EESTI PANK
Governor's Decree No 18
15 November 2010

Amendment of Eesti Pank Governor's Decree No 4, 9 May 2008, "Approval of TARGET2-Eesti rules"

This Decree is established on the basis of subsection 2 (1) and clause 14 3) of the Eesti Pank Act, and subsection 87 (2) of the Credit Institutions Act.

§ 1. The following amendments are made to Article 1 of Appendix "Harmonised conditions for participation in TARGET2-Eesti" (hereinafter also referred to as the *Appendix*) of Eesti Pank Governor's Decree No 4, 9 May 2008, "Approval of TARGET2-Eesti rules" (RTL 2008, 38, 548; 2009, 86, 1253):

(1) the definition of "*addressable BIC holder*" is replaced by the following:
""*addressable BIC holder*" means an entity which: a) holds a Business Identifier Code (BIC); b) is not recognised as an indirect participant; and c) is a correspondent or customer of a direct participant or a branch of a direct or indirect participant, and is able to submit payment orders to and receive payments from a TARGET2 component system via the direct participant;";
(2) the definition of "*public sector body*" is replaced by the following:
""*public sector body*" means an entity within the "public sector", the latter term as defined in Article 3 of Council Regulation (EC) No 3603/93 of 13 December 1993 specifying definitions for the application of the prohibitions referred to in Articles 104 ad 104b (1) of the Treaty;";
(3) the definition of "*credit institution*" is replaced by the following:
""*credit institution*" means a) a credit institution within the meaning of subsection 3 (1) of the Credit Institutions Act that is subject to supervision by a competent authority; or b) another credit institution within the meaning of Article 123 (2) of the Treaty on the Functioning of the European Union that is supervised on the basis of a standard comparable to the supervision carried out by a competent authority;";
(4) the definition of "*Bank Identifier Code (BIC)*" is replaced by the following:
""*Business Identifier Code (BIC)*" means a code as defined by ISO standard No 9362;";
(5) the following definition is introduced after the definition of "*investment firm*":
""*User detailed functional specifications (UDFS)*" means the most up-to-date version of the UDFS, which is the technical documentation that details how a participant interacts with TARGET2".

§ 2. Article 4 of the Appendix – Access criteria – is amended as follows:
(1) paragraph 1 is worded as follows:
"(1) The following types of entities are eligible for direct participation in TARGET2-Eesti:
(a) credit institutions established in the EEA, including when they act through a branch established in the EEA;
(b) credit institutions established outside the EEA, provided that they act through a branch established in the EEA; and
(c) NCBs of EU Member States and the ECB,
provided that the entities referred to in subparagraphs (a) and (b) are not subject to restrictive measures adopted by the Council of the European Union or Member States pursuant to Article 65(1)(b), Article 75 or Article 215 of the Treaty on the Functioning of the European Union, the implementation of which, in the view of Eesti Pank after informing the ECB, is incompatible with the smooth functioning of TARGET2.";
(2) in subparagraph (e) of paragraph 2, the terms "European Community" and "Community" are replaced by the term "Union".

§ 3. Article 32 of the Appendix – Evidence – is worded as follows:
"(4) Eesti Pank shall keep complete records of payment orders submitted and payments received by participants for a period of at least 10 years from the time at which such payment orders are submitted and payments are received; in any case, such complete records shall cover a minimum of five years for

any participant in TARGET2 that is subject to continuous vigilance pursuant to restrictive measures adopted by the Council of the European Union or Member States, or more if required by specific regulations.”.

§ 4. In Article 38 of the Appendix – Confidentiality – the term “Community” is replaced by the term “Union”.

§ 5. Paragraph 1 of Article 39 of the Appendix – Data protection, prevention of money laundering and related issues – is worded as follows:
“(1) Participants shall be deemed to be aware of, and shall comply with, all obligations on them relating to legislation on data protection, prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems, in particular in terms of implementing appropriate measures concerning any payments debited or credited on their PM accounts. Participants shall also acquaint themselves with the network service provider’s data retrieval policy prior to entering into the contractual relationship with the network service provider.”.

§ 6. In Article 40 of the Appendix – Notices – the term “SWIFT” is replaced by the term “BIC”.

§ 7. Article 44 of the Appendix – Governing law, jurisdiction and place of performance – is worded as follows:
“(2) Without prejudice to the competence of the Court of Justice of the European Union, any dispute arising from a matter relating to the relationship referred to in paragraph 1 falls under the exclusive competence of the competent courts of Estonia.”.

§ 8. In Appendix I “Technical specifications for the processing of payment orders”, the last three rows of the table in paragraph 2 “Payment message types” are replaced by the following:

MT 900	Optional	Confirmation of debit/Credit line change
MT 910	Optional	Confirmation of credit/Credit line change
MT 940/950	Optional	(Customer) statement message

§ 9. In Appendix V “Operating schedule”, the last row of the table in paragraph 3 is replaced by the following:

1.00–7.00	Settlement procedure of night-time ancillary system operations (only for ancillary system settlement procedure 6)

§ 10. The Appendix “Harmonised conditions for participation in TARGET2-Eesti” of the Eesti Pank Governor’s Decree No 4, 9 May 2008, “Approval of TARGET2-Eesti rules” is established as Appendix 1 to the Decree, and Appendix 2 “Supplemental and modified harmonised conditions for participation in TARGET2-Eesti using Internet-based access” (attached).

§ 11. This Decree shall enter into force on 22 November 2010.

Andres Lipstok
Governor

Appendix to
Eesti Pank Governor's Decree No 18,
15 November 2010,
"Amendment of "Approval of TARGET2-Eesti rules""
Appendix 2 to
Eesti Pank Governor's Decree No 4,
9 May 2008,
"Approval of TARGET2-Eesti rules"

Supplemental and modified harmonised conditions for participation in TARGET2-Eesti using Internet-based access

Article 1 – **Scope**

The conditions set out in Appendix 1 "Harmonised conditions for participation in TARGET2-Eesti" (hereinafter *Appendix 1* or *HC*) of the Eesti Pank Governor's Decree No 4, 9 May 2008, "Approval of TARGET2-Eesti rules" (hereinafter the *Decree*) apply to participants using Internet-based access to access one or more PM accounts subject to the provisions of this Appendix (hereinafter also referred to as *Appendix 2*).

Article 2 – **Definitions**

For the purposes of this Appendix, in addition to the definitions laid down in Appendix 1, the following definitions apply:

electronic certificates or *certificates* means an electronic file, issued by the certification authorities, that binds a public key with an identity and which is used to verify that a public key belongs to an individual, to authenticate the holder, to check a signature from this individual or to encrypt a message addressed to this individual. Certificates are held on a physical device such as a smart card or USB stick, and references to certificates include such physical devices. The certificates are instrumental in the authentication process of the participants assessing TARGET2 through the Internet and submitting payment messages or control messages;

Internet-based access means that the participant has opted for a PM account that can only be accessed via the Internet and the participant submits payment messages or control messages to TARGET2 by means of the Internet;

Internet service provider means the company or organisation, i.e. gateway, used by the TARGET2 participant for the purpose of accessing their TARGET2 account using Internet-based access;

certificate holder means a named, individual person, identified and designated by a TARGET2 participant as authorised to have Internet-based access to the participant's TARGET2 account. Their application for certificates will have been verified by the participant's home NCB and transmitted to the certification authorities, which will in turn have delivered certificates binding the public key with the credentials that identify the participant;

certification authorities means one or more NCBs designated as such by the Governing Council to act on behalf of the Eurosystem to issue, manage, revoke and renew electronic certificates.

Article 3 – **Inapplicable provisions**

The following provisions of Appendix 1 shall not apply with regard to Internet-based access: Article 4(1)(c) and (2)(d); Article 5 (2), (3) and (4); Articles 6 and 7; Article 11 (8); Article 14(1)(a); Articles 23 to 26; Article 41; and Appendices I, VI and VII.

Article 4 – **Supplemental and modified provisions**

The provisions of Appendix 1 shall apply with regard to Internet-based access in the following wording:

1) Article 2 (1):

"(1) The following Appendices form an integral part of the HC and apply to participants accessing a PM account using Internet-based access:

Appendix IA to Appendix 2: Technical specifications for the processing of payment orders for Internet-based access

Appendix IIA to Appendix 2: Fee schedule and invoicing for Internet-based access

Appendix II: TARGET2 compensation scheme

Appendix III: Terms of reference for capacity and country options

Appendix IV: Business continuity and contingency procedures, except paragraph 7(b) thereof

Appendix V: Operating schedule";

2) Article 3 (4) and (6):

"(4) Eesti Pank is the provider of services under the HC. Acts and omissions of the SSP-providing CBs and/or of the certification authorities shall be considered acts and omissions of Eesti Pank, for which it shall assume liability in accordance with Article 31 of the HC. Participation pursuant to the HC shall not create a contractual relationship between participants and the SSP-providing CBs when the latter act in that capacity. Instructions, messages or information which a participant receives from, or sends to, the SSP in relation to the services provided under the HC are deemed to be received from, or sent to, Eesti Pank.

(6) Participation in TARGET2 takes effect via participation in a TARGET2 component system. The HC describe the rights and obligations of participants in TARGET2-Eesti and Eesti Pank. The rules on the processing of payment orders (Title IV) refer to all payment orders submitted or payments received by any TARGET2 participant and shall apply subject to Appendix 2.";

3) Article 4(2)(e):

"(e) credit institutions or any of the entities of the types listed under subparagraphs (a) to (c), in both cases where these are established in a country with which the Union has entered into a monetary agreement allowing access by any of such entities to payment systems in the Union, subject to the conditions set out in the monetary agreement and provided that the relevant legal regime applying in the country is equivalent to the relevant Union legislation.";

4) Article 8, from the beginning of paragraph 8(1) to (including) paragraph (1)(a)(i):

"(1) To open an Interne—accessible PM account in TARGET2-Eesti, applicant participants shall:

(a) fulfil the following technical requirements:

(i) install, manage, operate and monitor and ensure the security of the necessary IT infrastructure to connect to TARGET2-Eesti and submit payment orders to it, in accordance with the technical specifications in Appendix IA to Appendix 2. In doing so, applicant participants may involve third parties, but retain sole liability; and";

5) Article 8, supplemented paragraph (1)(c):

"(c) specify that they wish to access their PM account by means of the Internet, and apply for a separate PM account in TARGET2 if they wish in addition to be able to access TARGET2 via the network service provider. Applicants shall submit a duly completed application form for the

issuance of the electronic certificates needed to access TARGET2 through Internet-based access.";
(6) Article 9 (3) and (5):
"(3) Participants using Internet-based access shall only be permitted to view the TARGET2 directory online and may not distribute it either internally or externally.
(5) Participants acknowledge that Eesti Pank and other CBs may publish participants' names and BICs."
(7) Article 10 (1), (2) and (5):
"(1) Eesti Pank shall offer Internet-based access described in this Appendix. Save where otherwise provided in the HC or required by law, Eesti Pank shall use all reasonable means within its powers to perform its obligations under the HC, without guaranteeing a result.
(2) Participants using Internet-based access to TARGET2 shall pay the fees laid down in Appendix IIA to Appendix 2.
(5) Participants shall do both of the following:
(a) actively check, at regular intervals throughout each business day, all information made available to them on the ICM, in particular for information relating to important system events (such as messages regarding the settlement of ancillary systems) and events of exclusion or suspension of a participant. Eesti Pank shall not be held responsible for any losses, direct or indirect, arising from a participant's failure to make these checks; and
(b) at all times both ensure compliance with the security requirements specified in Appendix IA to Appendix 2, in particular with respect to the safekeeping of certificates, and maintain rules and procedures to ensure that certificate holders are aware of their responsibilities with respect to the safeguarding of certificates.";
8) Article 11 (5a) and (6):
"(5a) Participants are responsible for the timely update of forms for the issuance of electronic certificates needed to access TARGET2 using Internet-based access and for the submission of new forms for the issuance of such electronic certificates to Eesti Pank. Participants are responsible for verifying the accuracy of information relating to them that is entered into TARGET2-Eesti.
(6) Eesti Pank shall be deemed to be authorised to communicate to certification authorities any information relating to participants which the certification authorities may need.";
9) Article 12 (5):
"(5) Eesti Pank shall make available a daily statement of accounts to any participant that has opted for such service.";
10) Article 13 (b):
"b) direct debit instructions received under a direct debit authorisation. Participants using Internet-based access shall not be able to send direct debit instructions from their PM account; and";
11) Article 14(1)(b):
"b) the payment message complies with the formatting rules and conditions of TARGET2-Eesti and passes the double-entry check described in Appendix IA to Appendix 2, and";
12) Article 18 (3):
"(3) When the Latest Debit Time Indicator is used, the accepted payment order shall be returned as non-settled if it cannot be settled by the indicated debit time. 15 minutes prior to the defined debit time, the instructing participant shall be informed via the ICM, rather than sent an automatic notification via the ICM. Instructing participant may also use the Latest Debit Time Indicator solely as a warning indicator. In such cases, the payment order concerned shall not be returned.";
13) Article 21 (4):
"(4) At the request of a payer, Eesti Pank may decide to change the queue position of a highly urgent payment order (except for highly urgent payment orders in the context of settlement

procedures 5 and 6) provided that this change would not affect the smooth settlement by ancillary systems in TARGET2 or would not otherwise give rise to systemic risk.";

14) Article 28 (1) and the supplemented paragraph (4):

"(1) Participants using Internet-based access shall implement adequate security controls, in particular those specified in Appendix IA to Appendix 2, to protect their systems from unauthorised access and use. Participants shall be exclusively responsible for the adequate protection of the confidentiality, integrity and availability of their systems.

(4) Participants using Internet-based access shall inform Eesti Pank immediately of any event that may affect the validity of the certificates, in particular those events specified in Appendix IA to Appendix 2, including without limitation any loss or improper use.";

15) Article 29:

"(1) The ICM:

(a) allows participants to input payments;

(b) allows participants to access information relating to their accounts and to manage liquidity;

(c) may be used to initiate liquidity transfer orders;

(d) allows participants to access system messages.

(2) Further technical details relating to the ICM to be used in connection with Internet-based access are contained in Appendix 1A to Appendix 2.";

16) Article 32 (1) and (3):

"(1) Unless otherwise provided in the HC, all payment and payment processing-related messages in relation to TARGET2, such as confirmations of debits or credits, or statement messages, between Eesti Pank and participants shall be made available for the participant on the ICM.

(3) If a participant's connection fails, the participant shall use the alternative means of transmission of messages laid down in Appendix IA to Appendix 2. In such cases, the saved or printed version of the message produced by Eesti Pank shall be accepted as evidence.

17) Article 34(4)(c):

"c) Once such an ICM broadcast message has been made available to participants using Internet-based access, those participants shall be deemed informed of the termination/- suspension of a participant's participation in TARGET2-Eesti or another TARGET2 component system. The participants shall bear any losses arising from the submission of a payment order to participants whose participation has been suspended or terminated if such payment order was entered into TARGET2-Eesti after the ICM broadcast message was made available.";

18) Article 39 (1):

"(1) Participants shall be deemed to be aware of, and shall comply with, all obligations on them relating to legislation on data protection, prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems, in particular in terms of implementing appropriate measures concerning any payments debited or credited on their PM accounts. Prior to entering into a contractual relationship with an Internet service provider, participants using Internet-based access shall acquaint themselves with that Internet service provider's data retrieval policy.";

19) Article 40 (1):

"(1) Except where otherwise provided for in the HC, all notices required or permitted pursuant to the HC shall be sent by registered post, facsimile or otherwise in writing. Notices to Eesti Pank shall be submitted to the Head of the Clearing and Settlement Department of Eesti Pank, Estonia pst 13, Tallinn, or to EPBEEE2X. Notices to the participant shall be sent to it at the address, fax number or its BIC address as the participant may from time to time notify to Eesti Pank.";

20) Article 45:

"Article 45 – Severability

If any provision in the HC or Appendix 2 is or becomes invalid, this shall not prejudice the

applicability of all the other provisions of the HC or Appendix 2.”

Appendix IA

Technical specifications for the processing of payment orders for Internet-based access

In addition to the Conditions, the following rules shall apply to the processing of payment orders using Internet-based access:

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

(1) Each participant using Internet-based access must connect to the ICM of TARGET2 using a local client, operating system and Internet browser as specified in the 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-Eesti.

(2) For the submission of payment orders and the exchange of payment messages in the PM the TARGET2 platform BIC, TRGTXEPMLVP, will 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 made by a participant using Internet-based access will identify that participant as the ordering institution.

(3) Participants using Internet-based access shall use public key infrastructure services as specified in the "User Manual: Internet Access for the public-key certification service".

2. Payment message types

(1) Internet-based participants can make the following types of payments:

(a) customer payments, i.e. credit transfers for which the ordering and/or beneficiary customer are not financial institutions;

(b) 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.

(c) bank-to-bank transfers to request the movement of funds between financial institutions;

(d) cover payments to request the movement of funds between financial institutions related to an underlying customer credit transfer.

In addition, participants using Internet-based access to a PM account can receive direct debit orders.

(2) Participants shall comply with the field specifications, as defined in Chapter 9.1.2.2 of the UDFS, Book 1.

(3) Field contents shall be validated at the level of TARGET2-Eesti in accordance with the UDFS requirements. Participants may agree among each other on specific rules regarding the field contents. However, in TARGET2-Eesti there shall be no specific checks as to whether participants comply with any such rules.

(4) Participants using Internet-based access 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

(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.

(2) The following fields of the message types shall be checked:

Details	Part of the message	Field
Sender	Basic Header	BIC Address
Message Type	Application Header	Message Type
Receiver	Application Header	Destination Address
Transaction Reference Number (TRN)	Text Block	:20
Related Reference	Text Block	:21
Value Date	Text Block	:32
Amount	Text Block	:32

(3) If all the fields described in subparagraph 2 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

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 Chapter 9.4.2 of the UDFS.

5. Predetermined settlement times

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

(2) For payment orders using the Latest Debit Time Indicator, two options shall be available:
(a) Codeword "/REJTIME/": if the payment order cannot be settled by the indicated debit time, the payment order shall be returned;
(b) Codeword "/TILTIME/": if the payment order cannot be settled by the indicated debit time, the payment order shall not be returned but shall be kept in the relevant queue.
Under both options, 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.

(3) If the codeword "/CLSTIME/" is used, the payment shall be treated in the same way as a payment order referred to in subparagraph 2(b).

6. Settlement of payment orders in the entry disposition

(1) Offsetting checks and, if appropriate, extended offsetting checks (both terms as defined in paragraphs 2 and 3) shall be carried out on payment orders entered into the entry disposition to provide quick, liquidity-saving gross settlement of payment orders.

(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 there is sufficient available liquidity on the payer's PM account.

(3) If the offsetting check fails, Eesti Pank 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 joined the queue. However, if in the queue of the payee there are higher priority payment orders addressed to other TARGET2 participants, 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

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

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

(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; 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 Chapter 2.8.1 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.

(a) Under Algorithm 1 ("all-or-nothing") Eesti Pank 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:

i) 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");

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

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

(b) Under Algorithm 2 ("partial"), Eesti Pank shall:

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

ii) 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.

Thereafter, Eesti Pank 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.

When extracting payment orders, Eesti Pank 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 Eesti Pank at its discretion.

(c) Under Algorithm 3 ("multiple"), Eesti Pank shall:

i) 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;

(ii) if, in relation to a pair of PM accounts as described under point (i), 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.

After performing the checks specified under subparagraphs (i) to (ii), Eesti Pank 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 subparagraphs (i) to (ii) shall apply mutatis mutandis.

(d) Under Algorithm 4 ("partial plus ancillary system settlement") Eesti Pank 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).

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

(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 TARGET2 participants' PM accounts concerned 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.

(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:

(a) algorithm 1;

(b) if algorithm 1 fails, then algorithm 2;

(c) if algorithm 2 fails, then algorithm 3, or if algorithm 2 succeeds, repeat algorithm 1.

When simultaneous multilateral settlement ("procedure 5") in relation to an ancillary system is pending, Algorithm 4 shall run.

(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) While included in a running algorithm, a payment order shall not be reordered (change of the position in a queue) or revoked. Requests for reordering or revocation of a payment order shall be queued until the algorithm is complete. If the payment order concerned 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

(1) The ICM may be used for inputting payment orders.

(2) The ICM may be used for obtaining information and managing liquidity.

(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.

(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.
(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.
(6) Each participant shall have at least one workstation with Internet access to access the ICM via U2A.
(7) Access rights to the ICM shall be granted by using certificates, the use of which is described more fully in paragraphs 10 to 13.
(8) Participants may also use the ICM to transfer liquidity:
(a) from their PM account to their account outside the PM;
(b) between the PM account and the participant's sub-accounts;
(c) from the PM account to the mirror account managed by the ancillary system.

9. The UDFS, the ICM User Handbook and the „User Manual: Internet Access for the Public Key Certification Service"

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 Eesti Pank's website and the TARGET2 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

(1) The participant shall request from Eesti Pank the issuance of certificates to allow them to access TARGET2-Eesti using Internet-based access.
(2) The participant shall request from Eesti Pank the suspension and reactivation of certificates, as well as the revocation and renewal of certificates, when a certificate holder no longer wishes to have access to TARGET2 or if the participant ceases its activities in TARGET2-Eesti (e.g. as the result of a merger or acquisition).
(3) The participant shall adopt every precaution and organisational measure to ensure that certificates are used only in conformity with the Harmonised Conditions.
(4) The participant shall promptly notify Eesti Pank of any material change to any of the information contained in the forms submitted to Eesti Pank in connection with the issuance of certificates.
(5) The participant may have a maximum of five active certificates for each PM account. Upon request, Eesti Pank may, at its discretion, apply for the issuance of further certificates from the certification authorities.

11. Handling of certificates by the participant

(1) The participant shall ensure the safekeeping of all certificates and adopt robust organisational and technical measures to avoid injury to third parties and to ensure that each certificate is only used by the specific certificate holder to which it was issued.
(2) The participant shall promptly provide all information requested by Eesti Pank and guarantee the reliability of that information. Participants shall at all times remain fully responsible for the continued accuracy of all information provided to Eesti Pank in connection with the issuance of certificates.
(3) The participant shall assume full responsibility for ensuring that all of its certificate holders keep their assigned certificates separate from the secret PIN and PUK codes.

(4) The participant shall assume full responsibility for ensuring that none of its certificate holders use the certificates for functions or purposes other than those for which the certificates were issued.
(5) The participant shall immediately inform Eesti Pank of any request and rationale for suspension, reactivation, revocation or renewal of certificates.
(6) The participant shall immediately request Eesti Pank to suspend any certificates, or the keys contained therein, that are defective or that are no longer in the possession of its certificate holders.
(7) The participant shall immediately notify Eesti Pank of any loss or theft of certificates.

12. Security requirements

(1) The computer system that a participant uses to access TARGET2 using Internet-based access shall be located in premises owned or leased by the participant. Access to TARGET2-Eesti shall only be allowed from such premises, and, for the avoidance of doubt, no remote access shall be allowed.
(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). The participant shall establish appropriate measures, 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.
(3) The participant shall establish an encrypted communication link with TARGET2-Eesti for Internet access.
(4) User computer accounts in the participant's workstations shall not have administrative privileges. Privileges shall be assigned in accordance with the "least privilege" principle.
(5) The participant shall at all times protect the computer systems used for TARGET2-Eesti Internet access as follows:

(a) using a firewall to shield the computer systems and workstations from incoming Internet traffic, and the workstations from unauthorised access over the internal network. The participant 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;

(b) 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;

(c) Participants shall at all times ensure that all software applications that run on the workstations are regularly updated and patched with the latest version. This applies in particular in respect of the operating system, the Internet browser and plug-ins.

(d) Participants shall at all times restrict outgoing traffic from the workstations to business-critical sites, as well as to sites required for legitimate and reasonable software updates;

(e) 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.

(6) The participant shall ensure that its certificate holders at all times follow secure browsing practices, including:

(a) reserving certain workstations to access sites of the same criticality level and only accessing those sites from those workstations;

(b) always restarting the browser session before and after accessing TARGET2-Eesti Internet access;

(c) verifying any server's SSL certificate authenticity at each logon to TARGET2-Eesti Internet access;

(d) being suspicious of e-mails that appear to come from TARGET2-Eesti, and never providing the certificate's password if asked for that password, as TARGET2-Eesti will never ask for a certificate's password in an e-mail or otherwise.

(7) The participant shall at all times implement the following management principles to alleviate risks to its system:

(a) establishing user management practices which ensure that only authorised users are created and remain on the system and maintaining an accurate and up-to-date list of authorised users;

(b) reconciling daily payment traffic to detect mismatches between authorised and actual daily payment traffic, both sent and received;

(c) ensuring that a certificate holder does not simultaneously browse any other Internet site at the same time as it accesses TARGET2-Eesti.

13. Additional security requirements

(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.

(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 leaves the participant's organisation.

(3) The participant shall have in place a user administration process and shall immediately and permanently block user IDs that are in any way compromised, including in cases where certificates are lost or stolen, or where a password has been phished.

(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 CBs may permanently block all the participant's user IDs.

Appendix IIA

Fee schedule and invoicing for Internet-based access

Fees for direct participants

1. The monthly fee for the processing of payment orders in TARGET2-[insert CB/country reference] for direct participants shall be EUR 70 per PM account Internet access fee plus EUR 100 per PM account plus a flat fee per transaction (debit entry) of EUR 0.80;
2. There shall be an additional monthly fee for direct participants who do not wish the BIC of their account to be published in the TARGET2 directory of EUR 30 per account.

Invoicing

3. In the case of direct participants, the following invoicing rules apply. The direct participant shall receive the invoice for the previous month specifying the fees to be paid, no later than on the fifth business day of the following month. Payment shall be made at the latest on the tenth working day of that month to the account specified by Eesti Pank and shall be debited from that participant's PM account.