EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital Euro Scheme Rulebook –

Annex D2

Back-end implementation specifications #4

Risk and Fraud

IMPORTANT NOTICE:

This rulebook is an interim draft of the digital euro rulebook developed by RDG

A separate set of pilot documentation has been developed that can be found here.

Although the pilot documentation is based on the draft rulebook, the draft rulebook should not be used for pilot or implementation purposes.

Rulebook version:	0.91
Status:	DRAFT
Date:	02/07/2025

DISCLAIMERS FOR DRAFT RULEBOOK v0.91

Preliminary and non-binding nature of version 0.91

This document represents a preliminary draft version (version 0.91) of the digital euro scheme rulebook and reflects the ECB's continuous effort to develop a draft rulebook in close cooperation with the Rulebook Development Group (RDG)[1], comprising senior representatives from European associations representing both the supply and demand side of the retail payments market. Version 0.91 is non-binding and does not necessarily reflect the final views of the ECB, the Eurosystem, the RDG, or any of its members or their constituencies.

No reliance for implementation

Due to its preliminary nature, the draft rulebook version 0.91 is not intended for use as a basis for implementing any systems, processes, or policies related to the digital euro or to the beta digital euro in a Digital Euro Pilot context. Any such actions, prior to the publication of the officially approved rulebook, are under actors' own responsibility.

[1] For more information on the RDG, refer to:
https://www.ecb.europa.eu/euro/digital_euro/timeline/rulebook/html/index.en.html

PREAMBLE

The draft digital euro scheme rulebook is being developed by the Eurosystem together with the support from the digital euro scheme rulebook development group (RDG). The current draft rulebook (v0.91) has been further developed compared to the last version 0.9 of the draft rulebook, which was commented by the RDG and its constituencies. The current draft has been advanced in both structure and content based on the RDG comments received, further elaborations and discussions, and benefited from the various RDG workstreams.

The current version of the rulebook is based on the European Commission's 2023 proposal for a regulation on the establishment of the digital euro (2023/0212/COD) and the Regulation on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro (2023/0211/COD). Given both proposals are currently progressing through the legislative process, and subject to amendments from the EU co-legislators, the rulebook will require updates once both regulations have been finalised for adoption. Additionally, other areas of the rulebook will be further developed in line with ongoing elaborations on subject matters and decisions by the Governing Council of the ECB or are dependent on the work of service providers.

As a result, all along this draft rulebook, text highlighted in yellow refers to placeholders to be updated at later stage when associated decisions or developments are made. It is worth noting that the draft rulebook assumes a single-account set-up for individual digital euro end-users, which deviates from the possibility of having multiple digital euro payment accounts as implied by the European Commission's 2023 proposal for a regulation on the establishment of the digital euro.

The Eurosystem is also cognisant that political agreement has been achieved on the Payment Services Regulation (PSR) and the Third Payment Services Directive (PSD3). The agreed measures must be formally adopted by the European Parliament and the Council of the European Union before they enter into force. The rulebook will be updated accordingly.

The purpose of the current draft is to update the RDG and its constituencies on the progress made following the market consultation, coordinated by the RDG and concluded on 31 October 2025, and to serve as a basis for the further development of the draft rulebook. This document represents a preliminary draft version which has not yet been subject to a general language and editorial review.

Table of Contents

8.	**Risk and fraud management service**	**5**
8.1.	Service Description	5
8.2.	Distributing PSP requirements	5
8.2.1.	*Function Description*	*5*
8.2.2.	*Interface description*	*5*
8.3.	Acquiring PSP requirements	12

1. Risk and fraud management service

1.1. Service Description

PSPs of the digital euro environment will operate their own systems and apply appropriate fraud prevention, risk management, and detection measurement rules. The central fraud detection mechanism shall enrich the PSPs' individual fraud risk view with insights on patterns and anomalies from a central infrastructure level perspective for online digital euro transactions.

The general fraud detection and prevention mechanism offered by DESP does not serve as a replacement for any deficiencies in individual PSPs' fraud and risk management processes. It can support and augment the activities at PSP level, by providing additional insights that may otherwise not be available to individual PSPs to support their fraud prevention activities.

Fraud prevention shall comprise activities during the payment validation process, in support of PSPs taking decisions to identify fraudulent or suspicious transactions before these are approved by the PSPs (i.e. by scoring the risk profile of a transaction) and afterwards (i.e. identifying fraudulent patterns across settled transactions and including a feedback loop to fine-tune the predictive capabilities of the scoring tool).

1.2. Distributing PSP requirements

1.2.1. Function Description

Risk score request

The risk score request is on the critical path in case of P2P and e-commerce payments. The PSP cannot finalise the payment before it receives the risk score from DESP. The PSP does not have to wait for the risk score request result from DESP before finalising the payment in case of POS-based transactions.

Feedback loop

The PSP is required to provide the component with information regarding confirmed fraudulent transactions on a daily basis. Previously reported transactions that were subsequently re-assessed as non-fraudulent should also be included in the participant's feedback loop.

1.2.2. Interface description

This section provides a detailed description of the interface designed to facilitate communication between PSPs and the DESP for the risk and fraud management service. The interface is based on RESTful API principles and the data format utilised is JSON (JavaScript Object Notation).

1.2.2.1. Overview of covered scenarios

Risk score request

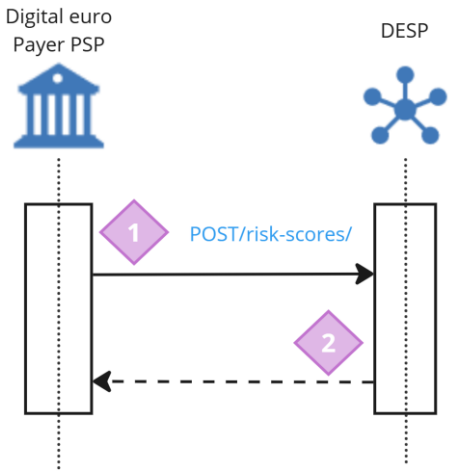

Figure 1 Risk score request flow

API call	Description	Covered in section
1	Payer PSP submits risk score request to DESP.	POST/ risk-scores - Request
2	DESP validates the request and sends the risk score to the payer PSP.	POST/ risk-scores – Response

Feedback loop

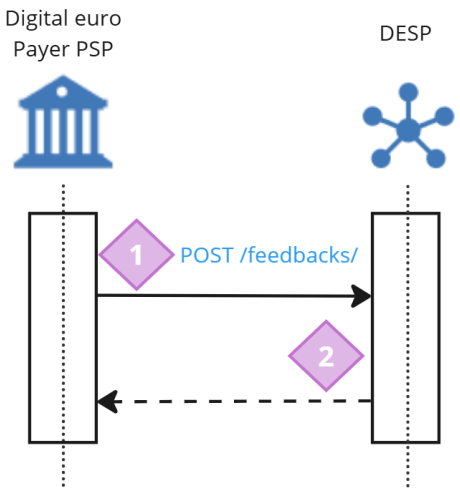

Figure Feedback loop flow

API call	Description	Covered in section
1	Payer PSP submits relevant data of fraudulent or reassessed transactions to DESP.	POST/feedbacks - Request
2	DESP confirms receipt of the request to the Payer PSP.	POST/feedbacks - Response

1.2.2.2. API endpoint overview

DESP API endpoints: For Payer PSPs to submit requests to DESP.

API nr	Description	Sending p[arty	Exposing party	Covered in section
1	Risk score request.	Payer PSP	DESP	POST/ risk-scores
2	Feedback loop.	Payer PSP	DESP	POST/feedbacks

PSP API endpoints: For DESP to send requests to PSPs.

Not applicable.

1.2.2.3. DESP API for PSPs to send requests to DESP

1.2.2.3.1. POST/ risk-scores

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/risk-scores/	RISKSCORE	PSPs request risk score

1.2.2.3.1.1. POST/ risk-scores – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:**

Data element	Element description	Type	Length	Presence indicator
Risk score request ID	Reference ID of the request.	STR	36	M

Request body fields

Data element	Element description	Type	Length	Presence indicator
Payment ID	Resource identifier for the submitted payment transaction.	STR	TBA	M
UETR	Unique end-to-end transaction reference of the submitted payment transaction.	STR	36	M
Payer PSP ID	BIC of the payer PSP holding the payer's digital euro payment account.	STR	11	M
Placeholder for further data elements				
Transaction session data				
Device IP	Device internet protocol address-range.	STR	15	M
Placeholder for further data elements				

1.2.2.3.1.2. POST/ risk-scores – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 200.

Data element	Element description	Type	Length	Presence indicator
Below rows repeat per fraud type				
Fraud type code	See “Fraud types” reference data table.	SSET	3	M
Fraud risk score	Possibility of the transaction falling into the particular fraud type.	N	4	M

1.2.2.3.2. POST/feedbacks

Applicable endpoint and method

Method	Endpoint	Resource	Description
POST	/v1/feedbacks/	FEEDBACK	PSP’s feedback on fraudulent transactions.

1.2.2.3.2.1. POST/feedbacks – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:**

Data element	Element description	Type	Length	Presence indicator
Feedback loop request ID	Reference ID of the request.	STR	TBA	M

Request body data elements

Data element	Element description	Type	Length	Presence indicator
Rows below repeat per transaction				
Payment ID	Resource identifier for the submitted payment transaction.	STR	TBA	M
UETR	Unique End-to-end Transaction Reference of the submitted payment transaction.	STR	36	M
Payer PSP ID	BIC of the payer PSP holding the payer's digital euro payment account.	STR	11	M
Transaction date and time	Date and time of the reported transaction.	ISODateTime	10	M
PSP fraud status	The fraud status set by the PSP: • Fraudulent transaction • Not fraudulent transaction	SSET		C, not fraudulent status is to be set only if the particular transaction was reported as fraudulent before
Fraud type code	See "Fraud types" reference data table.	SSET	TBA	C, filled in case the transaction is marked fraudulent M

1.2.2.3.2.2. POST/feedbacks – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 200.

1.2.2.4. PSP APIs for PSPs to receive requests from DESP

Not applicable.

1.3. Acquiring PSP requirements

Not applicable.