Rulebook development

ERPB Update

22 February 2023
Building blocks for the scheme rulebook
We have identified 6 building blocks, numbered from A to F, covering together all sections of the digital euro rulebook

<table>
<thead>
<tr>
<th>Building blocks</th>
<th>Digital euro rulebook</th>
</tr>
</thead>
<tbody>
<tr>
<td>F. Scheme generics</td>
<td>1. Document information</td>
</tr>
<tr>
<td></td>
<td>- References, defined terms, change history, purpose, ownership of the document</td>
</tr>
<tr>
<td></td>
<td>2. Digital euro scheme scope and interplay</td>
</tr>
<tr>
<td></td>
<td>- Vision and mission statement, scope, actors, binding nature of the rulebook, separation between scheme and payment infra., benefits of the scheme, additional optional services, scheme participation fees</td>
</tr>
<tr>
<td>A. Functional &amp; operational model</td>
<td>3. Functional and operational model</td>
</tr>
<tr>
<td></td>
<td>- Generic processing flows / end-to-end flows, core requirements / service endpoints / list of attributes, identification &amp; authentication / list of SCA approaches, min. UX standards²</td>
</tr>
<tr>
<td>B. Adherence model</td>
<td>4. Adherence model</td>
</tr>
<tr>
<td></td>
<td>- Scheme participation, reachability &amp; interoperability, eligibility criteria, becoming a participant, scheme register of participants, obligations of participants, liability, compliance and enforcement, rules of supervision, termination, exemptions and potential bilateral agreements, intellectual property, contractual provisions, applicable regulatory / legal framework, governing law</td>
</tr>
<tr>
<td>C. Technical scheme requirements</td>
<td>5. Technical scheme requirements</td>
</tr>
<tr>
<td></td>
<td>- IT infrastructure, IT security, Connectivity (e.g., API implementation), interplay with European standardization initiatives (specifications), interface standards / specifications², non-functional requirements</td>
</tr>
<tr>
<td>D. Risk management</td>
<td>6. Risk management</td>
</tr>
<tr>
<td>E. Scheme management</td>
<td>7. Scheme management</td>
</tr>
<tr>
<td></td>
<td>- Scheme management board, change management process, brand management, scheme operations</td>
</tr>
<tr>
<td></td>
<td>8. Defined terms and abbreviations</td>
</tr>
<tr>
<td></td>
<td>- Illustrative client journeys and client products, branding standards²</td>
</tr>
<tr>
<td></td>
<td>- Adherence and related documents¹, description of AML fulfillment and sanctions requirements</td>
</tr>
<tr>
<td></td>
<td>- Business conditions and commercial terms²</td>
</tr>
<tr>
<td></td>
<td>- Functional and technical architecture document including register, SLRs / KPs, reporting requirements and guidelines, reconciliation, interoperability policy to other payment systems</td>
</tr>
<tr>
<td></td>
<td>- Incident management, implementation guidelines including technical standards, certification and approval framework, onboarding document / toolkits²</td>
</tr>
</tbody>
</table>

1. The digital euro legal act currently being prepared may impact the rulebook scope and content and may require subsequent adjustments
2. Out of scope of Rulebook Development Group
3. Out of scope of current phase; to be detailed as part of implementation phase

Note: Overlaps with other engagement groups may materialize
High-level approach for the development of the scheme rulebook
1. "Regular approach" elements – i.e., sections of the rulebook drafted by the rulebook team without interactions with a dedicated workstream; 2. Updated references and defined terms and abbreviations will be presented on a regular basis to the RDG.
User Journeys
Why focusing on user journeys?

In particular, client journeys inform functional requirements, which in turn inform activities necessary from the Eurosystem and intermediaries, and thereby “generic flows”, in turn informing tasks and “end-to-end flows”.

User journeys allow to define and illustrate functional requirements.

Generic flows are related to activities\(^1\) that the Eurosystem and intermediaries need to perform to deliver the above functionalities.

End-to-end flows are related to tasks\(^1\) that the Eurosystem and intermediaries need to conduct to perform the above activities.

---

1. Activities and tasks related to communications between the different intermediaries and with the Eurosystem; internal activities and tasks are out of scope of generic flows and end-to-end flows.
A long list of ~45-50 journeys has been identified (including variations of similar use cases)

1. Core & optional requirements defined by Eurosystem

2. Use case & Form factors Prioritization by Eurosystem

User vs merchant perspective as a digital euro user

Intermediaries’ app vs D€ standalone app experience

~45-50 user journeys to be illustrated in total
## TM 1.4 – E-Com (incl. C2G) payment with QR Code

**Use Case**: Payer completes payment by scanning QR Code generated by Payee

<table>
<thead>
<tr>
<th># of actions (estimated)</th>
<th>4²</th>
<th>2</th>
<th>1</th>
<th>Pre-requisites</th>
<th>Business requirements</th>
</tr>
</thead>
</table>
| **Checkout**             |    |   |   | Pre-requisites | • Payer should be able to select D€ payment through QR Code  
  • Payee should be able to generate dynamic QR Code (to support encoding of the amount)  
  • Generated QR Code should be valid and compliant (e.g., with the EPC QR Code rulebook) |
| Payer selects D€ as payment method and QR Code with payment details is generated |    |   |   |                 |                       |
| **Payment initiation**   |    |   |   |                 | • Payer should be able to scan QR Code with a built-in QR scanner from their payment app  
  • Payer should be able to consent the transaction through one of the accepted authentication mechanisms  
  • Payer should be able to choose a preferred way to authenticate (e.g., code, biometrics)  
  • If amount exceeds available balance, reverse waterfall should be triggered for Payer |
| Payer scans QR Code      | 4² | 3 |   |                 |                       |
| **Consent & Authentication** |    |   |   |                 | • App should display amount and Payee of the transaction and confirm consent of Payer  
  • Payer should be able to consent the transaction through one of the accepted authentication mechanisms  
  • Payer should be able to choose a preferred way to authenticate (e.g., code, biometrics)  
  • If amount exceeds available balance, reverse waterfall should be triggered for Payer |
| Payer consents the transaction |    |   |   |                 |                       |
| **Payment confirmation** |    |   |   |                 | • Payer’s account/wallet should be debited, and Payee’s account/wallet should be credited  
  • Payer receives a confirmation message, including amount, date, time, and merchant name  
  • Transaction should be recorded in Payer’s and Payee’s transaction log |
| Payer receives payment confirmation |    |   |   |                 |                       |

**Open points to be tracked because they will impact the journeys**

- **Standard selected for QR Code (e.g., EPC)** could have impacts on type of information that can be channeled through the QR
- **Selection of payment method**: should an intermediate step be included in Step 2 for the selection of QR Code as the payment method?
- **Authentication**: authentication step may perhaps be skipped because the payer has authenticated earlier or because the amount is below the regulatory threshold for mandatory authentication

---

1. Select digital euro, select QR Code and QR Code generation
2. Open app, authenticate, select scan QR and scan QR
# TM 1.6 – M-Commerce payment (in-app)

**Use Case:** Payer completes payment by using an alias/proxy

<table>
<thead>
<tr>
<th># of actions (estimated)</th>
<th>Pre-requisites</th>
<th>Business requirements</th>
<th>Consent &amp; Authentication</th>
<th>Payment confirmation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Payer should be able to select pay with digital euro.</td>
<td>• A pop up from the digital euro wallet should appear on the screen.</td>
<td>Payer selects D€ as payment method</td>
<td>Payer receives payment confirmation</td>
</tr>
<tr>
<td></td>
<td>Payee must accept D€ as a payment method</td>
<td>• Payer should be able to choose a preferred way to authenticate (e.g., Code, biometrics).</td>
<td>Payer consents the transaction</td>
<td>Payer’s account should be debited and Payee’s account should be credited.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Payer should be able to consent the transaction through one of the accepted authentication mechanisms.</td>
<td></td>
<td>Payer receives a confirmation message, including amount, date and time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If amount exceeds available, reverse waterfall should be triggered for Payer.</td>
<td></td>
<td>Transaction should be recorded in Payer’s and Payee’s transaction log.</td>
</tr>
</tbody>
</table>

### Pre-requisites

- Payer and Payee must be enrolled
- Payee must accept D€ as a payment method

### Open points to be tracked because they will impact the journeys

- **Payment confirmation:** will the Payer receive an additional confirmation of the purchase, and if so, in which app?
- **Technical and regulatory requirements:** what is the in-app authentication impact on technical and regulatory requirements from other players?

### Illustrative draft to support discussion

1. Select digital euro, select alias/proxy and insert alias/proxy
2. Open app, authenticate and consent
# TM 1.1 – POS payment with Payee-generated QR Code

**Use Case:** Payer completes payment by scanning Payee’s QR Code

## Use Case Details

1. **Use Case:** Payer completes payment by scanning Payee’s QR Code

## Use Case Diagram

<table>
<thead>
<tr>
<th>Pre-requisites</th>
<th>Business requirements</th>
</tr>
</thead>
</table>
| **Payee** | • Payee should be able to generate dynamic QR Code (to support encoding of the amount)  
  • Payee should be able to scan QR Code, with a built-in QR scanner from their payment app  
  • Generated QR Code should be valid and compliant (e.g., with the EPC QR Code rulebook)  
  • Payer should be able to scan QR Code, with a built-in QR scanner from their payment app  
  • App should display amount and Payee of the transaction and confirm consent of Payer  
  • Payer should be able to consent the transaction through one of the accepted authentication mechanisms  
  • Payer should be able to choose a preferred way to authenticate (e.g., code, biometrics)  
  • If amount exceeds available balance, reverse waterfall should be triggered for Payer  
  • Payer’s account/wallet should be debited, and Payee’s account/wallet should be credited  
  • Both Payer and Payee should receive a confirmation message  
  • Payer’s confirmation message includes amount, date and time, merchant name and location  
  • Transaction should be recorded in Payer’s and Payee’s transaction log |
| **Payer** | • Payer must be enrolled  
  • Payer must accept DE as a payment method  
  • Payer has authenticated in the app  
  • Payee must have a POS equipped with QR Code technology  
  • Standard selected for QR Code (e.g., EPC) could have impacts on type of information that can be channelled through the QR  
  • Authentication: authentication step may perhaps be skipped because the payer has authenticated earlier or because the amount is below the regulatory threshold for mandatory authentication |

## Business Requirements

- **Payment of [amount] sent to [Payee] at [time]**
- **Authenticate**
- **Scan**
- **Consent**
- **Payment confirmation**

## Pre-requisites

- **Payee**
  - Payer and Payee must be enrolled
  - Payee must accept DE as a payment method
  - Payer has authenticated in the app
  - Payee must have a POS equipped with QR Code technology
- **Payer**
  - Payer has authenticated in the app

## Open Points to Be Tracked

- **Standard selected for QR Code (e.g., EPC)** could have impacts on type of information that can be channelled through the QR
- **Authentication:** authentication step may perhaps be skipped because the payer has authenticated earlier or because the amount is below the regulatory threshold for mandatory authentication

## # of actions (estimated)

<table>
<thead>
<tr>
<th># of actions (estimated)</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Checkout</strong></td>
<td>Payee generates QR Code with transaction amount</td>
</tr>
<tr>
<td><strong>Payment initiation</strong></td>
<td>Payer scans QR Code</td>
</tr>
<tr>
<td><strong>Consent &amp; Authentication</strong></td>
<td>Payer consents the transaction</td>
</tr>
<tr>
<td><strong>Payment confirmation</strong></td>
<td>Both Payer and Payee receive payment confirmation</td>
</tr>
</tbody>
</table>

## # of actions

<table>
<thead>
<tr>
<th># of actions</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open app, authenticate, select scan QR and scan QR</td>
<td>20.00 €</td>
</tr>
</tbody>
</table>
# TM 1.2 – POS payment with NFC

**Use Case:** Payer completes payment by using NFC technology

## Pre-requisites

<table>
<thead>
<tr>
<th></th>
<th>Payee</th>
<th>Payer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th># of actions (estimated)</th>
<th>1</th>
<th>3</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Checkout</strong>&lt;br&gt;Payer sets up POS terminal with transaction amount</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>Consent &amp; Authentication</strong>&lt;br&gt;Payer consents the transaction</td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>Payment confirmation</strong>&lt;br&gt;Both Payer and Payee receive payment confirmation</td>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
<td><img src="image9.png" alt="Image" /></td>
</tr>
</tbody>
</table>

## Business requirements

- POS terminal should display transaction amount and NFC icon
- NFC-based communication should comply with standards
- Payer should be able to consent the transaction through one of the accepted authentication mechanisms
- Payer should be able to choose a preferred way to authenticate (e.g., code, biometrics)
- If amount exceeds available balance, reverse waterfall should be triggered for Payer
- Alternatively, consent and authentication might be provided by activation of smartphone before bringing device near the NFC reader
- Payer’s account/wallet is debited, and Payee’s account/wallet is credited
- Payer’s account/wallet is credited
- Both Payer and Payee receive a confirmation message
- Payer’s confirmation message includes amount, date and time, merchant name and location
- Transaction should be recorded in Payer’s and Payee’s transaction log

## Pre-requisites

- Payer and Payee must be enrolled
- Payee must accept D€ as a payment method
- Payer has authenticated in the app
- Payee must have a POS equipped with NFC technology

## Open points to be tracked because they will impact the journeys

- **Smart devices:** “smart devices” allowed for NFC transactions (e.g., watches?)

1. Open app, authenticate and select payment method

![Illustrative draft to support discussion](image10.png)