EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital Euro Scheme Rulebook – Annex D2 Back-end implementation specification #3 SEPI service

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:	02/07/2026

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

1.1. Service description 5

1.1.1. Function description 7

1.1.2. Interface description 7

1.1.2.1. Overview of covered scenarios 7

1.1.2.2. Overview of API endpoints 8

1.1.2.3. DESP API for PSPs to send requests to DESP 8

1.1.2.3.1. POST/cryptogram-validations – Request 8

1.1.2.3.2. POST/cryptogram-validations – Response 9

Annex A: SEPI non-NFC service v0.90 Carried-over Content for Information Only **10**

A.1 Service description 10

A.1.1 Distributing PSP requirements 14

A.1.1.1 Function description *14*

A.1.1.2 Interface description *14*

A.1.2 Acquiring PSP requirements 29

A.1.2.1 Function Description *29*

A.1.2.2 Interface description *29*

1.1. Service description

SEPI service plays a key role in enabling online digital euro payments with NFC (near field communication) method.

Individual end users that have NFC capable devices can enrol to the service to perform proximity payments using their online digital euro holdings.

To facilitate NFC payments, SEPI supports various functions:

- End user enrolment and lifecycle management that are in the domain of the front-end specifications (covered in frontend specifications: XXX)
- Application cryptogram validation that is in scope of the back-end specifications and is detailed out in this document.

The following section provides a high-level summary of SEPI's role in the end-to-end process, offering greater context for its overall capabilities, while only the application cryptogram validation is in scope of this document.

Enrolment and lifecycle management

Upon end user enrolment, SEPI generates the enrolment data including a surrogate value and the first session key set. The session keys are later going to be used for application cryptogram generation.

SEPI is also responsible for surrogate value activation and deactivation and subsequent session key set generation.

SEPI itself does not directly interact with end-user mobile devices. The data is deployed to the mobile device via the relevant HCE components.

Application cryptogram validation

This function is in scope of the back-end specifications for the distributing PSPs. The NFC payment transaction's uniqueness and authenticity is validated by SEPI with the support of an application cryptogram. The application cryptogram is generated during each NFC payment transaction.

The application cryptogram is generated following a successful user authentication and completion of data exchange between the payee and payer devices based on the CPACE standard.

The HCE SDK generates the application cryptogram using a set of inputs, referred to as cryptogram metadata, that is defined in the form of standard CPACE tags. The list of the required tags can be found in the POST/cryptogram-validations request section.

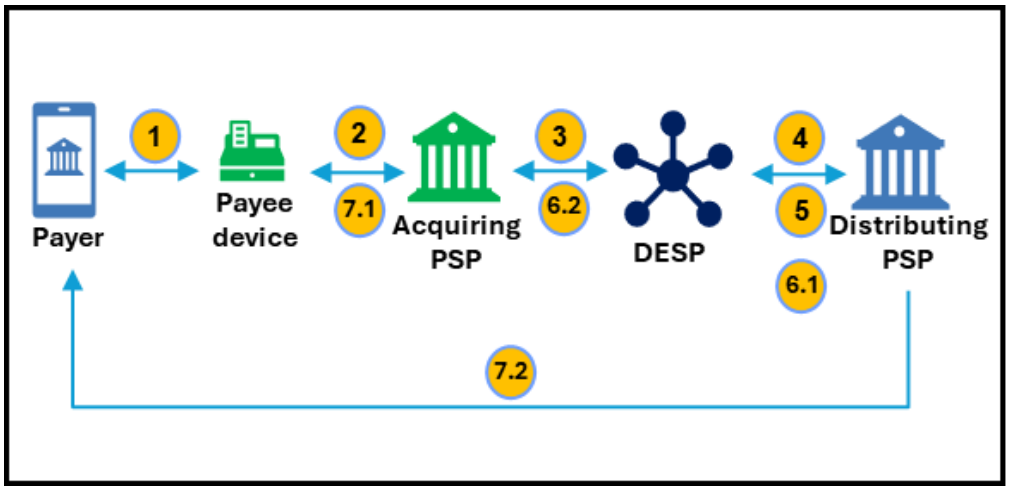
The HCE SDK uses the metadata structured in CDOL1 value (see cryptogram validations endpoint) and one session key as input for application cryptogram generation. To verify the

transaction, the distributing PSP sends an application cryptogram validation request to SEPI, including the token information, the application cryptogram, and the underlying data.

Upon receiving these inputs, SEPI recalculates the application cryptogram. If the recalculated application cryptogram matches the received application cryptogram, the transaction's authenticity is confirmed back to the distributing PSP.

NFC high-level payment flow

Below diagram is a simplified schematic flow of an NFC transaction. It is designed to emphasise the specific aspects of NFC functionality while abstracting away the complexities of various potential configurations in terms of actors, roles, and related processes.



Step	Description
1	• Payee enters amount to payee device. • Payer authenticates and activates the NFC payment function and taps mobile device to payee device. • Payer and payee device interaction happens based on CPACE protocol. • Mobile device generates application cryptogram (AC) and provides it to payee device.
2	• Payee device sends a payment initiation request to the acquiring PSP.
3	• Acquiring PSP sends a payment request to DESP.
4	• Based on the distributing PSP ID, DESP routes the request to the relevant PSP.
5	• The distributing PSP sends an application cryptogram validation request to SEPI. • Following a successful application cryptogram validation response from SEPI (and other controls), the distributing PSP confirms the payment request to DESP.
6.1 6.2	• DESP settles the payment transaction and sends status updates both to acquiring and the distributing PSPs.
7.1 7.2	• Acquiring PSP and distributing PSP inform the payee device and payer devices respectively on the successful transaction outcome.

1.1.1. Function description

Application cryptogram validation

The distributing PSP populates the necessary data in the application cryptogram validation request to SEPI from the inputs it previously received from the payment request. SEPI recalculates the application cryptogram and provides the synchronous response to the distributing PSP. A positive validation result confirms the transaction's authenticity.

1.1.2. Interface description

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

1.1.2.1. Overview of covered scenarios

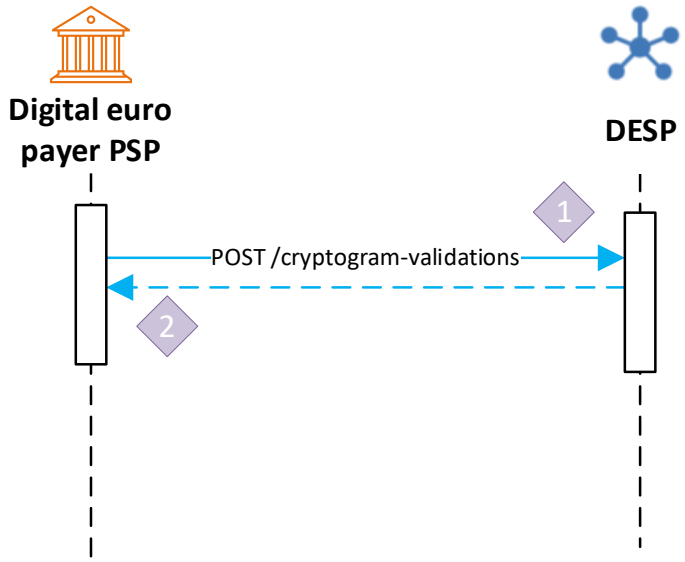


Figure 1 Application cryptogram validation flow

API call	Description	Covered In section
1	Digital euro payer PSP sends the application cryptogram validation request to DESP.	POST/ cryptogram-validations – Request
2	Synchronous response from DESP to provide the application cryptogram validation outcome.	POST/ cryptogram-validations – Response

1.1.2.2. Overview of API endpoints

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

API nr	Description	Sending party	Exposing party	Covered In section
1	Endpoint for the payer PSP to send a request for application cryptogram validation.	PSP	DESP	DESP API for PSPs to send requests to DESP

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

Not applicable.

1.1.2.3. DESP API for PSPs to send requests to DESP

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/cryptogram-validations	Cryptogram	Endpoint for the payer PSP to send a request for cryptogram validation.

1.1.2.3.1. POST/cryptogram-validations – Request

Request header:

- **Technical header:** please refer to Section 5.2.2.3.1.1 Technical header.
- **API specific header:** not applicable.

Request body data elements:

Data element	Element description	Type	Length	Presence indicator
Token (surrogate value)	Token key of payer details. (5A)	NUM	16	M
Cryptogram envelope	Concatenated datapoints and tags encoded in base64 format in the below order (as received in the payment request). Preliminary list: 1. Token – surrogate value (5A) 2. Issuer application data (9F10)	STR	TBA	M

	3. Application transaction counter – ATC (9F36) 4. Cryptogram information data (9F27) 5. EMV cryptogram (9F26) 6. CDOL1 (Card data Object List 1) – data wrapped in 8C: • Transaction type 9C: • Transaction currency (5F24), • Application interchange Profile (AIP – 82), • Terminal transaction date (9A), • Card verification method result (CVM – 9F34), • Amount, authorised (9F02), • Amount, other (9F03), • Unpredictable number (9F37)			

1.1.2.3.2. POST/cryptogram-validations – Response

Response header

- **Technical header: please refer to Section 5.2.2.3.1.1 Technical header.**
- **API specific header: not applicable.**

Response body data elements

- **In case of negative technical validation error: please refer to Section Technical errors.[3]**
- **In case of positive technical validation: HTTP Code 200.**

Data element	Element description	Type	Length	Presence indicator
Cryptogram validation status	Outcome of the application cryptogram validation.	SSET	4	M

Annex A: SEPI non-NFC service v0.90 carried-over content for information only

Disclaimer

This annex is included for completeness and contains content carried over from v0.90. The content has not been further updated or reviewed as part of v0.91. It is therefore provided for information only and is not subject to additional review in this release.

The content will be reviewed, updated and incorporated into the main specification body in a future release.

A.1 Service description

Digital euro payments require transaction data to be exchanged between the user device and the business user device (or another user device for P2P payments). This exchange needs to be secure to support the prevention of fraud.

The usage of surrogate values (tokens) is a way to achieve this.

The SEPI service consists of 2 tokenisation functions:

1. QR-Code and pay-by-link (PBL) tokenisation

   The rationale of tokenisation is the reduction of data to be encoded in the QR-code, allowing lower resolution of the QR-code and contributing to robustness. Less data presented in the QR-code addresses this, as well the privacy objective. A transaction-specific token contributes to higher transaction security. Both QR-code and PBL tokens are generated on a transaction basis.

   The digital euro scheme supports dynamic, payee-presented QR-code generation. The data encoded in the QR-code consists of plain text data and a token. The plain text data puts the payer in the position to consent the payment without the need to detokenise the payload. The plain text data is defined in the relevant chapters of Annex D1. During the detokenisation process, additional data on the transaction environment and payee is provided.

2. Contactless NFC tokenisation[2]

   The provisioning of NFC tokens serves the purpose of higher privacy and security.

[2] Out of scope in this version of the document.

Tokenisation flows vary depending on whether QR code or PBL based payment is being performed. The PBL flow has two options – in-app and browser based payments. All three possibilities are depicted below in high level diagrams.

QR Code flow

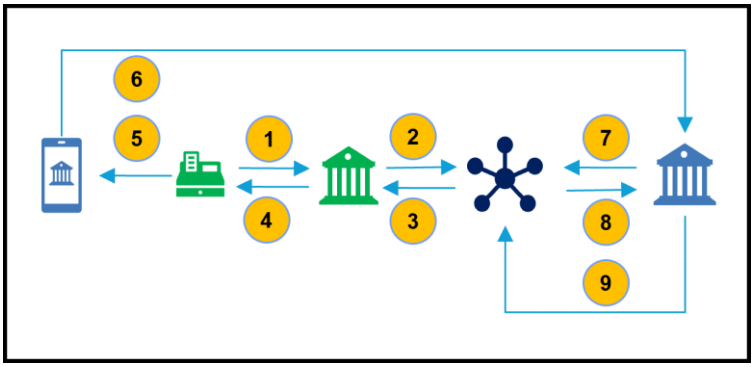


Figure 2 QR code process flow

Step	Description
1	Point-of-Interaction (POS, ATM, E-Commerce payment gateway or payee app) interacts with digital euro payee PSP to request QR token.
2	Digital euro payee PSP requests token from DESP submitting transaction payload.
3	DESP generates token and sends it back to digital euro payee PSP.
4	Digital euro payee PSP receives the token, generates the QR code and sends it to POI.
5	Payer scans QR code.
6	Payer initiates payment with token and plain text data from QR-code.
7	Digital euro payer PSP requests detokenisation from DESP to receive payload.
8	DESP detokenises and sends back payload data to digital euro payer PSP.
9	Following a consistency check between clear text data and detokenised payload, digital euro payer PSP initiates the payment.

Pay-by-link in-app flow

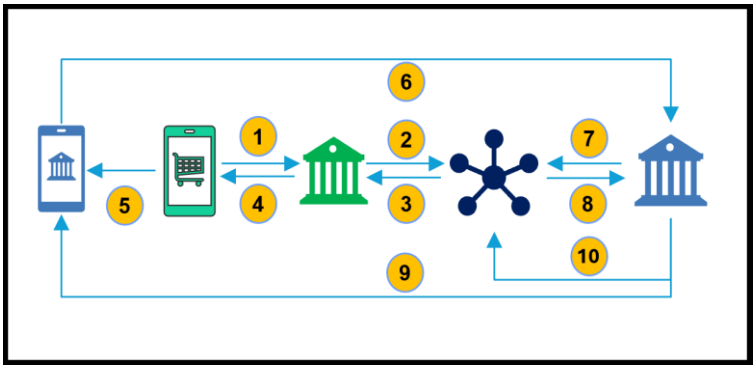


Figure 3 PBL in-app process flow

Step	Description
1	Point-of-Interaction (E-Commerce payment gateway or payee application) requests PBL token from digital euro payee PSP.
2	Digital euro payee PSP requests token from DESP submitting transaction payload.
3	DESP generates token and sends it back to digital euro payee PSP.
4	Digital euro payee PSP receives the token, generates the link and sends it to POI.
5	POI sends link to payer through email/messaging.
6	Payer clicks on link opens application that requests payment information from payer PSP.
7	Digital euro payer PSP requests detokenisation from DESP.
8	DESP detokenises and sends back data to digital euro payer PSP.
9	Digital euro payer PSP presents transaction to payer for SCA and consent.
10	Digital euro payer PSP initiates payment request after payer consent.

Pay-by-link browser based flow

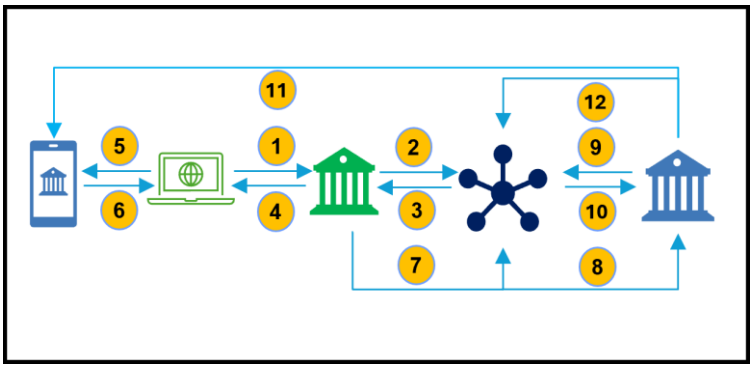


Figure 4 PBL browser based process flow

Step	Description
1	Point-of-Interaction (E-Commerce payment gateway or payee application) requests PBL token from digital euro payee PSP.
2	Digital euro payee PSP interacts with DESP to receive token.
3	DESP generates token and sends it back to digital euro payee PSP.
4	Digital euro payee PSP sends token to POI.
5	POI sends link to payer through email/messaging to payer.
6	Payer clicks on link and opens merchant PSP's website. The payer then also selects its own PSP.
7	Payee PSP sends payment request to DESP.
8	DESP forwards the payee PSP request to payer PSP.
9	After receiving the payment details from Payee PSP via DESP, digital euro payer PSP requests detokenisation from DESP.
10	DESP detokenises and sends back data to digital euro payer PSP.
11	Payer PSP presents transaction to payer for SCA and consent.
12	Digital euro payer PSP initiates payment after payer consent.

NFC tokenisation flow

[Placeholder]

A.1.1 Distributing PSP requirements

A.1.1.1 Function description

Tokenisation request

Tokenisation requests are sent to DESP for QR and PBL based online payments in case of:

- person-to-person (P2P) between two private users; or
- consumer-to-business (C2B) online payments between a private and a business user

Optional extensions for the recurring payments and reservations are only used by the acquiring PSPs in case of a C2B transaction.

Detokenisation request

PSPs also support QR code or PBL detokenisation requests towards DESP. In case of a C2B transaction with a QR code, the detokenisation request to DESP is sent by the payer PSP.

NFC tokenisation request

Placeholder

NFC detokenisation request

Placeholder

A.1.1.2 Interface description

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

A.1.1.2.1 Overview of covered scenarios

Tokenisation request

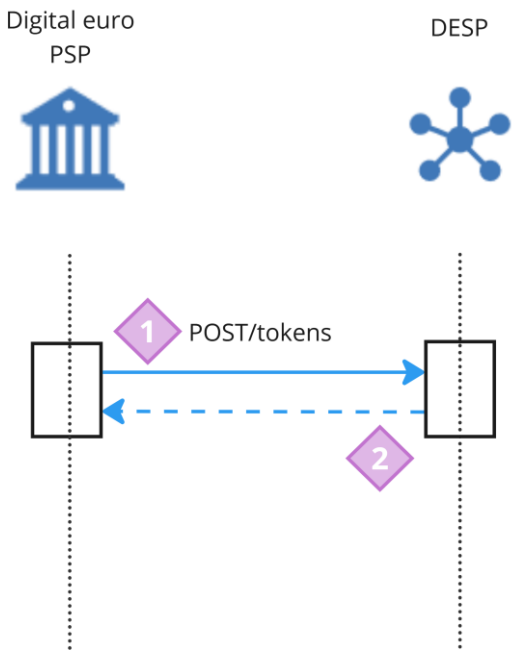


Figure 5 Tokenisation request

API Call	Description	Covered in sectionCovered in section
1	Digital euro PSP sends the tokenisation request to DESP indicating the token type (QR or PBL).	POST/tokens – Request
2	Synchronous response from DESP to provide the requested token.	POST/tokens – Response

Detokenisation request

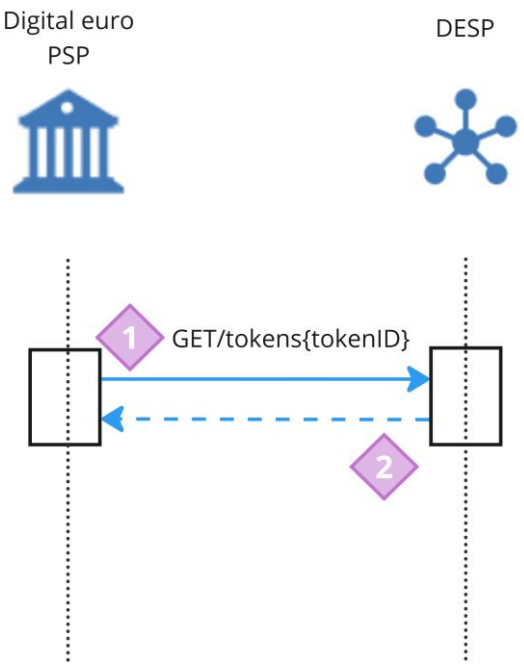


Figure 6 Detokenisation request

API Call	Description	Covered in sectionCovered in section
1	Digital euro PSP sends the detokenisation request to DESP indicating the token ID.	GET/tokens/{tokenID} – Request
2	Synchronous response from DESP to provide the detokenised data.	GET/tokens/{tokenID} – Response

A.1.1.2.2 Overview of API endpoints

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

API nr	Description	Sending Party	Exposing party	Covered in section
1	QR or PBL token request with underlying payload by payee PSP from DESP for both, P2P and C2B transactions.	PSP	DESP	POST/tokens
2	QR or PBL detokenisation request by payer PSP from DESP for both, P2P and C2B transactions.	PSP	DESP	GET/ tokens/{tokenID}
3	NFC tokenisation placeholder	PSP	DESP	POST/nfc-tokens
4	NFC detokenisation placeholder	PSP	DESP	GET/nfc-tokens /{tokenID}

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

Not applicable.

A.1.1.2.3 DESP API for PSPs to send requests to DESP

A.1.1.2.3.1 POST/tokens

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/tokens	TOKEN	QR-or PBL token request with underlying payload

A.1.1.2.3.1.1 POST /tokens – Request

Request header:

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

Request body

Data element	Element description	Type	Length	Presence indicator
Token type	The type of token, derived from the PSP and context in which it is used ("QRC" for QR code and "PBL" for pay-by-link).	SSET	3	M
End-to-end identification	Unique identification, as assigned by the initiating user, to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain. In case no reference was given by the user, "NOTPROVIDED" must be used.	STR	35	O
Payee name	Name of the payee.	STR	70	C, mandatory in case of C2B payments,

				registered company name of the business user payee.
Payee trade name	Name of the business user payee as it is presented to customers.	STR	25	C, mandatory in case of C2B payments.
Payee DEAN	Unique identification of the payee's digital euro payment account.	STR	18	M
Payee location (town)	Town of the business user payee.	STR	*13*	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (ZIP-Code)	ZIP-code of the business user payee.	NUM	10	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.

Payee location (country)	Country of the business user payee.	STR	*30*	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (address)	Address (street name and building number) of the business user payee.	STR	30	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee ID	Unique identification of the business user payee (acceptor) that was assigned to the payee by its PSP.	STR	*15*	O, payee's PSP should be able to decide if they need this data element.
Terminal ID	Unique identification of the POS-terminal used to initiate the transaction that was assigned to the payee by its PSP.	STR	*8*	C, mandatory in case of POS payments.

Merchant category code (MCC)	Merchant category code. For P2P MCC 4829 for money transfer must be used.	NSET	4	M
Payee PSP ID for digital euro.	Unique identification of the payee's PSP (BIC).	STR	11	M
Purpose code of credit Transfer	Purpose of digital euro payment.	SSET	4	O
Structured remittance information	The fields provide additional information about (the purpose of) the transaction in a standardised and structured format. It may include a type, a reference to a standard and a value. It is mandatory to include this field if the user provides the remittance.	STR	TBD	O
Transaction amount	The transaction amount to be transferred from the payer to the payee.	STR	14.3	M
Transaction currency	The currency in which the transaction amount is expressed. ISO 4217 three-letter code.	STR	3	M
Additional amount	Amount paid in addition to the transaction amount, e.g. in case of cashback or tip.	STR	14.3	O
Additional amount currency	The currency in which the additional amount is expressed. ISO 4217 three-letter code.	SSET	3	C, mandatory if "Additional amount" field is present.
Total amount	Sum of transaction amount and additional amount.	STR	14.3	C, mandatory if "Additional amount" present.
Total amount currency	The currency in which the total amount is expressed. ISO 4217 three-letter code.	SSET	3	C, mandatory if "Additional amount" present.

Transaction type	e.g. Purchase, Reservation, Purchase with cashback, cash withdrawal.	*SSET*	*4*	M
Payment type	Placeholder for fee calculation purposes.	*SSET*	*TBA*	
Transaction environment	Placeholder - to be specified.	SSET	8	M
Transaction date and time	Transaction date and time.	ISODateTime	26	M
Expiry date and time	The date and time at which both the token as well as the QR-code or link ceases to be valid.	ISODateTime	26	M
Payee return URL	Merchant URL where to redirect payer back to the merchant web page after payment is completed.	STR	Tbd	C, C2B only
Recurring payments object	See next table “Request body – optional object for recurring payments”.			O
Reservations object	See next table “Request body – optional object for reservations”.			O

Request body – optional object for recurring payments

Data element	Element description	Type	Length	Presence indicator
Recurring payment frequency	The field specifies the frequency of a recurring payment. Please refer to Annex D 1 Acquiring PSP requirements, section 8.3.1.1.2.1 Incoming message table for the possible values.	SSET	4	M
Confirmation indicator	The field specifies if each recurring payment required authentication and confirmation by the payer.	BOOL	NA	M

End date	The field specifies the date at which the authorisation for the series of recurring payment ends.	ISODateTime	26	M
Recurring payments agreement ID	Agreement ID of the recurring payments.	STR	tbd	M

Request body – optional object for reservations

Data element	Element description	Type	Length	Presence indicator
Reservation ID	Resource ID for the reservation transaction.	STR	tbd	M
Latest reserved amount	The remaining reserved amount before this settlement.	STR	14.3	M
Latest reserved currency	The currency in which the latest reserved amount is expressed. ISO 4217 three-letter code. Attribute of latest reserved amount.	STR	3	M
Settlement amount	The amount which needs to be settled (must be lower than or equal to latest reserved amount).	STR	14.3	M
Settlement currency	The currency in which the settlement amount is expressed. ISO 4217 three-letter code. Attribute of settlement amount.	STR	3	M
Reserved remaining amount	Attribute to indicate whether any remaining reserved amount (after settlement) must stay reserved or must be released.	BOOL	-	M

A.1.1.2.3.2 POST/tokens – Response

Response header

- **Technical header:** please refer to 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 201.

Data element	Element description	Type	Length	Presence indicator
Token ID	Token ID generated by DESP.	STR	12	M
Expiry date and time	The date and time at which both the token as well as the QR-code or link ceases to be valid.	ISODateTime	26	M

A.1.1.2.3.2 GET/ tokens/{tokenID}

Applicable endpoints and methods:

Method	Endpoint	Resource	Description
GET	/v1/tokens/{tokenID}	TOKEN	QR or PBL detokenisation request by payer PSP from DESP.

A.1.1.2.3.2.1 GET/tokens/{tokenID} – 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
Token ID	Token ID generated by DESP.	STR	12	M

A.1.1.2.3.2.2 GET/tokens/{tokenID} – 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
Token type	The type of token, derived from the PSP and context in which it is used ("QRC" for QR code and "PBL" for pay-by-link)	SSET	3	M
End-to-end identification	Unique identification, as assigned by the initiating user, to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain. In case no reference was given by the user, "NOTPROVIDED" must be used.	STR	35	O
Payee name	Name of the payee.	STR	70	C, mandatory in case of C2B payments, registered company name of the business user payee.
Payee trade name	Name of the business user payee as it is presented to customers.	STR	25	C, mandatory in case of C2B payments.
Payee DEAN	Unique identification of the payer's digital euro payment account.	STR	18	M

Payee location (town)	Town of the business user payee.	STR	13	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (ZIP-Code)	ZIP-code of the business user payee.	NUM	10	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (country)	Country of the business user payee.	STR	30	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (address)	Address (street name and building number) of the business user payee.	STR	30	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central

				registered address.
Payee ID	Unique identification of the business user payee (acceptor) that was assigned to the payee by its PSP.	STR	15	O, payee's PSP should be able to decide if they need this data element.
Terminal ID	Unique identification of the POS-terminal used to initiate the transaction that was assigned to the payee by its PSP.	STR	8	C, mandatory in case of POS payments.
Merchant category code (MCC)	Merchant category code. For P2P MCC 4829 for money transfer must be used.	NSET	4	M
Payee PSP ID for digital euro.	Unique identification of the payee's PSP (BIC).	STR	11	M
Purpose code of credit Transfer	Purpose of digital euro payment.	SSET	4	O
Structured remittance information	The fields provide additional information about (the purpose of) the transaction in a standardised and structured format. It may include a type, a reference to a standard and a value. It is mandatory to include this field if the user provides the remittance.	STR	TBD	O
Transaction amount	The transaction amount to be transferred from the payer to the payee.	STR	14.3	M
Transaction currency	The currency in which the transaction amount is expressed. ISO 4217 three-letter code.	STR	3	M
Additional amount	Amount paid in addition to the transaction amount, e.g. in case of cashback or tip.	STR	14.3	O
Additional amount currency	The currency in which the additional amount is expressed.	SSET	3	C, mandatory if "Additional

	ISO 4217 three-letter code.			amount" field is present.
Total amount	Sum of transaction amount and additional amount.	STR	14.3	C, mandatory if "Additional amount" present.
Total amount currency	The currency in which the total amount is expressed. ISO 4217 three-letter code.	SSET	3	C, mandatory if "Additional amount" present.
Transaction type	e.g. Purchase, Reservation, Purchase with cashback, cash withdrawal.	SSET	*4*	M
Payment type	Placeholder for fee calculation purposes.	SSET	*TBA*	
Transaction environment	Placeholder - to be specified.	SSET	8	M
Transaction date and time	Transaction date and time.	ISODateTime	26	M
Expiry date and time	The date and time at which both the token as well as the QR-code or link ceases to be valid.	ISODateTime	26	M
Payee return URL	Merchant URL where to redirect payer back to the merchant web page after payment is completed.	STR	Tbd	C, C2B only
Recurring payments object	See next table "Request body – optional object for recurring payments".			O
Reservations object	See next table "Request body – optional object for reservations".			O

Request body – optional object for recurring payments

Data element	Element description	Type	Length	Presence indicator
Recurring payment frequency	The field specifies the frequency of a recurring payment. Please refer to Annex D 1 Acquiring PSP	SSET	4	M

	requirements, section 8.3.1.1.2.1 Incoming message table for the possible values.			
Confirmation indicator	Specifies if each recurring payment required authentication and confirmation by the payer.	BOOL	NA	M
End date	Specifies the date at which the authorisation for the series of recurring payment ends.	ISODateTime	26	M

Request body – optional object for reservations

Data element	Element description	Type	Length	Presence indicator
Reservation ID	Resource ID for the reservation transaction.	STR	tbd	M
Latest Reserved Amount	The remaining reserved amount before this settlement.	STR	14.3	M
Latest Reserved Currency	The currency in which the latest reserved amount is expressed. ISO 4217 three-letter code. Attribute of latest reserved amount.	STR	3	M
Settlement Amount	The amount which needs to be settled (must be lower than or equal to latest reserved amount).	STR	14.3	M
Settlement Currency	The currency in which the settlement amount is expressed. ISO 4217 three-letter code. Attribute of settlement amount.	STR	3	M
Reserve Remaining Amount	Attribute to indicate whether any remaining reserved amount (after settlement) must stay reserved or must be released.	BOOL	-	M

A.1.1.2.3.3 POST/nfc-tokens

Placeholder for NFC tokenisation

A.1.1.2.3.3.1 POST/nfc-tokens – Request

A.1.1.2.3.3.2 POST/nfc-tokens – Response

A.1.1.2.3.4 GET/nfc-tokens/{tokenID}

Placeholder for NFC detokenisation

A.1.1.2.3.4.1 GET/nfc-tokens/{tokenID} – Request

A.1.1.2.3.4.2 GET/nfc-tokens/{tokenID} – Response

A.1.1.2.4 PSP API for PSPs to receive requests from DESP

Not applicable.

A.1.2 Acquiring PSP requirements

A.1.2.1 Function Description

Tokenisation request

Tokenisation requests are sent to DESP for QR and PBL based online payments in case of:

- person-to-person (P2P) between two private users; or
- consumer-to-business (C2B) online payments between a private and a business user

Optional extensions for the recurring payments and reservations are only used by the acquiring PSPs in case of a C2B transaction.

Detokenisation request

Not applicable for acquiring PSPs.

NFC tokenisation request

Not applicable for acquiring PSPs.

NFC detokenisation request

Not applicable for acquiring PSPs.

A.1.2.2 Interface description

A.1.2.2.1 Overview of covered scenarios

Please see the previous section for covered scenarios.

A.1.2.2.2 Overview of API endpoints

Please see rhe previous section for applicable API endpoints. The differences in the required data elements are detailed out in the presence indicator columns.