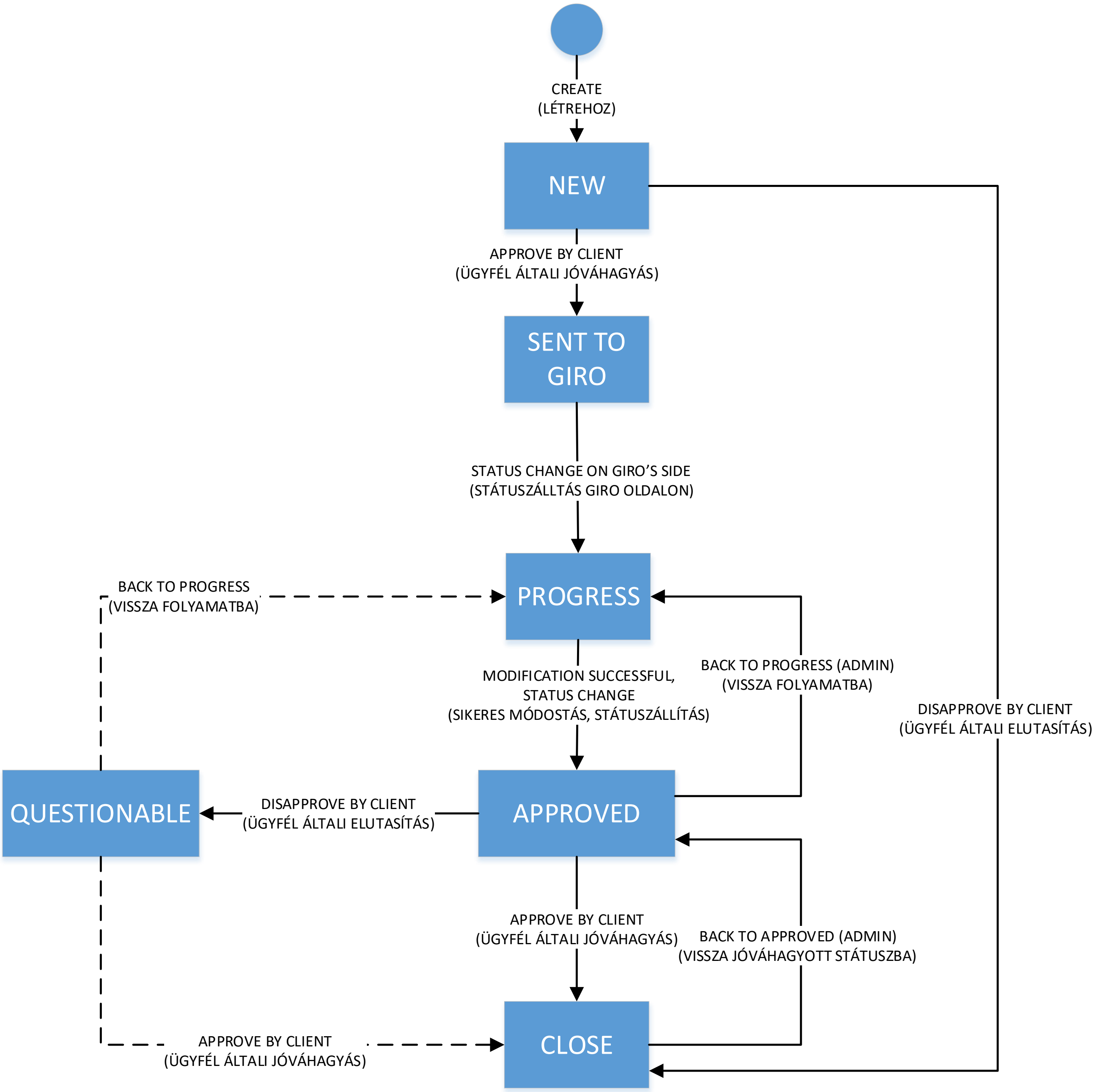
SHA 256 Cert. Fingerprint

Megosztás a következővel: Test Bank1

8.5.3 JIRA workflow

The workflow of JIRA is illustrated in the following diagram and description.

10. ábra JIRA workflow


CREATE
(LÉTREHOZ)
NEW
APPROVE BY CLIENT
(ÜGYFÉL ÁLTALI JÓVÁHAGYÁS)
SENT TO GIRO
STATUS CHANGE ON GIRO'S SIDE
(STÁTUSZÁLLTÁS GIRO OLDALON)
BACK TO PROGRESS
(VISSZA FOLYAMATBA)
PROGRESS
MODIFICATION SUCCESSFUL, STATUS CHANGE
(SIKERES MÓDOSTÁS, STÁTUSZÁLLÍTÁS)
BACK TO PROGRESS (ADMIN)
(VISSZA FOLYAMATBA)
DISAPPROVE BY CLIENT
(ÜGYFÉL ÁLTALI ELUTASÍTÁS)
QUESTIONABLE
DISAPPROVE BY CLIENT
(ÜGYFÉL ÁLTALI ELUTASÍTÁS)
APPROVED
APPROVE BY CLIENT
(ÜGYFÉL ÁLTALI JÓVÁHAGYÁS)
BACK TO APPROVED (ADMIN)
(VISSZA JÓVÁHAGYOTT STÁTUSZBA)
APPROVE BY CLIENT
(ÜGYFÉL ÁLTALI JÓVÁHAGYÁS)
CLOSE

Create: the client-side user initially creates the JIRA ticket by filling in the form, which is then displayed in the system.

STATUS - NEW: The status of the JIRA ticket according to which the client-side four-eyes-principle check is in progress.

Approve by client: the client-side user who validates the JIRA ticket forwards the generated JIRA ticket to the GIRO after a four-eyes-principle check. This step allows the client-side user to set the ticket to SENT TO GIRO status.

Disapprove by client: the client-side user checking the JIRA ticket rejects the ticket on a four-eyes-principle check, which is then set to CLOSE status. This step allows the client-side user to set the ticket to CLOSE status.

STATUS - SENT TO GIRO: The status of the JIRA ticket according to which the ticket has been created by the client-side user and has been checked by the client-side four-eye-principle and submitted to GIRO.

Status change on GIRO's side: the JIRA ticket will be changed to PROGRESS status on GIRO's side after receipt. This status means that processing is in progress. With this step, the ticket is changed to PROGRESS status.

STATUS - PROGRESS: The status of the JIRA ticket according to which the JIRA ticket has been uploaded for transmission and the record is in the process of being updated.

Modification successful, status change: the modification request in the JIRA ticket (be it registration or deletion) has been successfully uploaded, the register has been modified according to the request. With this step, GIRO will set the ticket to APPROVED status.

STATUS - APPROVED: The status of the JIRA ticket according to which the change request in the JIRA ticket has been successfully uploaded to the registry. This is the status of the ticket even if there is a duplicate registration or a request for cancellation is received for a mobile banking application that is not registered (in this case GIRO has no responsibility, it is considered a successful branch).

Approve by client: the change request in the JIRA ticket has been successfully uploaded according to the GIRO feedback, and the success of this change is confirmed on the client side. This step allows the client-side user to set the ticket to CLOSE status.

Disapprove by client: the change request in the JIRA ticket was successfully uploaded according to GIRO feedback, but the change is not confirmed as successful on the client side. This step allows the client-side user to set the ticket to QUESTIONABLE status.

STATUS - QUESTIONABLE: The status of the JIRA ticket according to which the change request in the JIRA ticket has been successfully uploaded to the register by GIRO, but their own verification on the client side does not confirm the success of the register update.

Approve by client: the change request in the JIRA ticket has been clarified and the success of the change is confirmed on the client side. This step allows the client-side user to set the ticket to CLOSE status.

Back to PROGRESS: The change request in the JIRA ticket has been successfully uploaded according to the GIRO feedback, but the customer has not confirmed the success of the change, so GIRO will initiate a re-upload. This step will allow GIRO to set the ticket to PROGRESS status.

STATUS - CLOSE: The status of the JIRA ticket is that the change request in the JIRA ticket has been successfully uploaded to the register by GIRO and the success of this change is confirmed on the client side, the JIRA ticket is closed.

Back to APPROVED (Admin): technical transition, which is only visible on the admin page.

Back to PROGRESS (Admin): technical transition, which is only visible on the admin page.

8.5.4 JIRA deadlines

The following deadlines must be met by the client and GIRO side in the JIRA interface:

- Tickets received with SENT TO GIRO status must be converted to APPROVED status by 23:59 on the 5th working day (T+5) after receipt. In practice, this means that during this period, GIRO ZRT. must transfer the received change request (registration or cancellation) to the register.
- A ticket with APPROVED status must be changed by the client-side user to CLOSE status with APPROVE or to QUESTIONABLE status with DISAPPROVE by 23:59 on the 5th business day (T+5) after the status is set. During this time interval, you must check back on your own side that the modified register is correct.

9 Certificate Storage

9.1 General overview

GIRO Zrt. maintains a certificate storage for the central registration of public keys and revoked certificate lists (hereinafter: CRL list) and ensures its availability by the Clearing Member every day of the calendar year, 0-24 hours, with 99.7% availability per month, in order to verify the authenticity of the instant credit transfer initiated using the EAM.

The certificate storage implemented by GIRO Zrt. is responsible for storing and making available to the Payer Payment Service Providers the private key pairs used for the signatures used in EAM, the public keys. These public keys are necessary for the execution of instant credit transfers initiated via the EAM. The Aggregator shall upload the public keys and the CRL list to the certificate storage provided by GIRO Zrt.

It is the responsibility of the Payer payment service provider to order the necessary privileges to access the certificate storage.

9.2 Certificate management features, rules

The certificate storage maintained by GIRO Zrt. has the following characteristics:

- The certificate storage is implemented by an LDAP database.
- Communication between the certificate storage and the payment service providers takes place via the GIRONet.
- The certificate storage supports the following functionalities:
  - receive uploaded public keys
  - storage of uploaded public keys
  - delete uploaded public keys
  - Receive CRL list
  - Store CRL list
  - Delete CRL list
  - provide a public key query
  - ensure all public keys are retrieved
  - Provision for querying the CRL list
- The list of public keys is the list of uploaded public keys issued by the Aggregator. A public key has an expiry date, may be compromised or revoked.
- Public keys can be uploaded to a certificate storage designed to store public keys for EAM certificates using API calls. The upload requires a GIROLock object authentication certificate and EAM certificate upload privileges from the Aggregator.
- The certificate storage can be accessed via the closed GIRONet provided by GIRO Zrt., to retrieve the certificate from the certificate storage the client must have GIRONet access and it is necessary to order the GIRONet channel setup required to access the certificate storage by completing the appropriate form and submitting it to GIRO Zrt.
- Payment service providers pre-fetch the uploaded public keys, which are cached in their own back-end systems to ensure a fast customer experience, and their mobile banking application does not query the certificate storage for public keys before each transaction, but rather this back-end system.

- Every day, the Aggregator uploads a list of public keys that have been withdrawn with a frequency of between 5 and 10 minutes (no more than 5 minutes and no less than 10 minutes).
- The uploaded CRL list available in the certificate storage maintained by GIRO Zrt. is always the current, most recent revoked certificate list.
- Payment service providers will also query the CRL list every day with a frequency of between 5 and 10 minutes (no more frequently than 5 minutes and no less frequently than 10 minutes).
- In the case of a compromised, revoked certificate, the Aggregator is required to issue an extraordinary CRL list. In such a case, the payment service providers shall instantly initiate a query for the CRL list after notification by GIRO Zrt.
- This CRL list is also cached in their own back-end systems, just like the public keys, and your mobile banking application does not query the certificate storage for the CRL list before each transaction, but this back-end system.
- Once uploaded, both the uploaded public keys and the CRL list are instantly available for query by payment service providers in the certificate storage.
- For technical details on uploading and retrieving public keys, CRL list, please refer to the EAM Certificate Storage Development and Management Guide.[3]

[3] Available at www.giro.hu after login.