

SUPPLEMENTAL AND MODIFIED CONDITIONS FOR THE OPENING AND OPERATION OF A PM ACCOUNT
IN TARGET2-BE USING INTERNET-BASED ACCESS'

Article 1

Scope

The Conditions set out in Annex I apply to participants using Internet-based access to access one or more PM accounts subject to the provisions of this Annex V.

Article 2

Definitions

For the purposes of this Annex, in addition to the definitions laid down in Annex I, the following definitions apply:

1. For the purposes of this Annex, the following definitions apply:
 - “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,
 - “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 for the following purposes: 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 in respect of participants accessing TARGET2 through the internet and submitting payment messages or control messages,
 - “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,
 - “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,
 - 1. “internet service provider” means the company or organisation, i.e. the gateway, used by the TARGET2 participant for the purpose of accessing their TARGET2 account using Internet-based access.
2. For the purposes of this Annex the definition of “payment order” is amended as follows:
 - “payment order” means a credit transfer order, a liquidity transfer order or a direct debit instruction.

Article 3

Inapplicable provisions

The following provisions of Annex I 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); Article 17(2); Articles 23 to 26; Article 41; and Appendices I, VI and VII.

Article 4

Supplemental and modified provisions

The following provisions of Annex I shall apply with regard to Internet-based access as modified below:

1. Article 2(1) is replaced by the following:

'1. The following Appendices form an integral part of these Conditions and apply to participants accessing a PM account using Internet-based access:

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

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

Appendix II: TARGET2 compensation scheme

Appendix III: Terms of reference for capacity and country opinions

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

Appendix V: Operating schedule.'

2. Article 3 is modified as follows:

(a) paragraph 1 is replaced by the following:

"1. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts."

(b) paragraph 2 is replaced by the following:

"2. The following payment orders are processed in TARGET2-BE:

(a) payment orders directly resulting from or made in connection with Eurosystem monetary policy operations;

(b) settlement of the euro leg of foreign exchange operations involving the Eurosystem;

(c) settlement of euro transfers resulting from transactions in cross-border large-value netting systems;

(d) settlement of euro transfers resulting from transactions in euro retail payment systems of systemic importance; and

(e) any other payment orders in euro addressed to TARGET2 participants."

(c) the following paragraph 2a is inserted:

"2a. In the interests of clarity, for technical reasons, internet-based participants shall not be able to make PM to DCA liquidity transfer orders."

(d) paragraph 4 is replaced by the following:

"4. The NBB is the provider of services under these Conditions. Acts and omissions of the SSP-providing NCBs and/or of the certification authorities shall be considered acts and omissions of NBB, for which it shall assume liability in accordance with Article 31 below. Participation pursuant to these Conditions shall not create a contractual relationship between participants and the SSP-providing NCBs 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 these Conditions are deemed to be received from, or sent to, NBB."; and

(e) paragraph 6 is replaced by the following:

"6. Participation in TARGET2 takes effect via participation in a TARGET2 component system. These Conditions describe the mutual rights and obligations of PM account holders in TARGET2-BE and the NBB. The rules on the processing of payment orders (Title IV) refer to all payment orders submitted or payments received by any PM account holder and shall apply subject to Annex V.'.

3. Article 4(2)(e) is replaced by the following:

'(e) credit institutions or any of the entities of the types listed under sub-paragraphs (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 is modified as follows:

(a) Paragraph (1)(a)(i) is replaced by the following:

'1. To open an Internet-accessible PM account in TARGET2-BE, 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-BE and submit payment orders to it, in accordance with the technical specifications in Appendix IA to Annex V. In doing so, applicant participants may involve third parties, but retain sole liability; and'; and

(b) The following paragraph (1)(c) is added:

'(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.’.

5. Article 9 is modified as follows:

(a) Paragraph 3 is replaced by the following:

‘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.’; and

(b) Paragraph 5 is replaced by the following:

‘5. Participants acknowledge that the NBB and other CBs may publish participant’s names and BICs.’.

6. Article 10 is modified as follows:

(a) Paragraphs 1 and 2 are replaced by the following:

‘1. The NBB shall offer Internet-based access described in Annex V. Save where otherwise provided in these Conditions or required by law, the NBB shall use all reasonable means within its power to perform its obligations under these Conditions, without guaranteeing a result.

2. Participants using Internet-based access to TARGET2 shall pay the fees laid down in Appendix IIA to Annex V.’; and

(b) The following paragraph 5 is added:

‘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. The NBB 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 Annex V, 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.’.

7. Article 11 is modified as follows:

(a) The following paragraph 5a is added:

‘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 the

NBB. Participants are responsible for verifying the accuracy of information relating to them that is entered into TARGET2-BE by the NBB.'; and

(b) Paragraph 6 is replaced by the following:

'6. The NBB shall be deemed to be authorised to communicate to certification authorities any information relating to participants which the certification authorities may need.'

8. Article 12(7) is replaced by the following:

'7. The NBB shall make available a daily statement of accounts to any participant that has opted for such service.'

9. Article 13 is replaced by the following:

'The following are classified as payment orders for the purposes of TARGET2:

- (a) credit transfer orders;
- (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;
- (c) liquidity transfer orders."

10. Article 14(1)(b) is replaced by the following:

'(b) the payment message complies with the formatting rules and conditions of TARGET2-BE and passes the double-entry check described in Appendix IA to Annex V;'

11. Article 16(2) is replaced by the following:

'2. Participants using Internet-based access shall not be allowed to use the AL group functionality in respect of their Internet-accessible PM account, or to combine that Internet-accessible PM account with any other TARGET2 account they hold. Limits may only be set in relation to an AL group in its entirety. Limits shall not be set in relation to a single PM account of an AL group member.'

12. Article 18(3) is replaced by the following:

'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) is replaced by the following:

'4. At the request of a payer, the NBB 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 is modified as follows:

(a) Paragraph 1 is replaced by the following:

'1. Participants using Internet-based access shall implement adequate security controls, in particular those specified in Appendix IA to Annex V, 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.'; and

(b) The following paragraph 4 is added:

'4. Participants using Internet-based access shall inform NBB immediately of any event that may affect the validity of the certificates, in particular those events specified in Appendix IA to Annex V, including, without limitation, any loss or improper use.'.

15. Article 29 is replaced by the following:

Article 29

Use of the ICM

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; and

(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 IA to Annex V.'.

16. Article 32 is modified as follows:

(a) Paragraph 1 is replaced with the following:

'1. Unless otherwise provided in these Conditions, all payment and payment processing-related messages in relation to TARGET2, such as confirmations of debits or credits, or statement messages, between the NBB and participants shall be made available for the participant on the ICM.'; and

(c) Paragraph 3 is replaced by the following:

'3. If a participant's connection fails, the participant shall use the alternative means of transmission of messages laid down in Appendix IV to Annex II. In such cases, the saved or printed version of the message produced by the NBB shall be accepted as evidence.'.

17. Article 34(4)(c) is replaced by the following:

- '(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-BE 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-BE after the ICM broadcast message was made available.'

18. Article 39(1) is replaced by the following:

- '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) is replaced by the following:

- '1. Except where otherwise provided for in these Conditions, all notices required or permitted pursuant to these Conditions shall be sent by registered post, facsimile or otherwise in writing. Notices to the NBB shall be submitted to the head of the [insert payment systems department or relevant CB unit] of NBB, [include relevant address of CB] or to the [insert BIC address of the CB]. 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 the NBB.'

20. Article 45 is replaced by the following:

'Article 45

Severability

If any provision in these Conditions or Annex V is or becomes invalid, this shall not prejudice the applicability of all the other provisions of these Conditions or Annex V.'

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-BE 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-BE.
 - (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-[insert country/CB reference] in accordance with the UDFS requirements. Participants may agree among each other on specific rules regarding the field contents. However, in TARGET2-[insert country/CB reference] 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 Number (TRN)	Reference 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, the NBB 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') the NBB 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 participants' 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'); and

(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, the NBB and other CBs involved shall settle all payments simultaneously on the PM accounts of the TARGET2 participants concerned.

(b) Under Algorithm 2 ('partial') the NBB shall:

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

(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, the NBB 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, the NBB shall start from the TARGET2 participants' 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 NBB at its discretion.

(c) Under Algorithm 3 ('multiple') the NBB shall:

(h) 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 CBs involved shall book those payments simultaneously on the two TARGET2 participants' PM accounts; and

- (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 CBs 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), the NBB shall check the multilateral settlement positions (between a participant's PM account and other TARGET2 participants' PM accounts in relation to which a multi-lateral 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') the NBB 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') the NBB shall follow the same procedure as for Algorithm 1, subject to the modification that the NBB 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) [insert if applicable] from their PM account to their account outside the PM;
 - (b) between the PM account and the participant's sub-accounts; and
 - (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 NBB'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 NBB the issuance of certificates to allow them to access TARGET2 BE using Internet-based access.
- (2) The participant shall request from NBB 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-BE, 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 NBB of any material change to any of the information contained in the forms submitted to NBB in connection with the issuance of certificates.

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 NBB and guarantee the reliability of that information. Participants shall at all times remain fully responsible for the continued accuracy of all information provided to NBB 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 NBB of any request and rationale for suspension, reactivation, revocation or renewal of certificates.

(6) The participant shall immediately request NBB 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 the NBB 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-BE 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-BE 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-BE Internet access as follows:

- (a) They 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. They shall use a firewall that protects against incoming traffic, as well as a firewall on work-stations 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-BE Internet access;
 - (c) verifying any server's SSL certificate authenticity at each logon to TARGET2-BE Internet access;
 - (d) being suspicious of e-mails that appear to come from TARGET2-BE, and never providing the certificate's password if asked for that password, as TARGET2-BE 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-BE.

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 NCBs may permanently block all the participant's user IDs.

FEE SCHEDULE AND INVOICING FOR INTERNET-BASED ACCESS

Fees for direct participants

1. The monthly fee for the processing of payment orders in TARGET2-BE for direct participants shall be EUR 70 per PM account Internet access fee plus EUR 150 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.
3. The NBB shall issue and maintain up to five active certificates per participant for each PM account free of charge. The NBB shall charge a fee of EUR 120 for the issuance of each additional subsequent active certificate. The NBB shall charge an annual maintenance fee of EUR 30 per each additional subsequent active certificate. Active certificates shall be valid for three years.

Invoicing

4. 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 the NBB and shall be debited from that participant's PM account.