TECHNICAL SPECIFICATIONS FOR THE PROCESSING OF PAYMENT ORDERS FOR INTERNET-BASED ACCESS

1. Technical requirements for participation in TARGET2-Latvija regarding infrastructure, network and formats

1.1 Each participant shall connect to the ICM of TARGET2 using a local client, operating system and Internet browser as specified in Annex "Internet-based Participation – System Requirements for Internet Access" to the User Detailed Functional Specifications (UDFS), with settings defined. Each participant's PM account shall be identified by an eight- or 11-digit BIC. Furthermore, each participant shall pass a series of tests to prove its technical and operational competence before it may participate in TARGET2-Latvija.

1.2 For the submission of payment orders and the exchange of payment messages in the PM, the TARGET2 platform BIC, TRGTXEPMLVP, shall be used as the message sender/receiver. Payment orders sent to a participant using Internet-based access should identify that receiving participant in the beneficiary institution field. Payment orders sent by a participant using Internet-based access shall identify the above participant as the ordering institution.

1.3 Participants shall use public key infrastructure services as specified in the User Manual: Internet Access for the Public-Key Certification Service.

2. Payment message types

2.1 Participants may make the following types of payments:
2.1.1 customer payments, i.e. credit transfers for which the ordering and/or beneficiary customer are not financial institutions;
2.1.2 customer payments STP, i.e. credit transfers for which the ordering and/or beneficiary customer are not financial institutions, executed in straight through processing mode;
2.1.3 bank-to-bank transfers to request the movement of funds between financial institutions;
2.1.4 cover payments to request the movement of funds between two financial institutions related to an underlying customer credit transfer.
2.1.5 In addition, participants using Internet-based access to a PM account can receive direct debit orders.

2.2 Participants shall comply with the field specifications, as defined in Paragraph 9.1.2.2, Volume 1 of the UDFS.

2.3 Field contents shall be validated at the level of TARGET2-Latvija in accordance with the UDFS requirements. Participants may agree among each other on specific rules regarding the field contents. However, specific checks as to whether participants comply with any such rules shall not be conducted in TARGET2-Latvija.

2.4 Participants may make cover payments via TARGET2, i.e. payments made by correspondent banks to settle (cover) credit transfer messages which are submitted to a
customer's bank by other, more direct means. Customer details contained in these cover payments shall not be displayed in the ICM.

3. Double-entry check

3.1 All payment orders shall pass a double-entry check, the aim of which is to reject payment orders that have been submitted more than once by mistake.

3.2 The following fields of the message types shall be checked:

<table>
<thead>
<tr>
<th>Details</th>
<th>Part of the message</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Basic Header</td>
<td>BIC Address</td>
</tr>
<tr>
<td>Message Type</td>
<td>Application Header</td>
<td>Message Type</td>
</tr>
<tr>
<td>Receiver</td>
<td>Application Header</td>
<td>Destination Address</td>
</tr>
<tr>
<td>Transaction Reference</td>
<td>Text Block</td>
<td>:20</td>
</tr>
<tr>
<td>Number (TRN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Reference</td>
<td>Text Block</td>
<td>:21</td>
</tr>
<tr>
<td>Value Date</td>
<td>Text Block</td>
<td>:32</td>
</tr>
<tr>
<td>Amount</td>
<td>Text Block</td>
<td>:32</td>
</tr>
</tbody>
</table>

3.3 If all the fields described in Paragraph 3.2 of the present Appendix in relation to a newly submitted payment order are identical to those in relation to a payment order that has already been accepted, the newly submitted payment order shall be returned.

4. Error codes

4.1 If a payment order is rejected, an abort notification shall be provided via the ICM indicating the reason for the rejection by using error codes. The error codes are defined in Paragraph 9.5.2, Volume 1 of the UDFS.

5. Predetermined settlement times

5.1 For payment orders using the Earliest Debit Time Indicator, the codeword "/FROTIME/" shall be used.

5.2 For payment orders using the Latest Debit Time Indicator, two options shall be available.
5.2.1 Codeword "/REJTIME/": if the payment order cannot be settled by the indicated debit time, the payment order shall be returned.
5.2.2 Codeword "/TILTIME/": if the payment order cannot be settled by the indicated debit time, the payment order shall not be returned but shall be put in the relevant queue.
5.2.3 In cases referred to in Sub-paragraphs 5.2.1 and 5.2.2 of the present Appendix, if a payment order with a Latest Debit Time Indicator is not settled 15 minutes prior to the time indicated therein, a notification shall automatically be provided via the ICM.

5.3 If the codeword "/CLSTIME/" is used, the payment shall be treated in the same way as a payment order referred to in Paragraph 5.2.2 of the present Appendix.

6. Settlement of payment orders in the entry disposition

6.1 Offsetting checks and, if appropriate, extended offsetting checks (both terms as defined in Paragraphs 6.2 and 6.3 of the present Appendix) shall be carried out on payment orders entered into the entry disposition to provide quick, liquidity-saving gross settlement of payment orders.

6.2 An offsetting check shall determine whether the payee's payment orders that are at the front of the highly urgent or, if inapplicable, the urgent queue are available to be offset against the payer's payment order (hereinafter, offsetting payment orders). If an offsetting payment order does not provide sufficient funds for the respective payer's payment order in the entry disposition, it shall be determined whether sufficient liquidity is available on the payer's PM account.

6.3 If the offsetting check fails, the Bank of Latvia may apply an extended offsetting check. An extended offsetting check determines whether offsetting payment orders are available in any of the payee's queues regardless of when they are placed in the queue. However, if higher priority payment orders addressed to other TARGET2 participants are in the queue of the payee, the FIFO principle may only be breached if settling such an offsetting payment order would result in a liquidity increase for the payee.

7. Settlement of payment orders in the queue

7.1 The treatment of payment orders placed in queues depends on the priority class to which it was designated by the instructing participant.

7.2 Payment orders in the highly urgent and urgent queues shall be settled by using the offsetting checks described in Section 6 of the present Appendix, starting with the payment order at the front of the queue in cases when there is an increase in liquidity or intervention at the queue level (change of queue position, settlement time or priority, or revocation of the payment order).

7.3 Payments orders in the normal queue shall be settled on a continuous basis including all highly urgent and urgent payment orders that have not yet been settled. Different optimisation mechanisms (algorithms) are used. If an algorithm is successful, the included payment orders will be settled, but if an algorithm fails, the included payment orders will remain in the queue. Three algorithms (1 to 3) shall be applied to offset payment flows. By means of Algorithm 4, settlement procedure 5 (as defined in Paragraph 2.8.1, Volume 1 of the UDFS) shall be available for the settlement of payment instructions of ancillary systems. To optimise the settlement of highly urgent ancillary system transactions on participants' sub-accounts, a special algorithm (Algorithm 5) shall be used.
7.3.1 Under Algorithm 1 ("all-or-nothing") the Bank of Latvia shall, both for each relationship in respect of which a bilateral limit has been set and also for the total sum of relationships for which a multilateral limit has been set:

7.3.1.1 calculate the overall liquidity position of each TARGET2 participant's PM account by establishing whether the aggregate of all outgoing and incoming payment orders pending in the queue is negative or positive and, if it is negative, check whether it exceeds that participant's available liquidity (the overall liquidity position shall constitute the "total liquidity position");

7.3.1.2 check whether limits and reservations set by each TARGET2 participant in relation to each relevant PM account are respected.

7.3.1.3 If the outcome of these calculations and checks is positive for each relevant PM account, the Bank of Latvia and other CBs involved shall settle all payments simultaneously on the PM accounts of the TARGET2 participants concerned.

7.3.2 Under Algorithm 2 ("partial") the Bank of Latvia shall:

7.3.2.1 calculate and check the liquidity positions, limits and reservations of each relevant PM account as under Algorithm 1;

7.3.2.2 if the total liquidity position of one or more relevant PM accounts is negative, extract single payment orders until the total liquidity position of each relevant PM account is positive;

7.3.2.3 thereafter, the Bank of Latvia and the other CBs involved shall, provided there are sufficient funds, settle all remaining payments (except the extracted payment orders) simultaneously on the PM accounts of the TARGET2 participants concerned;

7.3.2.4 when extracting payment orders, the Bank of Latvia shall start from the TARGET2 participant's PM account with the highest negative total liquidity position and from the payment order at the end of the queue with the lowest priority. The selection process shall only run for a short time, to be determined by the Bank of Latvia at its discretion.

7.3.3 Under Algorithm 3 ("multiple") the Bank of Latvia shall:

7.3.3.1 compare pairs of TARGET2 participants' PM accounts to determine whether queued payment orders can be settled within the available liquidity of the two TARGET2 participants' PM accounts concerned and within the limits set by them (by starting from the pair of PM accounts with the smallest difference between the payment orders addressed to each other), and the CB(s) involved shall book those payments simultaneously on the two TARGET2 participants' PM accounts;

7.3.3.2 if, in relation to a pair of PM accounts as described under Paragraph 7.3.3.1 of the present Appendix, liquidity is insufficient to fund the bilateral position, extract single payment orders until there is sufficient liquidity. In this case the CB(s) involved shall settle the remaining payments, except the extracted ones, simultaneously on the two TARGET2 participants' PM accounts.

7.3.3.3 After performing the checks specified under Paragraphs 7.3.3.1 to 7.3.3.2 of the present Appendix, the Bank of Latvia shall check the multilateral settlement positions (between a participant's PM account and other TARGET2 participants' PM accounts in relation to which a multilateral limit has been set). For this purpose, the procedure described under Paragraphs 7.3.3.1 to 7.3.3.2 of the present Appendix shall apply mutatis mutandis.

7.3.4 Under Algorithm 4 ("partial plus ancillary system settlement") the Bank of Latvia shall follow the same procedure as for Algorithm 2, but without extracting payment orders in relation to the settlement of an ancillary system (which settles on a simultaneous multilateral basis).

7.3.5 Under Algorithm 5 ("ancillary system settlement via sub-accounts") the Bank of Latvia shall follow the same procedure as for Algorithm 1, subject to the modification that the Bank
of Latvia shall start Algorithm 5 via the Ancillary System Interface and shall only check whether sufficient funds are available on participant sub-accounts. Moreover, no limits and reservations shall be taken into account. Algorithm 5 shall also run during night-time settlement.

7.4 Payment orders entered into the entry disposition after the start of any of algorithms 1 to 4 may nevertheless be settled immediately in the entry disposition if the positions and limits of the respective TARGET2 participants’ PM accounts are compatible with both the settlement of these payment orders and the settlement of payment orders in the current optimisation procedure. However, two algorithms shall not run simultaneously.

7.5 During daytime processing the algorithms shall run sequentially. As long as there is no pending simultaneous multilateral settlement of an ancillary system, the sequence shall be as follows:
7.5.1 Algorithm 1;
7.5.2 if Algorithm 1 fails, then Algorithm 2 shall run;
7.5.3 if Algorithm 2 fails, then Algorithm 3 shall run, or if Algorithm 2 succeeds, repeat Algorithm 1.
7.5.4 if simultaneous multilateral settlement ("procedure 5") in relation to an ancillary system is pending, Algorithm 4 shall run.

7.6 The algorithms shall run flexibly by setting a pre-defined time lag between the application of different algorithms to ensure a minimum interval between the running of two algorithms. The time sequence shall be automatically controlled. Manual intervention shall be possible.

7.7 While included in a running algorithm, a payment order shall not be revoked or reordered (change of the position in a queue). Requests for reordering or revocation of a payment order shall be queued until the algorithm is complete. If the respective payment order is settled while the algorithm is running, any request to reorder or revoke shall be rejected. If the payment order is not settled, the participant's requests shall be taken into account immediately.

8. Use of the ICM

8.1 The ICM may be used for inputting payment orders.

8.2 The ICM may be used for obtaining information and managing liquidity.

8.3 With the exception of warehoused payment orders and static data information, only data in relation to the current business day shall be available via the ICM. The screens shall be offered in English only.

8.4 Information shall be provided in "pull" mode, which means that each participant has to ask to be provided with information. Participants shall check the ICM regularly throughout the business day for important messages.

8.5 Only user-to-application mode (U2A) shall be available for participants using Internet-based access. U2A permits direct communication between a participant and the ICM. The
information is displayed in a browser running on a PC. Further details are described in the ICM User Handbook.

8.6 Each participant shall have at least one workstation with Internet access to access the ICM via U2A.

8.7 Access rights to the ICM shall be granted by using certificates, the use of which is described in more detail in Paragraphs 10 to 13 of the present Appendix.

8.8 Participants may also use the ICM to transfer liquidity:
8.8.1 between the PM account and the participant’s sub-accounts; and
8.8.2 from the PM account to the mirror account managed by the ancillary system.


9.1 Further details and examples explaining the above rules are contained in the UDFS and the ICM User Handbook, as amended from time to time and published on the ECB website in English, and in the User Manual: Internet Access for the Public Key Certification Service.

10. Issuance, suspension, reactivation, revocation and renewal of certificates

10.1 The participant shall request from Bank of Latvia the issuance of certificates allowing to access TARGET2-Latvija using Internet-based access.

10.2 The participant shall request from the Bank of Latvia the suspension or reactivation of certificates, as well as the revocation or renewal of certificates, when a certificate holder no longer wishes to have access to TARGET2 or if the participant ceases its activities in TARGET2- Latvija (e.g. as the result of a merger or acquisition).

10.3 The participant shall take every precautionary and organisational measure to ensure that certificates are used only in conformity with the System Rules.

10.4 The participant shall promptly notify the Bank of Latvia of any material change to any of the information contained in the forms submitted to the Bank of Latvia in connection with the issuance of certificates.

11. Handling of certificates by the participant

11.1 The participant shall ensure the safekeeping of all certificates and take robust organisational and technical measures to prevent damage to third parties and to ensure that each certificate is only used by the specific certificate holder to which it has been issued.

11.2 The participant shall promptly provide all information requested by the Bank of Latvia and guarantee the reliability of that information. Participants shall at all times remain fully responsible for the continued accuracy of all information provided to the Bank of Latvia in connection with the issuance of certificates.
11.3 The participants shall be fully liable for ensuring that all of their certificate holders keep their assigned certificates separate from the secret PIN and PUK codes.

11.4 The participants shall be fully liable for ensuring that none of its certificate holders use the certificates for functions or purposes other than those for which the certificates were issued.

11.5 The participant shall immediately notify the Bank of Latvia of any request and rationale for suspension, reactivation, revocation or renewal of certificates.

11.6 The participant shall immediately request the Bank of Latvia to suspend any certificates, or the keys contained therein, that are defective or that are no longer in the possession of its certificate holders.

11.7 The participant shall immediately notify the Bank of Latvia of any loss or theft of certificates.

12. Security requirements

12.1 The computer system that a participant uses to access TARGET2 using Internet-based access shall be located on the premises owned or leased by the participant. Access to TARGET2-Latvija shall only be allowed from such premises, and, for the avoidance of doubt, no remote access shall be allowed.

12.2 The participant shall run all software on computer systems that are installed and customised in accordance with current international IT security standards, which as a minimum shall include the requirements detailed in Paragraphs 12.3 and 13.4 of the present Appendix. The participant shall establish appropriate security measures regarding the computer system, including in particular anti-virus and malware protection, anti-phishing measures, hardening, and patch management procedures. All such measures and procedures shall be regularly updated by the participant.

12.3 The participant shall establish an encrypted communication link with TARGET2-Latvija for Internet access.

12.4 The user accounts in the participant's workstations shall not have administrative privileges. Privileges shall be assigned in accordance with the "least privilege" principle.

12.5 The participant shall protect the computer systems used for TARGET2-Latvija Internet access as follows:

12.5.1 it shall protect the computer systems and workstations from unauthorised physical and network access, at all times using a firewall to shield the computer systems and workstations from incoming Internet traffic, and the workstations from unauthorised access over the internal network. In addition, it shall use a firewall that protects against incoming traffic, as well as a firewall on workstations that ensures that only authorised programs communicate with the outside;

12.5.2 participants shall only be permitted to install on workstations the software that is necessary to access TARGET2 and that is authorised under the participant's internal security policy;
12.5.3 participants shall ensure that all software applications that run on the workstations are regularly updated and patched with the latest version. This applies in particular to the operating system, the Internet browser and plug-ins;
12.5.4 participants shall at all times restrict outgoing traffic from the workstations to business-critical sites, allowing only the sites required for work as well as for legitimate and reasonable software updates;
12.5.5 participants shall ensure that all critical internal flows to or from the workstations are protected against disclosure and malicious changes, especially if files are transferred through a network.
12.6 The participant shall ensure that its certificate holders at all times follow secure browsing practices, including:
12.6.1 reserving certain workstations to access sites of the same criticality level and only accessing those sites from those workstations;
12.6.2 always restarting the browser session before and after accessing TARGET2-Latvija Internet access;
12.6.3 verifying any server's SSL certificate authenticity at each logon to TARGET2-Latvija Internet access;
12.6.4 treating with suspicion e-mails that appear to come from TARGET2-Latvija, and never providing the certificate's password if asked for that password, as TARGET2-Latvija will never request a certificate’s password in an e-mail or otherwise.
12.7 The participant shall at all times implement the following management principles to alleviate risks to its system:
12.7.1 establish user management practices which ensure that only authorised users are created and remain on the system and maintain an accurate and up-to-date list of authorised users;
12.7.2 reconcile daily payment traffic to detect mismatches between authorised and actual daily payment traffic, both sent and received;
12.7.3 ensure that the certificate holders do not simultaneously browse any other Internet site and do not accesses TARGET2-Latvija at the same time.

13. Additional security requirements

13.1 The participant shall at all times ensure by means of appropriate organisational and/or technical measures that user IDs disclosed for the purpose of controlling access rights (Access Right Review) are not abused, and, in particular, that no unauthorised persons gain knowledge of them.

13.2 The participant shall have in place a user administration process to ensure the immediate and permanent deletion of the related user ID in the event that an employee or other user of a system on the premises of a participant terminates its the employment relationship with the participant's organisation.

13.3 The participant shall have in place a user administration process and shall immediately and permanently block the user IDs that are in any way exposed to risks, including the cases where certificates are lost or stolen, or where a password has been phished.

13.4 If a participant is unable to eliminate security-related faults or configuration errors (e.g. resulting from malware infected systems) after three occurrences, the SSP-providing NCBs may permanently block all the participant users' IDs.