21 November 2021

SPECIAL TERMS AND CONDITIONS FOR THE OPENING AND OPERATION OF A PM ACCOUNT IN TARGET2-BUNDESBANK (TARGET2-BBk) USING THE INTERNET-BASED ACCESS

TITLE I

GENERAL PROVISIONS

Article 1 - Definitions

For the purposes of these Terms and Conditions (hereinafter the 'Conditions'), the following definitions apply:

- 'addressable BIC holder' means an entity which: (a) holds a Business Identifier Code (BIC); (b) is not recognised as an indirect participant in the PM; and (c) is a correspondent or customer of a PM account holder or a branch of a direct or indirect participant in the PM, and is able to submit payment orders to and receive payments from a TARGET2 component system via the PM account holder;
- 'AL agreement' means the multilateral aggregated liquidity agreement entered into by the AL group members and their respective AL NCBs, for the purposes of the AL mode;
- 'AL group' means a group composed of AL group members that use the AL mode;
- 'AL group member' means a TARGET2 participant that has entered into an AL agreement;
- 'AL mode' means the aggregation of available liquidity on PM accounts;
- 'AL NCB' means a participating NCB that is party to an AL agreement and acts as the counterparty for the AL group members which participate in its TARGET2 component system;
- 'ancillary system (AS)' means a system managed by an entity established in the European Union or the European Economic Area (EEA) that is subject to supervision and/or oversight by a competent authority and complies with the oversight requirements for the location of infrastructures offering services in euro, as amended from time to time and published on the ECB's website[1], in which payments and/or financial instruments are exchanged and/or cleared or recorded with (a) the monetary obligations settled in TARGET2 and/or (b) funds held in TARGET2, in accordance with

[1] The Eurosystem's current policy for the location of infrastructure is set out in the following statements, which are available on the ECB's website at www.ecb.europa.eu: (a) the policy statement on euro payment and settlement systems located outside the euro area of 3 November 1998; (b) the Eurosystem's policy line with regard to consolidation in central counterparty clearing of 27 September 2001; (c) the Eurosystem policy principles on the location and operation of infrastructures settling euro-denominated payment transactions of 19 July 2007; (d) the Eurosystem policy principles on the location and operation of infrastructures settling euro-denominated payment transactions: specification of 'legally and operationally located in the euro area' of 20 November 2008; (e) the Eurosystem oversight policy framework, revised version of July 2016.(**) Guideline ECB/2012/27 of the European Central Bank of 5 December 2012 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (OJ L 30, 30.1.2013, p. 1).

Guideline ECB/2012/27 of the European Central Bank[2] and a bilateral arrangement between the ancillary system and the relevant Eurosystem CB,

- 'available liquidity' means a credit balance on a participant's PM account and, if applicable, any intraday credit line granted by the relevant euro area NCB in relation to such account but not yet drawn upon, or, if applicable, decreased by the amount of any processed reservations of liquidity on the PM account,
- 'Business Identifier Code (BIC)' means a code as defined by ISO Standard No 9362;
- 'branch' means a branch within the meaning of number 17 of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[3];
- 'business day' or "TARGET2 business day" means any day on which TARGET2 is open for the settlement of payment orders, as set out in Appendix V,
- 'CAI mode' means the provision of consolidated account information (CAI) in relation to PM accounts via the ICM;
- 'capacity opinion' means a participant-specific opinion that contains an assessment of a participant's legal capacity to enter into and carry out its obligations under these Conditions;
- 'central banks (CBs)' means the Eurosystem CBs and the connected CBs;
- '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,
- '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 of the participants accessing TARGET2 through the internet and submitting payment messages or control messages;
- '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;

---

2 Guideline ECB/2012/27 of the European Central Bank of 5 December 2012 on a Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET2) (OJ L 30, 30.1.2013, p. 1).

3 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

- 'connected CB' means a national central bank (NCB), other than a Eurosystem CB, which is connected to TARGET2 pursuant to a specific agreement;
- ‘Contingency Solution’ means the SSP functionality that processes very critical and critical payments in contingency;
- 'credit institution' means either a) credit institution within the meaning of number 1 of Article 4(1) of Regulation (EU) No 575/2013 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 (TFEU) that is subject to scrutiny of a standard comparable to supervision by a competent authority; 'credit transfer order' means an instruction by a payer to make funds available to a payee by means of a book entry on a PM account;
- 'deposit facility' means a Eurosystem standing facility which counterparties may use to make overnight deposits with an NCB at a pre-specified deposit rate;
- 'deposit facility rate' means the interest rate applicable to the deposit facility;
- ‘direct debit authorisation’ means a general instruction by a payer to its CB entitling and obliging that CB to debit the payer’s account upon receipt of a valid direct debit instruction from a payee,’;;
- 'direct debit instruction' means an instruction from a payee submitted to its CB pursuant to which the CB of the payer debits the payer's account by the amount specified in the instruction, on the basis of a direct debit authorisation;
- 'entry disposition' means a payment processing phase during which TARGET2-BBk attempts to settle a payment order which has been accepted pursuant to Article 13 by means of specific procedures as described in Article 19;
- ‘European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme’ or ‘SCT Inst scheme’ means an automated, open standards scheme providing a set of interbank rules to be complied with by SCT Inst participants, allowing payment services providers in SEPA to offer an automated, SEPA-wide euro instant credit transfer product,
- 'Eurosystem CB' means the ECB or the NCB of a Member State that has adopted the euro;
- 'event of default' means any impending or existing event, the occurrence of which may threaten the performance by a participant of its obligations under these Conditions or any other rules applying to the relationship between that participant and the Deutsche Bundesbank or any other CB, including:
  (a) where the participant no longer meets the access criteria laid down in Article 4 or the requirements laid down in Article 7(1)(a)(i);
  (b) the opening of insolvency proceedings in relation to the participant;
  (c) the submission of an application relating to the proceedings referred to in subparagraph (b);
  (d) the issue by the participant of a written declaration of its inability to pay all or any part of its debts or to meet its obligations arising in relation to intraday credit;

(e) the entry of the participant into a voluntary general agreement or arrangement with its creditors;

(f) where the participant is, or is deemed by its CB to be, insolvent or unable to pay its debts;

(g) where the participant's credit balance on its PM account or all or a substantial part of the participant's assets are subject to a freezing order, attachment, seizure or any other procedure that is intended to protect the public interest or the rights of the participant's creditors;

(h) where participation of the participant in another TARGET2 component system and/or in an ancillary system has been suspended or terminated;

(i) where any material representation or pre-contractual statement made by the participant or which is implied to have been made by the participant under the applicable law is incorrect or untrue; or

(j) the assignment of all or a substantial part of the participant's assets;

– 'group' means:

a) composition of credit institutions included in the consolidated financial statements of a parent company where the parent company is obliged to present consolidated financial statements under International Accounting Standard 27 (IAS 27), adopted pursuant to Commission Regulation (EC) No 1126/2008[4] and consisting of either:

(i) a parent company and one or more subsidiaries; or

(ii) two or more subsidiaries of a parent company; or

(b) a composition of credit institutions as referred to in subparagraphs (a)(i) or (ii), where a parent company does not present consolidated financial statements in accordance with IAS 27, but may be able to satisfy the criteria defined in IAS 27 for consolidated financial statements, subject to the verification of the CB of the direct participant or, in the case of an AL group, the managing NCB; or

(c) a bilateral or multilateral network of credit institutions that is:

(i) organised through a statutory framework determining the affiliation of credit institutions to such a network; or

(ii) characterised by self-organised mechanisms of cooperation (promoting, supporting and representing the business interests of its members) and/or economic solidarity going beyond the ordinary cooperation usual between credit institutions, such cooperation and solidarity being permitted by credit institutions' by-laws or articles of incorporation or established by virtue of separate agreements;

and in each case referred to in (c) the ECB's Governing Council has approved an application to be considered as constituting a group;

[4] Commission Regulation (EC) No 1126/2008 of 3 November 2008 adopting certain international accounting standards in accordance with Regulation (EC) No 1606/2002 of the European Parliament and of the Council (OJ L 320, 29.11.2008, p. 1).

- ‘‘Home Account” means an account opened outside the PM by a euro area NCB for a credit institution established in the Union or the EEA,
- 'Information and Control Module (ICM)' means the SSP module that allows PM account holders to obtain online information and gives them the possibility to submit liquidity transfer orders, manage liquidity and, if applicable, initiate backup payment orders or payment orders to the Contingency Solution in a contingency,
- 'ICM broadcast message' means information made simultaneously available to all or a selected group of PM account holders via the ICM,
- 'indirect participant' means a credit institution established in the Union or the EEA, which has entered into an agreement with a direct participant to submit payment orders and receive payments via such direct participant's PM account, and which has been recognised by a TARGET2 component system as an indirect participant;
- 'insolvency proceedings' means insolvency proceedings within the meaning of Article 2(j) of the Settlement Finality Directive;
- 'instructing participant' means a TARGET2 participant that has initiated a payment order;
- '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. the gateway, used by the TARGET2 participant for the purpose of accessing their TARGET2 account using internet-based access;
- 'intraday credit' means credit extended for a period of less than one business day;
- 'investment firm' means an investment firm within the meaning of section 2 (10) of the Securities Trading Act or of comparable EU Member State regulations, excluding the institutions specified in section 3 of the aforementioned Act, provided that the investment firm in question is:
  (a) authorised and supervised by a recognised competent authority, which has been designated as such under Directive 2014/65/EU; and
  (b) entitled to carry out the activities referred to under section 2 (8) sentence 1 numbers 2, 3, 5 and 6 as well as sentence 6 of the Securities Trading Act or under comparable EU Member State regulations;
- 'liquidity transfer order' means a payment order, the main purpose of which is to transfer liquidity between different accounts of the same participant or within a CAI or AL group;
- 'marginal lending facility' means a Eurosystem standing facility which counterparties may use to receive overnight credit from a Eurosystem CB at the pre-specified marginal lending rate;
- 'marginal lending rate' means the interest rate applicable to the Eurosystem marginal lending facility;

- 'multi-addressee access' means the facility by which branches or credit institutions established in the Union or the EEA can access the relevant TARGET2 component system by submitting payment orders and/or receiving payments directly to and from the TARGET2 component system; this facility authorises these entities to submit their payment orders through the direct participant's PM account without that participant's involvement;
- 'network service provider' means the undertaking appointed by the ECB's Governing Council to provide computerised network connections for the purpose of submitting payment messages in TARGET2;
- 'non-settled payment order' means a payment order that is not settled on the same business day as that on which it is accepted;
- 'participant' or "direct participant" means an entity that holds at least one PM account (PM account holder) with a Eurosystem CB,
- 'payee', except where used in Article 34, means a TARGET2 participant whose PM account will be credited as a result of a payment order being settled;
- 'payer', except where used in Article 34, means a TARGET2 participant whose PM account will be debited as a result of a payment order being settled;
- 'payment order' means a credit transfer order, a liquidity transfer order or a direct debit instruction;
- 'Payments Module (PM)' means an SSP module in which payments of TARGET2 participants are settled on PM accounts;
- 'PM account' means an account held by a TARGET2 participant in the PM with a CB which is necessary for such TARGET2 participant to:
  (a) submit payment orders or receive payments via TARGET2; and
  (b) settle such payments with such CB;
- 'public sector body' means an entity within the 'public sector', the latter term as defined in Article 3 of Council Regulation (EC) 3603/93 of 13 December 1993 specifying definitions for the application of the prohibitions referred to in Articles 104 and 104b (1) of the Treaty [5] (now Articles 123 and 125 (1) TFEU);'Settlement Finality Directive' means Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems[6];
- reachable party" means an entity which:
  (a) holds a BIC;
  (b) is designated as a reachable party by a TIPS DCA holder or by an ancillary system;
  (c) is a correspondent, customer or branch of a TIPS DCA holder or a participant of an ancillary system, or a correspondent, customer, or branch of a participant of an ancillary system; and

[5] OJ L 332, 31/12/1993, p 1.
[6] OJ L 166, 11/06/1998, p 45.

(d) is addressable through the TIPS Platform and is able to submit instant payment orders and receive instant payment orders either via the TIPS DCA holder or the ancillary system or, if so authorised by the TIPS DCA holder or by the ancillary system, directly;

- 'Single Shared Platform (SSP)' means the single technical platform infrastructure provided by the SSP-providing CBs;
- 'SSP-providing CBs' means the Deutsche Bundesbank, the Banque de France and the Banca d'Italia in their capacity as the CBs building and operating the SSP for the Eurosystem's benefit;
- 'static data collection form' means a form developed by the Deutsche Bundesbank for the purpose of registering applicants for TARGET2-BBk services and registering any changes in relation to the provision of such services;
- 'suspension' means the temporary freezing of the rights and obligations of a participant for a period of time to be determined by the Deutsche Bundesbank;
- TARGET2-BBk means the TARGET2 component system operated by the Deutsche Bundesbank;
- 'TARGET2' means the entirety resulting from all TARGET2 component systems of the CBs;
- 'TARGET2 component system' means any of the CBs' real-time gross settlement (RTGS) systems that form part of TARGET2;
- 'TARGET2 CUG' means a subset of the network service provider's customers grouped for the purpose of their use of the relevant services and products of the network service provider when accessing the PM;
- 'TARGET2 participant' means any participant in any TARGET2 component system;
- 'technical malfunction of TARGET2' means any difficulty, defect or failure in the technical infrastructure and/or the computer systems used by TARGET2-BBk, or any other event that makes it impossible to execute and complete the same business-day processing of payments in TARGET2-BBk;
- ‘TARGET Instant Payment Settlement (TIPS) service’ means the settlement in central bank money of instant payment orders on the TIPS Platform,
- ‘TIPS Dedicated Cash Account (TIPS DCA)’ means an account held by a TIPS DCA holder, opened in TARGET2 -BBk, and used for the provision of instant payment services to its customers,
- ‘TIPS Platform’ means the single technical platform infrastructure provided by the TIPS Platform-providing NCBs,
- ‘TIPS Platform-providing NCBs’ means the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d’Italia in their capacity as the CBs building and operating the TIPS Platform for the Eurosystem’s benefit,
- '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;

Article 1a Scope

The present Terms and Conditions govern the relationship between the Deutsche Bundesbank (hereinafter the 'Bank') and its PM account holder as far the opening and the operation of the PM account using the internet-based access is concerned.

Article 2 – Appendices

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

   Appendix I: Technical specifications for the processing of payment orders for

   internet-based access

   Appendix II: TARGET2 compensation scheme

   Appendix III: Terms of reference for capacity and country opinions

   Appendix IV: Business continuity and contingency procedures

   Appendix V: Operating schedule

   Appendix VI: Fee schedule and invoicing for internet-based access

   Appendix VII: Requirements regarding information security management and business continuity management

2. In the event of any conflict or inconsistency between the content of any Appendix and the content of any other provision in these Conditions, the latter shall prevail.

Article 3 - General description of TARGET2

1. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts.
2. The following transactions are processed in TARGET2-BBk:

(a) transactions 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 transactions in euro addressed to TARGET2 participants.

3. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts. TARGET2 is established and functions on the basis of the SSP through which payment orders are submitted and processed and through which payments are ultimately received in the same technical manner.
4. The Bank 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 the Bank, for which it shall assume liability in accordance with Article 26 below. Participation

pursuant to these Conditions 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 these Conditions are deemed to be received from, or sent to, the Bank.

5. TARGET2 is legally structured as a multiplicity of payment systems composed of all the TARGET2 component systems, which are designated as "systems" under the national laws implementing Directive 98/26/EC. TARGET2-BBk is designated as a "system" under section 1 (16) of the Banking Act.

6. Participation in TARGET2 takes effect via participation in a TARGET2 component system. These Conditions describe the mutual rights and obligations of participants in TARGET2-BBk using internet-based access and the Bank. 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 these conditions.

TITLE II

PARTICIPATION

Article 4 - Access criteria

1. The following types of entities are eligible for direct participation in TARGET2-BBk using internet-based access:

   (a) credit institutions established in the Union or the EEA, including when they act through a branch established in the Union or the EEA;

   (b) credit institutions established outside the EEA, provided that they act through a branch established in the Union or the EEA;

   provided that the entities referred to in points (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 the Bank after informing the ECB, is incompatible with the smooth functioning of TARGET2.

2. The Bank may, at its discretion, also admit the following entities as direct participants:

   (a) treasury departments of central or regional governments of Member States;

   (b) public sector bodies of Member States authorised to hold accounts for customers;

   (c) (i) investment firms established in the Union or the EEA, including when they act through a branch established in the Union or the EEA; and

   (ii) investment firms established outside the EEA, provided that they act through a branch established in the Union or the EEA; and

   (d) 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.

3. Electronic money institutions within the meaning of section 1 (2) number 1 of the Payment Services Supervision Act are not entitled to participate in TARGET2-BBk.

Article 5 - Direct participants

1. Direct participants in TARGET2-BBk using internet-based access shall comply with the requirements set out in Article 7(1) and (2). They shall have at least one PM account with the Bank. PM account holders that have adhered to the SCT Inst scheme by signing the SEPA Instant Credit Transfer Adherence Agreement shall be and shall remain reachable in the TIPS Platform at all times, either as a TIPS DCA holder or as a reachable party via a TIPS DCA holder.

2. Direct participants using internet-based access may not designate indirect participants or addressable BIC holders; the Bank does not provide multi-addressee access, AL mode and CAI mode to direct participants in TARGET2-BBk using internet-based access.

Article 6 - Direct participant's responsibility

1. Direct participants using the access via the network provider may designate indirect participants or addressable BIC holders and may use the multi-addressee access. For the avoidance of doubt, payment orders submitted or payments received by indirect participants and by branches with multi-addressee access shall be deemed to have been submitted or received in this case by the direct participant itself.
2. The direct participant shall be bound by such payment orders, regardless of the content of, or any non-compliance with, the contractual or other arrangements between that participant and any of the entities referred to in paragraph 1.

Article 7 - Application procedure

1. To open an internet-accessible PM account in TARGET2-BBk or to establish an internet-based access to an already existing PM account, 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 the SSP Platform and submit payment orders to it in accordance with the technical specifications in Appendix I. In doing so, applicant participants may involve third parties, but retain sole liability;
      (ii) have passed the tests required by the Bank; and
   (b) fulfil the following legal requirements:
      (i) provide a capacity opinion in the form specified in Appendix III, unless the information and representations to be provided in such capacity opinion have already been obtained by the Bank in another context; and
      (ii) for the entities referred to in Article 4(1)(b) and in Article 4(2)(c)(ii), provide a country opinion in the form specified in Appendix III, unless the information and representations to be provided in such country opinion have already been obtained by the Bank in another context.
   (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.
2. Applicants shall apply in writing to the Bank, as a minimum enclosing the following documents/information:
   (a) completed static data collection forms as provided by the Bank,
   (b) the capacity opinion, if required by the Bank, and
   (c) the country opinion, if required by the Bank.

3. The Bank may also request any additional information it deems necessary to decide on the application to participate.

4. The Bank shall reject the application to participate if:

   (a) access criteria referred to in Article 4 are not met;

   (b) one or more of the participation criteria referred to in paragraph 1 are not met; and/or

   (c) in the Bank's assessment, such participation would endanger the overall stability, soundness and safety of TARGET2-BBk or of any other TARGET2 component system, or would jeopardise the Bank's performance of its tasks as described in section 3 of the Bundesbank Act and the Statute of the European System of Central Banks and of the European Central Bank, or poses risks on the grounds of prudence.

5. The Bank shall communicate its decision on the application to participate to the applicant within one month of the Bank's receipt of the application to participate. Where the Bank requests additional information pursuant to paragraph 3, the decision shall be communicated within one month of the Bank's receipt of this information from the applicant. Any rejection decision shall contain reasons for the rejection.

Article 8 - TARGET2 directory

1. The TARGET2 directory is the database of BICs used for the routing of payment orders addressed to:

   (a) TARGET2 participants and their branches with multi-addressee access;

   (b) indirect participants of TARGET2, including those with multi-addressee access; and

   (c) addressable BIC holders of TARGET2.

   It shall be updated weekly.

2. Unless otherwise requested by the participant, its BIC(s) shall be published in the TARGET2 directory.

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.

4. Entities specified in paragraph 1(b) and (c) shall only use their BIC in relation to one direct participant.

5. The participants consent to their names and BICs being published by the Bank and other CBs.

TITLE III

OBLIGATIONS OF THE PARTIES

Article 9 – Obligations of the Bank and the participants

1. The Bank shall offer the services described in Title IV via the internet-based access. Save where otherwise provided in these Conditions or required by law, the Bank shall use all reasonable means within its power to perform its obligations under these Conditions, without guaranteeing a result.
2. Participants shall pay to the Bank the fees laid down in Appendix VI.
3. Participants shall ensure that they are connected to TARGET2-BBk on business days, in accordance with the operating schedule in Appendix V.
4. The participant represents and warrants to the Bank that the performance of its obligations under these Conditions does not breach any law, regulation or by-law applicable to it or any agreement by which it is bound.
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 Bank 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 I, 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.

Article 10 - Cooperation and information exchange

1. In performing their obligations and exercising their rights under these Conditions, the Bank and participants shall cooperate closely to ensure the stability, soundness and safety of TARGET2-BBk. They shall provide each other with any information or documents relevant for the performance of their respective obligations and the exercise of their respective rights under these Conditions, without prejudice to any banking secrecy obligations.
2. The Bank shall establish and maintain a system support desk to assist participants in relation to difficulties arising in connection with system operations.
3. 'Up-to-date information on the SSP's operational status shall be available on the TARGET2 Information System (T2IS) on a dedicated webpage on the ECB's website. The T2IS may be used to obtain information on any event affecting the normal operation of TARGET2.
4. The Bank may either communicate messages to participants by means of an ICM broadcast or by any other means of communication.
5. Participants are responsible for the timely update of existing static data collection forms and the submission of new static data collection forms to the Bank. Participants are responsible for verifying the accuracy of information relating to them that is entered into TARGET2-BBk by the Bank.

6. Participants using the internet-based access 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 Bank. Participants are responsible for verifying the accuracy of information relating to them that is entered into TARGET2-BBk by the Bank.

7. The Bank shall be deemed to be authorised to communicate to certification authorities any information relating to internet-based participants which the certification authorities may need.

8. Participants shall inform the Bank about any change in their legal capacity and relevant legislative changes affecting issues covered by the country opinion relating to them.

9. Participants shall immediately inform the Bank if an event of default occurs in relation to themselves or if they are subject to crisis prevention measures or crisis management measures within the meaning of Directive 2014/59/EU of the European Parliament and of the Council[7] or any other equivalent applicable legislation.

TITLE IV

MANAGEMENT OF PM ACCOUNTS AND PROCESSING OF PAYMENT ORDERS

Article 11 - Opening and management of PM accounts

1. The Bank shall open and operate at least one PM account for each participant. At the request of a participant that is also a clearing institution the Bank will open one or more sub-accounts in TARGET2-BBk for the purpose of dedicating liquidity.

2. PM accounts and their sub-accounts shall either be remunerated at zero per cent or at the deposit facility rate, whichever is lower, unless they are used to hold minimum reserves or they are used to hold excess reserves.

   In the case of minimum reserves, the calculation and payment of remuneration of holdings shall be governed by Council Regulation (EC) No 2531/98[8] and Regulation (EU) 2021/378 of the European Central Bank (ECB/2021/1)[9].

   In the case of excess reserves, the calculation and payment of remuneration of holdings shall be governed by Decision (EU) 2019/1743 (ECB/2019/31)[10].

---

[7] Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

[8] Council Regulation (EC) No 2531/98 of 23 November 1998 concerning the application of minimum reserves by the European Central Bank (OJ L 318, 27.11.1998, p. 1).

[9] Regulation (EU) 2021/378 of the European Central Bank of 22 January 2021 on the application of minimum reserve requirements (ECB/2021/1) (OJ L 73, 3.3.2021, p. 1).

[10] Decision (EU) 2019/1743 of the European Central Bank of 15 October 2019 on the remuneration of holdings of excess reserves and of certain deposits (ECB/2019/31) (OJ L 267, 21.10.2019, p. 12).

3. In addition to the settlement of payment orders in the Payments Module, a PM account may be used to settle payment orders to and from HAM-Accounts, according to the rules laid down by the Bank.

4. The Bank shall provide a daily statement of accounts to any participant that has opted for such service.

Article 12 - Types of payment orders

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; and

(c) liquidity transfer orders.

Article 13 - Acceptance and rejection of payment orders

1. Payment orders submitted by participants are deemed accepted by the Bank if:

   (a) the payment message complies with the formatting rules and conditions of TARGET2-BBk and passes the double-entry check described in Appendix I; and

   (b) in cases where a payer or a payee has been suspended, the suspended participant's CB's explicit consent has been obtained.

2. The Bank shall immediately reject any payment order that does not fulfil the conditions laid down in paragraph 1. The Bank shall inform the participant of any rejection of a payment order, as specified in Appendix I.

3. The SSP attaches its timestamp for the processing of payment orders in the sequence of their receipt.

Article 14 - Priority rules

1. Instructing participants shall designate every payment order as one of the following:

   (a) normal payment order (priority class 2);

   (b) urgent payment order (priority class 1); or

   (c) highly urgent payment order (priority class 0).

   If a payment order does not indicate the priority, it shall be treated as a normal payment order.

2. Highly urgent payment orders may only be designated by:

   (a) CBs; and

   (b) participants, in cases of payments to and from CLS Bank International, with the exception of payments related to the CLS CCP and the CLSNow services, and liquidity transfers in relation to ancillary system settlement using the ASI.

   All payment instructions submitted by an ancillary system through the ASI to debit or credit the participants' PM accounts shall be deemed to be highly urgent payment orders.

3. Liquidity transfers initiated in the ICM constitute urgent payment orders.

4. In the case of urgent and normal payment orders, the payer may change the priority via the ICM with immediate effect. It shall not be possible to change the priority of a highly urgent payment.

Article 15 - Liquidity limits

1. A participant may limit the use of available liquidity for payment orders in relation to other TARGET2 participants, except any of the CBs, by setting bilateral or multilateral limits. Such limits may only be set in relation to normal payment orders.

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.

3. By setting a bilateral limit, a participant instructs the Bank that an accepted payment order shall not be settled if the sum of its outgoing normal payment orders to another TARGET2 participant's PM account minus the sum of all incoming urgent and normal payments from such TARGET2 participant's PM account would exceed this bilateral limit.

4. A participant may set a multilateral limit only for any relationship that is not subject to a bilateral limit. A multilateral limit may only be set if the participant has set at least one bilateral limit. If a participant sets a multilateral limit, it instructs the Bank that an accepted payment order shall not be settled if the sum of its outgoing normal payment orders to all TARGET2 participants' PM accounts in relation to which no bilateral limit has been set, minus the sum of all incoming urgent and normal payments from such PM accounts would exceed this multilateral limit.

5. The minimum amount of any of the limits shall be EUR 1 million. A bilateral or a multilateral limit with an amount of zero shall be treated as if no limit has been set. Limits between zero and EUR 1 million are not possible.

6. Limits may be changed in real time with immediate effect or with effect from the next business day via the ICM. If a limit is changed to zero, it shall not be possible to change it again on the same business day. The setting of a new bilateral or multilateral limit shall only be effective from the next business day.

Article 16 - Liquidity reservation facilities

1. Participants may reserve liquidity for highly urgent or urgent payment orders via the ICM.

2. By requesting to reserve a certain amount of liquidity for highly urgent payment orders, a participant instructs the Bank only to settle urgent and normal payment orders if there is available liquidity after the amount reserved for highly urgent payment orders has been deducted.

3. By requesting to reserve a certain amount of liquidity for urgent payment orders, a participant instructs the Bank only to settle normal payment orders if there is available liquidity after the amount reserved for urgent and highly urgent payment orders has been deducted.

4. After receipt of the reservation request the Bank shall check whether the amount of liquidity on the participant's PM account is sufficient for the reservation. If this is not the case, only the liquidity available on the PM account shall be reserved. The rest of the requested liquidity reservation shall be reserved if additional liquidity is available.

5. The level of the liquidity reservation may be changed. Participants may make a request via the ICM to reserve new amounts with immediate effect or with effect from the next business day.

Article 16a – Direct debit orders for the purpose of reserving and dedicating liquidity

1. Participants may predetermine the reserved liquidity amount for highly urgent or urgent payment orders via the ICM. This direct debit order or any modification to it shall be effective as of the next business day.

2. Participants may use the ICM to predetermine the reserved liquidity amount needed for the settlement of ancillary systems. This direct debit order or any modification to it shall be effective as of the next business day. The Bank shall be deemed as having received instructions from participants to dedicate liquidity (ie to transfer it to the respective participant's sub-account) if an application to this effect is submitted by the ancillary system concerned.

Article 17 - Predetermined settlement times

1. Instructing participants may predetermine the settlement time of the payment orders within a business day by using the Earliest Debit Time Indicator or the Latest Debit Time Indicator.

2. When the Earliest Debit Time Indicator is used, the accepted payment order is stored and only entered into the entry disposition at the indicated time.

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, but will not receive 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

4. Instructing participants can change the Earliest Debit Time Indicator and the Latest Debit Time Indicator via the ICM.

5. Further technical details are contained in Appendix I.

Article 18 - Payment orders submitted in advance

1. Payment orders may be submitted up to five business days before the specified settlement date (warehoused payment orders).

2. Warehoused payment orders shall be accepted and entered into the entry disposition on the date specified by the instructing participant at the start of daytime processing, as referred to in Appendix V. They shall be placed in front of payment orders of the same priority.

3. Articles 14(3), 21(2) and 24(1)(a) shall apply mutatis mutandis to warehoused payment orders.

Article 19 - Settlement of payment orders in the entry disposition

1. Unless instructing participants have indicated the settlement time in the manner described in Article 17, accepted payment orders shall be settled immediately or at the latest by the end of the business day on which they were accepted, provided that sufficient funds are available on the payer's PM account and taking into account any liquidity limits and liquidity reservations as referred to in Articles 15 and 16.
2. Funding may be provided by:
   (a) the available liquidity on the PM account; or
   (b) incoming payments from other TARGET2 participants, subject to the applicable optimisation procedures.
3. For highly urgent payment orders the 'first in, first out' (FIFO) principle shall apply. This means that highly urgent payment orders shall be settled in chronological order. Urgent and normal payment orders shall not be settled for as long as highly urgent payment orders are queued.
4. For urgent payment orders the FIFO principle shall also apply. Normal payment orders shall not be settled if urgent and highly urgent payment orders are queued.
5. By derogation from paragraphs 3 and 4, payment orders with a lower priority (or of the same priority but accepted later) may be settled before payment orders with a higher priority (or of the same priority which were accepted earlier), if the payment orders with a lower priority would net out with payments to be received and result on balance in a liquidity increase for the payer.
6. Normal payment orders shall be settled in accordance with the FIFO by-passing principle. This means that they may be settled immediately (independently of other queued normal payments accepted at an earlier time) and may therefore breach the FIFO principle, provided that sufficient funds are available.
7. Further details on the settlement of payment orders in the entry disposition are contained in Appendix I.

Article 20 - Settlement and return of queued payment orders

1. Payment orders that are not settled immediately in the entry disposition shall be placed in the queues in accordance with the priority to which they were designated by the relevant participant, as referred to in Article 14.
2. To optimise the settlement of queued payment orders, the Bank may use the optimisation procedures described in Appendix I.
3. Except in the case of highly urgent payment orders, the payer may change the queue position of payment orders in a queue (ie reorder them) via the ICM. Payment orders may be moved either to the front or to the end of the respective queue with immediate effect at any time during daytime processing, as referred to in Appendix V.
4. At a payer’s request, the Bank may decide to change the position of a highly urgent payment order in the queue (with the exception of highly urgent payment orders included in the settlement

procedures 5 and 6) provided this change does not impede the smooth functioning of settlement operations by ancillary systems in TARGET2 or lead to systemic risks elsewhere.

5. Liquidity transfer orders initiated in the ICM shall be immediately returned as non-settled if there is insufficient liquidity. Other payment orders shall be returned as non-settled if they cannot be settled by the cut-off times for the relevant message type, as specified in Appendix V.

Article 21 - Entry of payment orders into the system and their irrevocability

1. For the purposes of the first sentence of Article 3(1) of the Settlement Finality Directive and the German national law provisions implementing this Settlement Finality Directive, payment orders are deemed entered into TARGET2-BBk at the moment that the relevant participant's PM account is debited.

2. Payment orders may be revoked until they are entered into TARGET2-BBk in accordance with paragraph 1. Payment orders that are included in an algorithm, as referred to in Appendix I, may not be revoked during the period that the algorithm is running.

TITLE V

SECURITY REQUIREMENTS AND CONTINGENCY ISSUES

Article 22 – Business continuity and contingency procedures

1. In the event of an abnormal external event or any other event which affects the operation of the SSP, the business continuity and contingency procedures described in Appendix IV shall apply.

2. The Eurosystem provides a Contingency Solution if the events described in paragraph 1 occur. Connection to and use of the Contingency Solution shall be mandatory for participants considered by the Bank to be critical. Other participants, not using the internet-based access, may, on request, connect to the Contingency Solution.

Article 23 - Security Requirements and Control Procedures

1. Participants using internet-based access shall implement adequate security controls, in particular those specified in Appendix I, 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.

2. Participants shall inform the Bank of any security-related incidents in their technical infrastructure and, where appropriate, security-related incidents that occur in the technical infrastructure of the third party providers. The Bank may request further information about the incident and, if necessary, request that the participant take appropriate measures to prevent a recurrence of such an event.3. The Bank may impose additional security requirements, in particular with regard to cybersecurity or the prevention of fraud, on all participants and/or on participants that are considered critical by the Bank.

4. Participants using internet-based access shall provide the Bank on annual basis with the TARGET2 self-certification statement as published on the Bank's website and on the ECB's website in English.

4a. The Bank shall assess the participant's self-certification statement(s) on the participants level of compliance with each of the requirements set out in the TARGET2 self-certification requirements. These requirements are listed in Appendix VII, which in addition to the other Appendices listed in Article 2(1), shall form an integral part of these Conditions.

4b. The participant's level of compliance with the requirements of the TARGET2 self-certification shall be categorised as follows, in increasing order of severity: 'full compliance'; 'minor non-compliance'; or, 'major non-compliance'. The following criteria apply: full compliance is reached where participants satisfy 100% of the requirements; minor non-compliance is where a participant satisfies less than 100% but at least 66% of the requirements and major non-compliance where a participant satisfies less than 66% of the requirements. If a participant demonstrates that a specific requirement is not applicable to it, it shall be considered as compliant with the respective requirement for the purposes of the categorisation. A participant which fails to reach 'full compliance' shall submit an action plan demonstrating how it intends to reach full compliance. The Bank shall inform the relevant supervisory authorities of the status of such participant's compliance.

4c. If the participant does not provide the TARGET2 self-certification the participant's level of compliance shall be categorised as 'major non-compliance'.

4d. The Bank shall re-assess compliance of participants on an annual basis.

4e. The Bank may impose the following measures of redress on participants whose level of compliance was assessed as minor or major non-compliance, in increasing order of severity:

(i) enhanced monitoring: the participant shall provide the Bank with a monthly report, signed by a senior executive, on their progress in addressing the non-compliance. The participant shall additionally incur a monthly penalty charge for each affected account equal to its monthly fee as set out in paragraph 1 of Appendix VI excluding the transaction fees. This measure of redress may be imposed in the event the participant receives a second consecutive assessment of minor non-compliance or an assessment of major non-compliance;

(ii) suspension: participation in TARGET2-BBk may be suspended in the circumstances described in Article 29(2)(b) and (c) of these Terms and Conditions. By way of derogation from Article 29 of these Terms and Conditions, the participant shall be given three months' notice of such suspension. The participant shall incur a monthly penalty charge for each suspended account of double its monthly fee as set out in paragraph 1 of Appendix VI, excluding the transaction fees. This measure of redress may be imposed in the event the participant receives a second consecutive assessment of major non-compliance;

(iii) termination: participation in TARGET2-BBk may be terminated in the circumstances described in Article 29(2)(b) and (c) of these Terms and Conditions. By way of derogation from

Article 29 of these Terms and Conditions, the participant shall be given three months' notice of such termination. The participant shall incur an additional penalty charge of EUR 1000 for each terminated account. This measure of redress may be imposed if the participant has not addressed the major non-compliance to the satisfaction of Bank following three months of suspension.

5. Participants using internet-based access shall inform the Bank immediately of any event that may affect the validity of the certificates, in particular those events specified in Appendix I, including, without limitation, any loss or improper use.

TITLE VI

THE INFORMATION AND CONTROL MODULE (ICM)

Article 24 - 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 I.

TITLE VII

COMPENSATION, LIABILITY REGIME AND EVIDENCE

Article 25 - Compensation scheme

If a payment order cannot be settled on the same business day on which it was accepted due to a technical malfunction of TARGET2, the Bank shall offer to compensate the direct participants concerned in accordance with the special procedure laid down in Appendix II.

Article 26 - Liability regime

1. In performing their obligations pursuant to these Conditions, the Bank and the participants shall be bound by a general duty of reasonable care in relation to each other.
2. The Bank shall be liable vis-à-vis its participants in cases of fraud (including but not limited to wilful misconduct) or gross negligence for any loss arising out of the operation of TARGET2-BBk. In cases of ordinary negligence, the Bank's liability shall be limited to the participant's direct loss, ie the amount of the transaction in question and/or the loss of interest thereon, excluding any consequential loss.
3. The Bank is not liable for any loss that results from any malfunction or failure in the technical infrastructure (including but not limited to the Bank's computer infrastructure, programmes, data, applications or networks), if such malfunction or failure arises in spite of the Bank having adopted

those measures that are reasonably necessary to protect such infrastructure against malfunction or failure, and to resolve the consequences of such malfunction or failure (the latter including but not limited to initiating and completing the business continuity and contingency procedures referred to in Appendix IV).

4. The Bank shall not be liable

   (a) to the extent that the loss is caused by the participant; or

   (b) if the loss arises out of external events beyond the Bank's reasonable control (*force majeure*).

5. When acting as an intermediary, the Bank shall be liable within the framework of statutory recourse (section 676a of the German Civil Code), only insofar as the payment service provider could not have excluded or limited its liability vis-à-vis the payment service user in accordance with the statutory provisions.

6. The Bank and the participants shall take all reasonable and practicable steps to mitigate any damage or loss referred to in this Article.

7. In performing some or all of its obligations under these Conditions, the Bank may commission third parties in its own name, particularly telecommunications or other network providers or other entities, if this is necessary to meet the Bank's obligations or is standard market practice. The Bank's obligation shall be limited to the due selection and commissioning of any such third parties and the Bank’s liability shall be limited accordingly. For the purposes of this paragraph, the SSP-providing CBs shall not be considered as third parties.

Article 27 - Evidence

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 Bank and participants using internet-based access shall be made available for the participant on the ICM.

2. Electronic or written records of the messages retained by the Bank or by the network service provider shall be accepted as a means of evidence of the payments processed through the Bank. The saved or printed version of the original message of the network service provider shall be accepted as a means of evidence, regardless of the form of the original message.

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

4. The Bank shall keep complete records of payment orders submitted and payments received by participants for a period of ten years from the time at which such payment orders are submitted and payments are received.

5. The Bank's own books and records (whether kept on paper, microfilm, microfiche, by electronic or magnetic recording, in any other mechanically reproducible form or otherwise) shall be accepted as

a means of evidence of any obligations of the participants and of any facts and events that the parties rely on.

TITLE VIII

TERMINATION OF PARTICIPATION AND CLOSURE OF ACCOUNTS

Article 28 - Duration and ordinary termination of participation

1. Without prejudice to Article 29, participation in TARGET2-BBk is for an indefinite period of time.
2. A participant may terminate its participation in TARGET2-BBk at any time giving 14 business days' notice thereof, unless it agrees a shorter notice period with the Bank.
3. The Bank may terminate a participant's participation in TARGET2-BBk at any time, giving 3 months' notice thereof, unless it agrees a different notice period with that participant.
4. On termination of participation, the confidentiality duties laid down in Article 33 remain in force for a period of five years starting on the date of termination.
5. On termination of participation, the PM accounts of the participant concerned shall be closed in accordance with Article 30.

Article 29 - Suspension and extraordinary termination of participation

1. A participant's participation in TARGET2-BBk shall be immediately terminated without prior notice or suspended in the same manner if one of the following events of default occurs:
   (a) the opening of insolvency proceedings; and/or
   (b) the participant no longer meets the access criteria laid down in Article 4.
2. For the purposes of this paragraph, the taking of crisis prevention measures or crisis management measures within the meaning of Directive 2014/59/EU of the European Parliament and of the Council[11] against a PM account holder shall not automatically qualify as the opening of insolvency proceedings.2. The Bank may terminate without prior notice or suspend the participant's participation in TARGET2-BBk if:
   (a) one or more events of default (other than those referred to in paragraph 1) occur;
   (b) the participant is in material breach of these Conditions;
   (c) the participant fails to carry out any material obligation to the Bank;
   (d) the participant is excluded from, or otherwise ceases to be a member of, a TARGET2 CUG;
   (e) any other participant-related event occurs which, in the Bank’s assessment, would threaten the overall stability, soundness and safety of TARGET2-BBk or of any other TARGET2 component system, or which would jeopardise the Bank’s performance of its tasks as

[11] Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

described in section 3 of the Bundesbank Act and the Statute of the European System of Central Banks and of the European Central Bank, or poses risks on the grounds of prudence; and/or

(f) an NCB suspends or terminates the participant's access to intraday credit.

3. In exercising its discretion under paragraph 2, the Bank shall take into account, *inter alia*, the seriousness of the event of default or events mentioned in subparagraphs (a) to (c).

4. (a) In the event that the Bank suspends or terminates a PM account holder's participation in TARGET2-BBk under paragraph 1 or 2, the Bank shall immediately inform, by means of an ICM broadcast message that PM account holder, other CBs and PM account holders in all of the TARGET2 component systems of such suspension or termination. Such message shall be deemed to have been issued by the home NCB of the PM account holder that receives the message.

(b) 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-BBk 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-BBk after the ICM broadcast message was made available.

5. Upon termination of a participant's participation, TARGET2-BBk shall not accept any new payment orders from such participant. Payment orders in the queue, warehoused payment orders or new payment orders in favour of such participant shall be returned.

6. If a PM account holder is suspended from TARGET2-BBk on grounds other than those specified in paragraph 1 (a), all of its incoming payments and outgoing payment orders shall be stored and only entered into the entry disposition after they have been explicitly accepted by the suspended PM account holder's CB.

7. If a PM account holder is suspended from TARGET2-BBk on the grounds specified in paragraph 1 (a), any outgoing payment orders from that PM account holder shall only be processed on the instructions of its representatives, including those appointed by a competent authority or a court, such as the PM account holder's insolvency administrator, or pursuant to an enforceable decision of a competent authority or a court providing instructions as to how the payments are to be processed. All incoming payments shall be processed in accordance with paragraph 6.

Article 30 - Closure of PM accounts

1. Participants may close their PM accounts at any time provided they give the Bank 14 business days' notice thereof.

2. On termination of participation, pursuant to either Article 28 or 29, the Bank shall close the PM accounts of the participant concerned, after having:

(a) settled or returned any queued payment orders; and

(b) made use of its rights of pledge and set-off under Article 31.

TITLE IX

FINAL PROVISIONS

Article 31 – Bank's rights of pledge and set-off

1. The Bank shall have a pledge over the participant's existing and future credit balances on its PM accounts, thereby collateralising any current and future claims arising out of the legal relationship between the parties.
2. Notwithstanding the commencement of any insolvency proceedings in respect of a participant and notwithstanding any assignment, judicial or other attachment or other disposition of or in respect of the participant's rights, on the occurrence of such event all obligations of the participant shall be automatically and immediately accelerated, so as to be immediately due in case of
   (a) an event of default, referred to in Article 29, paragraph 1 or
   (b) any other event of default or event referred to in article 29 (2) that has led to the termination or suspension of the participant's participation in TARGET2-BBk

   Such acceleration shall occur without prior notice and without the need for any prior approval of any authority. In addition, the mutual obligations of the participant and the Bank shall automatically be set off against each other, and the party owing the higher amount shall pay to the other the difference.
3. The Bank shall promptly give the participant notice of any set-off pursuant to paragraph 2 after such set-off has taken place.
4. The Bank may, without prior notice, debit any participant's PM account by any amount which the participant owes the Bank resulting from the legal relationship between the participant and the Bank.

Article 32 - Security rights in relation to funds on sub-accounts

1. The Bank shall have a right of pledge over the balance on a participant's sub-account opened for the settlement of AS-related payment instructions under the arrangements between the relevant ancillary system and its CB. Such balance shall collateralise the participant's obligation referred to in paragraph 7 towards the Bank in relation to such settlement.
2. The Bank shall freeze the balance on the sub-account of the participant upon communication by the ancillary system (via a 'start-of-cycle' message). Subsequent to this, the Bank shall, where necessary, increase or reduce the frozen amount by crediting or debiting funds to /from the sub-account in the form of payments by way of cross-system settlement or through crediting liquidity transfers to the sub-account Such freezing shall expire upon communication by the ancillary system (via an 'end-of-cycle' message).
3. By confirming the freezing of the balance on the participant's sub-account, the Bank guarantees to the ancillary system payment up to the amount of this particular balance. Any confirmation which

may have to be submitted concerning action to increase or reduce the frozen amount by crediting or debiting funds to /from the sub-account by means of payments via cross-system settlement or through crediting liquidity transfers to the sub-account automatically has the effect of increasing or reducing the guarantee by the amount of said payments. Irrespective of the abovementioned increase or reduction, the guarantee shall be irrevocable, unconditional and payable on first demand. If the Bank is not the ancillary system's CB, the Bank shall be deemed instructed to issue the abovementioned guarantee to the ancillary system's CB.

4. In the absence of any insolvency proceedings in relation to the participant, the AS-related payment instructions for the squaring of the participant's settlement obligation shall be settled without drawing on the guarantee and without recourse to the security right over the balance on the participant's sub-account.

5. In the event of the participant's insolvency, the AS-related payment instruction for the squaring of the participant's settlement obligation shall be a first demand for payment under the guarantee; the debiting of the instructed amount from the participant's sub-account (and crediting of the AS's technical account) shall therefore equally involve the discharge of the guarantee obligation by the Bank and a realisation of its collateral right over the balance on the participant's sub-account.

6. The guarantee shall expire upon communication by the ancillary system that the settlement has been completed (via an 'end-of-cycle' message).

7. The participant shall be obliged to reimburse to the Bank any payment made by the latter under such guarantee.

Article 33 - Confidentiality

1. The Bank shall keep confidential all sensitive or secret information, including when such information relates to payment, technical or organisational information belonging to the participant, participants from the same group or the participant's customers, unless the participant or its customer has given its written consent to disclose or such disclosure is permitted or required under German law.

1a. By derogation from paragraph 1, the participant agrees that information on any action taken under Article 29 shall not be considered as confidential.

2. By derogation from paragraph 1, the participant agrees that the Bank may disclose payment, technical or organisational information regarding the participant, participants from the same group or the participant's customers obtained in the course of the operation of TARGET2-BBk to (a) other CBs or third parties that are involved in the operation of TARGET2-BBk, to the extent that this is necessary for the efficient functioning of TARGET2 or the monitoring of the participant's or its group's exposure; (b) other CBs in order to carry out the analyses necessary for market operations, monetary policy functions, financial stability or financial integration; or (c) supervisory, resolution and oversight authorities of Member States and the Union, including CBs, to the extent that this is necessary for the performance of their public tasks, and provided in all such cases that

the disclosure is not in conflict with the applicable law. The Bank shall not be liable for the financial and commercial consequences of such disclosure.

3. By derogation from paragraph 1 and provided that this does not make it possible, whether directly or indirectly, to identify the participant or the participant's customers, the Bank may use, disclose or publish payment information regarding the participant or the participant's customers for statistical, historical, scientific or other purposes in the exercise of its public functions or of functions of other public entities to which the information is disclosed.

4. Information relating to the operation of TARGET2-BBk to which participants have had access may only be used for the purposes laid down in these Conditions. Participants shall keep such information confidential unless the Bank has explicitly given its written consent to disclose. Participants shall ensure that any third parties to whom they outsource, delegate or subcontract tasks which have or may have an impact on the performance of their obligations under these Conditions are bound by the confidentiality requirements in this Article.

5. The Bank shall be authorised, in order to settle payment orders, to process and transfer the necessary data to the network service provider.

Article 34 - Data protection, prevention of money laundering, administrative or restrictive measures and related issues

1. Participants shall be deemed to be aware of, shall comply with, and shall be able to demonstrate that compliance to the relevant competent authorities with all obligations on them relating to legislation on data protection. They shall be deemed to be aware of, and shall comply with all obligations on them relating to legislation on 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 ensure that they are informed about the internet service provider's data retrieval policy prior to entering into the contractual relationship with the internet service provider.

2. Participants shall be deemed to have authorised the Bank to obtain any information relating to them from any financial or supervisory authority or trade body, whether national or foreign, if such information is necessary for the participant's participation in TARGET2-BBk.

3. Participants, when acting as the payment service provider of a payer or payee, shall comply with all requirements resulting from administrative or restrictive measures imposed pursuant to Articles 75 or 215 of the Treaty to which they are subject, including with respect to notification and/or the obtaining of consent from a competent authority in relation to the processing of transactions. In addition:

   (a) when the Bank is the payment service provider of a participant that is a payer:

      (i) the participant shall make the required notification or obtain consent on behalf of the central bank that is primarily required to make notification or obtain consent,

and shall provide the Bank with evidence of having made a notification or having received consent;

(ii) the participant shall not enter any payment order for the transfer of funds to an account held by an entity different than the participant, into TARGET2 until it has obtained confirmation from the Bank that the required notification has been made or the consent has been obtained by or on behalf of the payment service provider of the payee;

(b) when the Bank is a payment service provider of a participant that is a payee, the participant shall make the required notification or obtain consent on behalf of the central bank that is primarily required to make notification or obtain consent, and shall provide the Bank with evidence of having made a notification or having received consent.

For the purposes of this paragraph, the terms 'payment service provider', 'payer' and 'payee' shall have the meanings ascribed to them in the applicable administrative or restrictive measures.

Article 35 - Notices

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 Bank are to be sent to the head of the TARGET2-BBk National Service Desk at the Deutsche Bundesbank, Wilhelm-Epstein-Strasse 14, 60431 Frankfurt am Main, Germany or to the BIC of the Deutsche Bundesbank, MARKDEFF. Notices to the participant shall be sent to it at the address, fax number or designated BIC provided by such participant.
2. To prove that a notice has been sent, it shall be sufficient to prove that the notice was delivered to the relevant address or that the envelope containing such notice was properly addressed and posted.
3. All notices shall be given in German and/or English.
4. Participants shall be bound by all forms and documents of the Bank that the participants have filled in and/or signed, including but not limited to static data collection forms, as referred to in Article 7(2)(a), and information provided under Article 10(5), which were submitted in compliance with paragraphs 1 and 2 and which the Bank reasonably believes to have received from the participants, their employees or agents.

Article 36 - Amendment procedure

The Bank may at any time unilaterally amend these Conditions, including the Appendices. Amendments to these Conditions, including the Appendices, shall be announced by mail or by electronic means. Amendments shall be deemed to have been accepted unless the participant expressly objects within 14 days of being informed of such amendments. In the event that a participant objects to the amendment, the Bank is entitled to immediately terminate that participant's participation in TARGET2-BBk and close any of its PM accounts.

Article 37 - Third party rights

1. Any rights, interests, obligations, responsibilities and claims arising from or relating to these Conditions shall not be transferred, pledged or assigned by participants to any third party without the Bank's written consent.
2. These Conditions do not create any rights in favour of or obligations in relation to any entity other than the Bank and participants in TARGET2-BBk.

Article 38 - Governing law, jurisdiction and place of performance

1. The bilateral relationship between the Bank and participants in TARGET2-BBk shall be governed by German law.
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 Frankfurt am Main.
3. The place of performance concerning the legal relationship between the Bank and the participants shall be Frankfurt am Main.

Article 39 - Severability

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

Article 39a – Transitional provisions

1. Once the TARGET system is operational and TARGET2 has ceased operation, PM account balances shall be transferred to the account holder’s corresponding successor accounts in the TARGET system. With the start of operation of TARGET PM accounts will be closed and these Terms and Conditions become inapplicable.
2. The requirement that PM account holders adhering to the SCT Inst scheme be reachable in the TIPS Platform pursuant to Article 5 shall apply as of 25 February 2022.

Article 40 - Entry into force and binding nature

1. These Conditions become effective from 21 November 2021.
2. By requesting a PM account in TARGET2-BBk, applicant participants using internet-based access automatically agree to these Conditions in relation to the other participants and to the Bank.

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

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

1. Technical requirements for participation in TARGET2-BBk 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 Appendix "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 SWIFT BIC. Furthermore, each participant shall pass a series of tests to prove its technical and operational competence before it may participate in TARGET2-BBk.

(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 User Detailed Functional Specifications (UDFS), Book 1.

(3) Field contents shall be validated at the level of TARGET2-BBk in accordance with the UDFS requirements. Participants may agree among each other on specific rules regarding the field

contents. However, in TARGET2-BBk 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 SWIFT 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 paragraph 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 paragraph 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 Bank 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 the order 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 Bank 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'); 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 relevant each PM account, the Bank and other CBs involved shall settle all payments simultaneously on the PM accounts of the TARGET2 participants concerned.

(b) Under Algorithm 2 ('partial') the Bank 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 Bank 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 Bank 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 at its discretion.

(c) Under Algorithm 3 ('multiple') the Bank 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 PM accounts of the two TARGET2 participants; 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 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 points (i) to (ii), the Bank 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') the Bank 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 Bank shall follow the same procedure as for Algorithm 1, subject to the modification that the Bank shall start Algorithm 5 via the Ancillary System Interface (ASI) 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 the 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) f 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 Information and Control Module (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 HAM-Account;

(b) between the PM account and the participant's sub-accounts; and

(c) from the PM account to the technical account managed by the ancillary system using settlement procedure 6 real-time.

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 Bank's website (www.target2.bundesbank.de) 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 the Bank the issuance of certificates to allow them to access TARGET2-BBk using internet-based access.

(2) The participant shall request from the Bank 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-BBk (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 the Bank of any material change to any of the information contained in the forms submitted to the Bank in connection with the issuance of certificates.

(5) The participant may have a maximum of five active certificates for each PM account. Upon request, the Bank 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 the Bank 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 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 the Bank of any request and rationale for suspension, reactivation, revocation or renewal of certificates.

(6) The participant shall immediately request the Bank 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 Bank 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-BBk 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-BBk 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-BBk 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 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-BBk internet access;

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

(d) being suspicious of e-mails that appear to come from TARGET2-BBk, and never providing the certificate's password if asked for that password, as TARGET2-BBk 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-BBk.

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.

TARGET2 COMPENSATION SCHEME

1. General principles

(a) If there is a technical malfunction of TARGET2, direct participants may submit claims for compensation in accordance with the TARGET2 compensation scheme laid down in this Appendix.

(b) Unless otherwise decided by the ECB's Governing Council, the TARGET2 compensation scheme shall not apply if the technical malfunction of TARGET2 arises out of external events beyond the reasonable control of the CBs concerned or as a result of acts or omissions by third parties.

(c) Compensation under the TARGET2 compensation scheme shall be the only compensation procedure offered in the event of a technical malfunction of TARGET2. Participants may, however, use other legal means to claim for losses. If a participant accepts a compensation offer under the TARGET2 compensation scheme, this shall constitute the participant's irrevocable agreement that it thereby waives all claims it may have against any CB in relation to the payment orders for which it accepts compensation (including any claims for consequential loss), and that its receipt of the corresponding compensation payment constitutes full and final settlement of all such claims. The participant shall indemnify the CBs concerned, up to a maximum of the amount received under the TARGET2 compensation scheme, in respect of any further claims which are raised by any other participant or any other third party in relation to the payment order or payment concerned.

(d) The making of a compensation offer shall not constitute an admission of liability by the Bank or any other CB in respect of a technical malfunction of TARGET2.

2. Conditions for compensation offers

(a) A payer may submit a claim for an administration fee and interest compensation if, due to a technical malfunction of TARGET2, a payment was not settled on the business day on which it was accepted.

(b) A payee may submit a claim for an administration fee if, due to a technical malfunction of TARGET2, it did not receive a payment that it was expecting to receive on a particular business day. The payee may also submit a claim for interest compensation if one or more of the following conditions are met:

(i) in the case of participants that have access to the marginal lending facility: due to a technical malfunction of TARGET2, a payee had recourse to the marginal lending facility; and/or

(ii) in the case of all participants: it was technically impossible to have recourse to the money market or such refinancing was impossible on other, objectively reasonable grounds.

3. Calculation of compensation

(a) With respect to a compensation offer for a payer:

(i) the administration fee shall be EUR 50 for the first non-settled payment order, EUR 25 for each of the next four such payment orders and EUR 12.50 for each further such payment order. The administration fee shall be calculated separately in relation to each payee;

(ii) interest compensation shall be determined by applying a reference rate to be fixed from day to day. This reference rate shall be the lower of the euro overnight index average (EONIA) rate and the marginal lending rate. The reference rate shall be applied to the amount of the payment order not settled as a result of the technical malfunction of TARGET2 for each day in the period from the date of the actual or, in relation to payment orders referred to in paragraph 2(b)(ii), intended submission of the payment order until the date on which the payment order was or could have been successfully settled. Any interest or charges resulting from the placing of any non-settled payment orders on deposit with the Eurosystem shall be deducted from or charged to the amount of any compensation, as the case may be;

(iii) no interest compensation shall be payable if and in so far as funds resulting from non-settled payment orders were placed in the market or used to fulfil minimum reserve requirements.

(b) With respect to a compensation offer for a payee:

(i) the administration fee shall be EUR 50 for the first non-settled payment order, EUR 25 for each of the next four such payment orders and EUR 12.50 for each further such payment order. The administration fee shall be calculated separately in relation to each payer;

(ii) the method set out in subparagraph (a)(ii) for calculating interest compensation shall apply except that interest compensation shall be payable at a rate equal to the difference between the marginal lending rate and the reference rate, and shall be calculated on the amount of any recourse to the marginal lending facility occurring as a result of the technical malfunction of TARGET2.

4. Procedural rules

a) A claim for compensation shall be submitted on the claim form available in English on the website of the Bank (www.bundesbank.de). Payers shall submit a separate claim form in respect of each payee and payees shall submit a separate claim form in respect of each payer. Sufficient additional information and documents shall be provided to support the information

indicated in the claim form. Only one claim may be submitted in relation to a specific payment or payment order.

(b) Participants shall submit their claim form(s) to the Bank within four weeks of a technical malfunction of TARGET2. Any additional information and evidence requested by the Bank shall be supplied within two weeks of such request being made.

(c) The Bank shall review the claims and forward them to the ECB. Unless otherwise decided by the ECB's Governing Council and communicated to the participants, all received claims shall be assessed no later than 14 weeks after the technical malfunction of TARGET2 occurs.

(d) The Bank shall communicate the result of the assessment referred to in subparagraph (c) to the relevant participants. If the assessment entails a compensation offer, the participants concerned shall, within four weeks of the communication of such offer, either accept or reject it, in respect of each payment or payment order comprised within each claim, by signing a standard letter of acceptance in the form available on the website of the Bank (see www.bundesbank.de). If such letter has not been received by the Bank within four weeks, the participants concerned shall be deemed to have rejected the compensation offer.

(e) The Bank shall make compensation payments on receipt of a participant's letter of acceptance of compensation. No interest shall be payable on any compensation payment.

TERMS OF REFERENCE FOR CAPACITY AND COUNTRY OPINIONS

Terms of reference for capacity opinions for participants in TARGET2

Addressee:
Deutsche Bundesbank
Wilhelm-Epstein-Strasse 14
60431 Frankfurt am Main
Germany

Participation in TARGET2-BBk

[location], [date]

Dear Sir or Madam

We have been asked to provide this Opinion as [in-house or external] legal advisers to [specify name of Participant or branch of Participant] in respect of issues arising under the laws of [jurisdiction in which the Participant is established; hereinafter the 'jurisdiction'] in connection with the participation of [specify name of Participant] (hereinafter the 'Participant') in the TARGET2-BBk component system] (hereinafter the 'System').

This Opinion is confined to the laws of [jurisdiction] as they exist on the date of this Opinion. We have made no investigation of the laws of any other jurisdiction as a basis for this Opinion, and do not express or imply any opinion in this regard. Each of the statements and opinions presented below applies with equal accuracy and validity under the laws of [jurisdiction], whether or not the Participant acts through its head office or one or more branches established inside or outside of [jurisdiction] (hereinafter the 'State') in submitting payment orders and receiving payments.

I. DOCUMENTS EXAMINED

For the purposes of this Opinion, we have examined:

(1) a certified copy of the [specify relevant article(s) of incorporation] of the Participant such as is/are in effect on the date hereof;

(2) [if applicable] an extract from the [specify relevant company register] and [if applicable] [register of credit institutions or analogous register];

(3) [if applicable] a copy of the Participant's licence or other proof of authorisation to provide banking, investment, funds transfer or other financial services in (jurisdiction);

(4) [if applicable] a copy of a resolution adopted by the board of directors or the relevant governing body of the Participant on [insert date], [insert year], evidencing the Participant's agreement to adhere to the System Documents, as defined below; and

(5) [specify all powers of attorney and other documents constituting or evidencing the requisite power of the person or persons accepting the relevant System Documents (as defined below) on behalf of the Participant];

and all other documents relating to the Participant's constitution, powers, and authorisations necessary or appropriate for the provision of this Opinion (hereinafter the 'Participant Documents').

For the purposes of this Opinion, we have also examined:

(1) The "SPECIAL TERMS AND CONDITIONS FOR THE OPENING AND OPERATION OF A PM ACCOUNT IN TARGET2-BUNDESBANK (TARGET2-BBk) USING THE INTERNET-BASED ACCESS" of [insert date] (hereinafter the "Rules") and

(2) […].

The Rules and the […] shall be referred to hereinafter as the 'System Documents' (and collectively with the Participant Documents as the 'Documents').

II. ASSUMPTIONS

For the purposes of this Opinion we have assumed in relation to the Documents that:

(1) the System Documents with which we have been provided are originals or true copies;

(2) the terms of the System Documents and the rights and obligations created by them are valid and legally binding under the laws of Germany, by which they are expressed to be governed, and the choice of the laws of Germany to govern the System Documents is recognised by the laws of Germany.

(3) the Participant Documents are within the capacity and power of and have been validly authorised, adopted or executed and, where necessary, delivered by the relevant parties; and

(4) the Participant Documents are binding on the parties to which they are addressed, and there has been no breach of any of their terms.

III. OPINIONS REGARDING THE PARTICIPANT

A. The Participant is a corporation duly established and registered or otherwise duly incorporated or organised under the laws of [jurisdiction].

B. The Participant has all the requisite corporate powers to execute and perform the rights and obligations under the System Documents to which it is party.

C. The adoption or execution and the performance by the Participant of the rights and obligations under the System Documents to which the Participant is party will not in any way breach any provision of the laws or regulations of [jurisdiction] applicable to the Participant or the Participant Documents.

D. No additional authorisations, approvals, consents, filings, registrations, notarisations or other certifications of or with any court or governmental, judicial or public authority that is competent in [jurisdiction] are required by the Participant in connection with the adoption, validity or enforceability of any of the System Documents or the execution or performance of the rights and obligations thereunder.

E. The Participant has taken all necessary corporate action and other steps necessary under the laws of [jurisdiction] to ensure that its obligations under the System Documents are legal, valid and binding

This Opinion is stated as of its date and is addressed solely to the Bundesbank and the [Participant]. No other persons may rely on this Opinion, and the contents of this Opinion may not be disclosed to persons other than its intended recipients and their legal counsel without our prior written consent, with the exception of the European Central Bank and the national central banks of the European System of Central Banks [and [the national central bank/relevant regulatory authorities] of [jurisdiction]].

Yours faithfully

[signature]

Terms of reference for country opinions for non-EEA participants in TARGET2

Addressee:
Deutsche Bundesbank
Wilhelm-Epstein-Strasse 14
60431 Frankfurt am Main
Germany

TARGET2-BBk

[location], [date]

Dear Sir or Madam

We have been asked as [external] legal advisers to [specify name of Participant or branch of Participant] (the 'Participant') in respect of issues arising under the laws of [jurisdiction in which the Participant is established; hereinafter the 'jurisdiction'] to provide this Opinion under the laws of [jurisdiction] in connection with the participation of the Participant in a system which is a component of TARGET2 (hereinafter the 'System'). References herein to the laws of [jurisdiction] include all applicable regulations of [jurisdiction]. We express an opinion herein under the law of [jurisdiction], with particular regard to the Participant established outside the Federal Republic of Germany in relation to rights and obligations arising from participation in the System, as presented in the System Documents defined below.

This Opinion is confined to the laws of [jurisdiction] as they exist on the date of this Opinion. We have made no investigation of the laws of any other jurisdiction as a basis for this Opinion, and do not express or imply any opinion in this regard. We have assumed that there is nothing in the laws of another jurisdiction which affects this Opinion.

1. DOCUMENTS EXAMINED

For the purposes of this Opinion, we have examined the documents listed below and such other documents as we have deemed necessary or appropriate:

(1) The "SPECIAL TERMS AND CONDITIONS FOR THE OPENING AND OPERATION OF A PM ACCOUNT IN TARGET2-BUNDESBANK (TARGET2-BBk) USING THE INTERNET-BASED ACCESS" of [insert date] (hereinafter the "Rules") and

(2) any other document governing the System and/or the relationship between the Participant and other participants in the System, and between the participants in the System and the Bank.

The Rules and the […] shall be referred to hereinafter as the 'System Documents'.

2. ASSUMPTIONS

For the purposes of this Opinion we have assumed in relation to the System Documents that:

(1) the System Documents are within the capacity and power of and have been validly authorised, adopted or executed and, where necessary, delivered by the relevant parties;

(2) the terms of the System Documents and the rights and obligations created by them are valid and legally binding under the laws of Germany, by which they are expressed to be governed, and the choice of the laws of Germany to govern the System Documents is recognised by the laws of Germany.

(3) the participants in the System through which any payment orders are sent or payments are received, or through which any rights or obligations under the System Documents are executed or performed, are licensed to provide funds transfer services, in all relevant jurisdictions; and

(4) the documents submitted to us in copy or as specimens conform to the originals.

3. OPINION

Based on and subject to the foregoing, and subject in each case to the points set out below, we are of the opinion that:

3.1 Country-specific legal aspects [to the extent applicable]

The following characteristics of the legislation of [jurisdiction] are consistent with and in no way contradict the obligations of the Participant arising out of the System Documents: [list of country-specific legal aspects].

3.2 General insolvency and crisis management issues

3.2.a Types of insolvency and crisis management proceedings

The only types of insolvency proceedings (including composition or rehabilitation) which, for the purpose of this Opinion, shall include all proceedings in respect of the Participant's assets or any branch it may have in [jurisdiction] to which the Participant may become subject in [jurisdiction], are the following: [list proceedings in original language and English translation] (together collectively referred to as 'Insolvency Proceedings').

In addition to Insolvency Proceedings, the Participant, any of its assets, or any branch it may have in [jurisdiction] may become subject in [jurisdiction] to [list any applicable moratorium, receivership, or any other proceedings as a result of which payments to and/or from the Participant may be suspended, or limitations can be imposed in relation to such payments, or similar proceedings, including crisis prevention and crisis management measures equivalent to those defined in Directive 2014/59/EU, in original language and English translation] (hereinafter collectively referred to as 'Proceedings').

3.2.b Insolvency treaties

[jurisdiction] or certain political subdivisions within [jurisdiction], as specified, is/are party to the following insolvency treaties: [specify, if applicable which have or may have an impact on this Opinion].

3.3 Enforceability of System Documents

Subject to the points set out below, all provisions of the System Documents will be binding and enforceable in accordance with their terms under the laws of [jurisdiction], in particular in the event of the opening of any Insolvency Proceedings or Proceedings with respect to the Participant.

In particular, we are of the opinion that:

3.3.a Processing of payment orders

The provisions on processing of payment orders [list of sections] of the Rules are valid and enforceable. In particular, all payment orders processed pursuant to such sections will be valid, binding and will be enforceable under the laws of [jurisdiction]. The provision of the Rules which specifies the precise point in time at which payment orders submitted by the Participant to the System become enforceable and irrevocable (Article 21 of the Rules) is valid, binding and enforceable under the laws of [jurisdiction].

3.3.b Authority of the Bank to perform its functions

The opening of Insolvency Proceedings or Proceedings against the Participant will not affect the authority and powers of the Bank arising out of the System Documents. [Specify [to the extent applicable] that: the same opinion is also applicable in respect of any other entity which provides the Participants with services directly and necessarily required for participating in the System (eg network service provider)].

3.3.c Remedies in the event of default

[Where applicable to the Participant, the provisions contained in Article 31 of the Rules regarding accelerated performance of claims which have not yet matured, the set-off of claims for using the deposits of the Participant, the enforcement of a pledge, suspension and termination of participation, claims for default interest, and termination of agreements and transactions (Articles 28-32 of the Rules) are valid and enforceable under the laws of [jurisdiction].]

3.3.d Suspension and termination

Where applicable to the Participant, the provisions contained in Articles 28 and 29 of the Rules (in respect of suspension and termination of the Participant's participation in the System on the opening of Insolvency Proceedings or Proceedings or other events of default, as defined in the System Documents, or if the Participant represents any kind of systemic risk or has serious operational problems) are valid and enforceable under the laws of [jurisdiction].

3.3.e Assignment of rights and obligations

The rights and obligations of the Participant cannot be assigned, altered or otherwise transferred by the Participant to third parties without the prior written consent of the Bank.

3.3.f Choice of governing law and jurisdiction

The provisions contained in Articles 35 and 38 of the Rules, and in particular in respect of the governing law, the resolution of a dispute, competent courts, and service of process are valid and enforceable under the laws of [jurisdiction].

3.4 Voidable preferences

We are of the opinion that no obligation arising out of the System Documents, the performance thereof, or compliance therewith prior to the opening of any Insolvency Proceedings or Proceedings in respect of the Participant may be set aside in any such proceedings as a preference, voidable transaction or otherwise under the laws of [jurisdiction].

In particular, and without limitation to the foregoing, we express this opinion in respect of any payment orders submitted by any participant in the System. In particular, we are of the opinion that the provisions of Article 21 of the Rules establishing the enforceability and irrevocability of payment orders will be valid and enforceable and that a payment order submitted by any participant and processed pursuant to Title IV of the Rules may not be set aside in any Insolvency Proceedings or Proceedings as a preference, voidable transaction or otherwise under the laws of [jurisdiction].

3.5 Attachment

If a creditor of the Participant seeks an attachment order (including any freezing order, order for seizure or any other public or private law procedure that is intended to protect the public interest or the rights of the Participant's creditors) - hereinafter referred to as an 'Attachment' - under the laws of [jurisdiction] from a court or governmental, judicial or public authority that is competent in [jurisdiction], we are of the opinion that [insert the analysis and discussion].

3.6 Collateral [if applicable]

3.6.a Assignment of rights or deposit of assets for collateral purposes, pledge, repo and/or guarantee

Assignments for collateral purposes will be valid and enforceable under the laws of [jurisdiction]. Specifically, the creation and enforcement of a pledge or repo under the Rules of TARGET2-BBk will be valid and enforceable under the laws of [jurisdiction].

3.6.b Priority of assignees', pledgees' or repo purchasers' interest over that of other claimants

In the event of Insolvency Proceedings or Proceedings in respect of the Participant, the rights or assets assigned for collateral purposes, or pledged by the Participant in favour of the Bank or other participants in the System, will rank in priority of payment above the claims of all other creditors of the Participant and will not be subject to priority or preferential creditors.

3.6.c Enforcing title to security

Even in the event of Insolvency Proceedings or Proceedings in respect of the Participant, other participants in the System and the Bank as [assignees, pledgees or repo purchasers as applicable] will still be free to enforce and collect the Participant's rights or assets through the action of the Bank pursuant to the Rules.

3.6.d Form and registration requirements

There are no form requirements for the assignment for collateral purposes of, or the creation and enforcement of a pledge or repo over the Participant's rights or assets and it is not necessary for the [assignment for collateral purposes, pledge or repo, as applicable], or any particulars of such [assignment, pledge or repo, as applicable] to be registered or filed with any court or governmental, judicial or public authority that is competent in [jurisdiction].

3.7 Branches [to the extent applicable]

3.7.a Applicability of Opinion to action through branches

Each of the statements and opinions presented above with regard to the Participant applies with equal accuracy and validity under the laws of [jurisdiction] in situations where the Participant acts through one or more of its branches established outside [jurisdiction].

3.7.b Conformity with law

Neither the execution and performance of the rights and obligations under the System Documents nor the submission, transmission or receipt of payment orders by a branch of the Participant will in any respect breach the laws of [jurisdiction].

3.7.c Required authorisations

Neither the execution and performance of the rights and obligations under the System Documents nor the submission, transmission or receipt of payment orders by a branch of a Participant will require any additional authorisations, approvals, consents, filings, registrations, notarisations or other certifications of or with any court or governmental, judicial or public authority that is competent in [jurisdiction].

This Opinion is stated as of its date and is addressed solely to the Bundesbank and the [Participant]. No other persons may rely on this Opinion and the contents of this Opinion may not be disclosed to persons other than its intended recipients and their legal counsel without our prior written consent, with the

exception of the European Central Bank and the national central banks of the European System of Central Banks [and [the national central bank/relevant regulatory authorities] of [jurisdiction]].

Yours faithfully

[signature]

BUSINESS CONTINUITY AND CONTINGENCY PROCEDURES

1. General provisions

(a) This Appendix sets out the arrangements between the Bank and participants, or ancillary systems, if one or more components of the SSP or the telecommunications network fail or are affected by an abnormal external event, or if the failure affects any participant or ancillary system.

b) All references to specific times in this Appendix refer to local time at the seat of the ECB, ie Central European Time (CET).[12].

2. Measures of business continuity and contingency processing

a) In the event that an abnormal external event occurs and/or there is a failure of the SSP or the telecommunications network which affects the normal operation of TARGET2, the Bank shall be entitled to adopt business continuity and contingency processing measures.

b) The following main business continuity and contingency processing measures shall be available in connection with TARGET2:

(i) relocating the operation of the SSP to an alternative site;

(ii) changing the SSP's operating hours; and

(iii) initiating contingency processing of very critical and critical payments, as defined in paragraph 6(c) and (d) respectively.

c) In relation to business continuity and contingency processing measures, the Bank shall have full discretion regarding whether and which measures are adopted to settle payment orders.

3. Incident communication

(a) Information about the failure of the SSP and/or an abnormal external event shall be communicated to participants through the domestic communication channels, the ICM and T2IS. In particular, communications to participants shall include the following information:

(i) a description of the event;

(ii) the anticipated delay in processing (if known);

(iii) information on the measures already taken; and

(iv) the advice to participants.

(b) In addition, the Bank may notify participants of any other existing or anticipated event which has the potential to affect the normal operation of TARGET2.

4. Relocation of the operation of the SSP to an alternative site

[12]The term “CET” takes into account the change-over to Central European Summertime (CEST).

(a) In the event that any of the events referred to in paragraph 2(a) occurs, the operation of the SSP may be relocated to an alternative site, either within the same region or in another region.

(b) In the event that the operation of the SSP is relocated from one region (Region 1) to another region (Region 2), the participants shall endeavour to reconcile their positions up to the point of the failure or the occurrence of the abnormal external events and provide to the Bank all relevant information in this respect.

5. Change of operating hours

(a) The daytime processing of TARGET2 may be extended or the opening time of a new business day may be delayed. During any extended operating time of TARGET2, payment orders shall be processed in accordance with the terms and conditions for the opening and operation of a PM account in TARGET-BBk, subject to the modifications contained in this Appendix.

(b) Daytime processing *may* be extended and the closing time thereby delayed if an SSP failure has occurred during the day but has been resolved before 18.00. Such a closing time delay shall in normal circumstances not exceed two hours and shall be announced to participants as early as possible. If such a delay is announced before 16.50, the minimum period of one hour between the cut-off time for customer and interbank payment orders shall remain in place. Once such a delay has been announced it may not be withdrawn.

(c) The closing time shall be delayed in cases where an SSP failure has occurred before 18:00 and has not been resolved by 18.00. The Bank shall immediately communicate the delay of closing time to participants.

d) Upon recovery of the SSP, the following steps shall take place:

(i) The Bank shall seek to settle all queued payments within one hour; this time is reduced to 30 minutes in the event that the SSP failure occurs at 17.30 or later (in cases where the SSP failure was ongoing at 18.00).

(ii) Participants' final balances shall be established within one hour; this time shall be reduced to 30 minutes in the event that the SSP failure occurs at 17.30 or later, in cases where the SSP failure was ongoing at 18.00.

(iii) At the cut-off time for interbank payments, the end-of-day processing, including recourse to the Eurosystem standing facilities shall likewise take place.

(e) Ancillary systems that require liquidity in the early morning need to have established means to cope with cases where the daytime processing cannot be started in time due to an SSP failure on the previous day.

6. Contingency processing

(a) If the Bank deems it necessary to do so, it shall initiate the contingency processing of payment orders using the Contingency Solution of the SSP. In such cases, only a minimum service level

shall be provided to participants and ancillary systems. The Bank shall inform its participants and ancillary systems of the start of contingency processing by any available means of communication.

(b) In contingency processing, payment orders shall be submitted by the participants not using the internet-based access and authorised by the Bank. In addition, the ancillary systems may submit files containing payment instructions, which may be uploaded into the Contingency Solution by the Bank. (c) The following payments shall be considered 'very critical' and the Bank shall use best efforts to process them in contingency situations:

(i) CLS Bank International-related payments, with the exception of payments related to the CLS CCP and the CLSNow services;

(ii) end-of-day settlement of EURO1; and

(iii) central counterparty margin calls.

(d) Payments required to avoid systemic risk shall be considered as ‘critical’ and the Bank may decide to initiate contingency processing in relation to them.

(e) Participants not using the internet-based access shall submit payment orders for contingency processing directly into the Contingency Solution and information to payees shall be provided through the Contingency Solution. Ancillary systems shall submit files which contain payment instructions to Bank for uploading into the Contingency Solution and which authorise the Bank to do so. The Bank may, exceptionally, also manually input payments on behalf of participants not using the internet-based access. Information concerning account balances and debit and credit entries may be obtained via the Bank.

(f) Payment orders that have already been submitted to TARGET2-BBk, but are queued, may also undergo contingency processing. In such cases, the Bank shall endeavour to avoid the double processing of payment orders, but the participants shall bear the risk of such double processing if it occurs.

(g) For contingency processing of payment orders, participants shall provide eligible assets as collateral. During contingency processing, incoming contingency payments may be used to fund outgoing contingency payments. For the purposes of contingency processing, participants’ available liquidity may not be taken into account by the Bank.

7. Failures linked to participants or ancillary systems

(a) In the event that a participant has a problem that prevents it from settling payments in TARGET2 it shall be its responsibility to resolve the problem. In particular, a participant may use in-house solutions or the ICM functionality, i.e. backup liquidity redistribution payments and backup contingency payments (e.g. CLS, EURO1).

(b) If the measures referred to in subparagraph (a) are exhausted or if they are inefficient, the participant may request support from the Bank.

(c) In the event that a failure affects an ancillary system, that ancillary system shall be responsible for resolving the failure. If the ancillary system so requests, the Bank may act on its behalf. The Bank shall have discretion to decide what support it gives to the ancillary system, including during the night-time operations of the ancillary system. The following contingency measures may be taken:

(i) the ancillary system initiates clean payments (ie payments that are not linked to the underlying transaction) via the Participant Interface (PI);

(ii) the Bank creates and/or processes XML instructions/files on behalf of the ancillary system; and/or

(iii) the Bank makes clean payments on behalf of the ancillary system.

(d) The detailed contingency measures with respect to ancillary systems shall be contained in the bilateral arrangements between the Bank and the relevant ancillary system.

8. Other provisions

(a) In the event that certain data are unavailable because one of the events referred to in paragraph 3(a) has occurred, the Bank is entitled to start or continue processing payment orders and/or operate TARGET2-BBk on the basis of the last available data, as determined by the Bank. If so requested by the Bank, participants and ancillary systems shall resubmit their FileAct/Interact messages or take any other action deemed appropriate by the Bank.

(b) In the event of a failure of the Bank, some or all of its technical functions in relation to TARGET2-BBk may be performed by other Eurosystem CBs or the operational team of the SSP.

(c) The Bank may require that the participants participate in regular or ad hoc testing of business continuity and contingency processing measures, training or any other preventive arrangements, as deemed necessary by the Bank. Any costs incurred by the participants as a result of such testing or other arrangements shall be borne solely by the participants.

OPERATING SCHEDULE

1. TARGET2 is open on all days, except Saturdays, Sundays, New Year's Day, Good Friday and Easter Monday (according to the calendar applicable at the seat of the ECB), 1 May, Christmas Day and 26 December.
2. The reference time for the system is the local time at the seat of the ECB, ie CET.
3. The current business day is opened during the evening of the previous business day and operates to the following schedule:

Time	Description
06.45 - 07.00	Business window to prepare daytime operations *
07.00 - 18.00	Daytime processing
17.00	Cut-off time for customer payments (ie payments where the originator and/or the beneficiary of a payment is not a direct or indirect participant as identified in the system by the use of an MT 103 or MT 103+ message)
18.00	Cut-off time for interbank payments (ie payments other than customer payments)
18.00 – 18.45 **	End-of-day processing
18.15 **	General cut-off time for the use of standing facilities
(Shortly after) 18.30 ***	Data for the update of accounting systems are available to CBs
18.45 - 19.30 ***	Start-of-day processing (new business day)
19.00 ***– 19.30 **	Provision of liquidity on the PM account
19.30 ***	'Start-of-procedure' message and settlement of the standing orders to transfer liquidity from the PM accounts to the sub-account(s)/technical account(s) (ancillary system-related settlement)
19.30 *** - 22.00	Execution of additional liquidity transfers via the ICM for settlement procedure 6 real time; execution of additional liquidity transfers via the ICM before the ancillary system sends the “start of cycle” messages for settlement procedure 6 interfaced; settlement period of night-time ancillary system operations (only for ancillary system settlement procedure 6 real-time and settlement procedure 6 interfaced)

22.00 - 01.00	Technical maintenance period
01.00 - 07.00	Settlement procedure of night-time ancillary system operations (only for ancillary system settlement procedure 6 real-time and settlement procedure 6 interfaced)

* Daytime operations means daytime processing phase and end-of-day processing.

** Ends 15 minutes later on the last day of the reserve maintenance period.

*** Starts 15 minutes later on the last day of the reserve maintenance period.

4. The ICM is available for liquidity transfers from 19.30 *** until 18.00 the next day, except during the technical maintenance period from 22.00 until 1.00.

5. The operating hours may be changed in the event that business continuity measures are adopted in accordance with paragraph 5 of Appendix IV.

6. Up-to-date information on the SSP's operational status shall be available on the TARGET2 Information System (T2IS) on a dedicated webpage on the ECB's website. The information on the SSP's operational status on T2IS and the ECB's website shall only be updated during normal business hours.

FEE SCHEDULE AND INVOICING FOR INTERNET-BASED ACCESS

Fees for direct participants

1. The monthly fee for the processing of payment orders in TARGET2-BBk 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 Bank shall issue and maintain up to five active certificates per participant for each PM account free of charge. The Bank shall charge a fee of EUR 120 for the issuance of a sixth and for each subsequent active certificate. The Bank] shall charge an annual maintenance fee of EUR 30 for the sixth and for each subsequent active certificate. Active certificates shall be valid for five 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 ninth business day of the following month. Payments shall be made no later than the 14th business day of that month to the account specified by the Bank or shall be debited from an account specified by the participant.

REQUIREMENTS REGARDING INFORMATION SECURITY MANAGEMENT AND BUSINESS CONTINUITY MANAGEMENT

Information security management

These requirements are applicable to each participant, unless the participant demonstrates that a specific requirement is not applicable to it. In establishing the scope of application of the requirements within its infrastructure, the participant should identify the elements that are part of the Payment Transaction Chain (PTC). Specifically, the PTC starts at a Point of Entry (PoE), i.e. a system involved in the creation of transactions (e.g. workstations, front-office and back-office applications, middleware), and ends at the system responsible to send the message to SWIFT (e.g. SWIFT VPN Box) or Internet (with the latter applicable to Internet-based Access).

Requirement 1.1: Information security policy

The management shall set a clear policy direction in line with business objectives and demonstrate support for and commitment to information security through the issuance, approval and maintenance of an information security policy aiming at managing information security and cyber resilience across the organisation in terms of identification, assessment and treatment of information security and cyber resilience risks. The policy should contain at least the following sections: objectives, scope (including domains such as organisation, human resources, asset management etc.), principles and allocation of responsibilities.

Requirement 1.2: Internal organisation

An information security framework shall be established to implement the information security policy within the organisation. The management shall coordinate and review the establishment of the information security framework to ensure the implementation of the information security policy (as per Requirement 1.1) across the organisation, including the allocation of sufficient resources and assignment of security responsibilities for this purpose.

Requirement 1.3: External parties

The security of the organisation's information and information processing facilities should not be reduced by the introduction of, and/or the dependence on, an external party/parties or products/services provided by them. Any access to the organisation's information processing facilities by external parties shall be controlled. When external parties or products/services of external parties are required to access the organisation's information processing facilities, a risk assessment shall be carried out to determine the security implications and control requirements. Controls shall be agreed and defined in an agreement with each relevant external party.

Requirement 1.4: Asset management

All information assets, the business processes and the underlying information systems, such as operating systems, infrastructures, business applications, off-the-shelf products, services and user-developed applications, in the scope of the Payment Transaction Chain shall be accounted for and have a nominated owner. The responsibility for the maintenance and the operation of appropriate controls in the business processes and the related IT components to safeguard the information assets shall be assigned. Note: the owner can delegate the implementation of specific controls as appropriate, but remains accountable for the proper protection of the assets.

Requirement 1.5: Information assets classification
Information assets shall be classified in terms of their criticality to the smooth delivery of the service by the participant. The classification shall indicate the need, priorities and degree of protection required when handling the information asset in the relevant business processes and shall also take into consideration the underlying IT components. An information asset classification scheme approved by the management shall be used to define an appropriate set of protection controls throughout the information asset lifecycle (including removal and destruction of information assets) and to communicate the need for specific handling measures.

Requirement 1.6: Human resources security
Security responsibilities shall be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third party users shall be adequately screened, especially for sensitive jobs. Employees, contractors and third party users of information processing facilities shall sign an agreement on their security roles and responsibilities. An adequate level of awareness shall be ensured among all employees, contractors and third party users, and education and training in security procedures and the correct use of information processing facilities shall be provided to them to minimise possible security risks. A formal disciplinary process for handling security breaches shall be established for employees. Responsibilities shall be in place to ensure that an employee's, contractor's or third party user's exit from or transfer within the organisation is managed, and that the return of all equipment and the removal of all access rights are completed.

Requirement 1.7: Physical and environmental security
Critical or sensitive information processing facilities shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They shall be physically protected from unauthorised access, damage and interference. Access shall be granted only to individuals who fall within the scope of Requirement 1.6. Procedures and standards shall be established to protect physical media containing information assets when in transit.
Equipment shall be protected from physical and environmental threats. Protection of equipment (including equipment used off-site) and against the removal of property is necessary to reduce the risk of unauthorised access to information and to guard against loss or damage of equipment or

information. Special measures may be required to protect against physical threats and to safeguard supporting facilities such as the electrical supply and cabling infrastructure.

Requirement 1.8: Operations management

Responsibilities and procedures shall be established for the management and operation of information processing facilities covering all the underlying systems in the Payment Transaction Chain end-to-end. As regards operating procedures, including technical administration of IT systems, segregation of duties shall be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse. Where segregation of duties cannot be implemented due to documented objective reasons, compensatory controls shall be implemented following a formal risk analysis. Controls shall be established to prevent and detect the introduction of malicious code for systems in the Payment Transaction Chain. Controls shall be also established (including user awareness) to prevent, detect and remove malicious code. Mobile code shall be used only from trusted sources (e.g. signed Microsoft COM components and Java Applets). The configuration of the browser (e.g. the use of extensions and plugins) shall be strictly controlled.

Data backup and recovery policies shall be implemented by the management; those recovery policies shall include a plan of the restoration process which is tested at regular intervals at least annually. Systems that are critical for the security of payments shall be monitored and events relevant to information security shall be recorded. Operator logs shall be used to ensure that information system problems are identified. Operator logs shall be regularly reviewed on a sample basis, based on the criticality of the operations. System monitoring shall be used to check the effectiveness of controls which are identified as critical for the security of payments and to verify conformity to an access policy model.

Exchanges of information between organisations shall be based on a formal exchange policy, carried out in line with exchange agreements among the involved parties and shall be compliant with any relevant legislation. Third party software components employed in the exchange of information with TARGET2 (like software received from a Service Bureau in scenario 2 of the scope section of the TARGET2 self-certification arrangement document) must be used under a formal agreement with the third-party.

Requirement 1.9: Access control

Access to information assets shall be justified on the basis of business requirements (need-to-know[1]) and according to the established framework of corporate policies (including the information security policy). Clear access control rules shall be defined based on the principle of least privilege[2] to reflect closely the needs of the corresponding business and IT processes. Where relevant, (e.g. for backup

[1] The need-to-know principle refers to the identification of the set of information that an individual needs access to in order to carry out her/his duties.

[2] The principle of least privilege refers to tailoring a subject's access profile to an IT system in order to match the corresponding business role.

management) logical access control should be consistent with physical access control unless there are adequate compensatory controls in place (e.g. encryption, personal data anonymisation).
Formal and documented procedures shall be in place to control the allocation of access rights to information systems and services that fall within the scope of the Payment Transaction Chain. The procedures shall cover all stages in the lifecycle of user access, from the initial registration of new users to the final deregistration of users that no longer require access.
Special attention shall be given, where appropriate, to the allocation of access rights of such criticality that the abuse of those access rights could lead to a severe adverse impact on the operations of the participant (e.g. access rights allowing system administration, override of system controls, direct access to business data).
Appropriate controls shall be put in place to identify, authenticate and authorise users at specific points in the organisation's network, e.g. for local and remote access to systems in the Payment Transaction Chain. Personal accounts shall not be shared in order to ensure accountability.
For passwords, rules shall be established and enforced by specific controls to ensure that passwords cannot be easily guessed, e.g. complexity rules and limited-time validity. A safe password recovery and/or reset protocol shall be established.
A policy shall be developed and implemented on the use of cryptographic controls to protect the confidentiality, authenticity and integrity of information. A key management policy shall be established to support the use of cryptographic controls.
There shall be policy for viewing confidential information on screen or in print (e.g. a clear screen, a clear desk policy) to reduce the risk of unauthorised access.
When working remotely, the risks of working in an unprotected environment shall be considered and appropriate technical and organisational controls shall be applied.

Requirement 1.10: Information systems acquisition, development and maintenance
Security requirements shall be identified and agreed prior to the development and/or implementation of information systems.
Appropriate controls shall be built into applications, including user-developed applications, to ensure correct processing. These controls shall include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls shall be determined on the basis of security requirements and risk assessment according to the established policies (e.g. information security policy, cryptographic control policy).
The operational requirements of new systems shall be established, documented and tested prior to their acceptance and use. As regards network security, appropriate controls, including segmentation and secure management, should be implemented based on the criticality of data flows and the level of risk of the network zones in the organisation. There shall be specific controls to protect sensitive information passing over public networks.

Access to system files and program source code shall be controlled and IT projects and support activities conducted in a secure manner. Care shall be taken to avoid exposure of sensitive data in test environments. Project and support environments shall be strictly controlled. Deployment of changes in production shall be strictly controlled. A risk assessment of the major changes to be deployed in production shall be conducted.
Regular security testing activities of systems in production shall also be conducted according to a predefined plan based on the outcome of a risk-assessment, and security testing shall include, at least, vulnerability assessments. All of the shortcomings highlighted during the security testing activities shall be assessed and action plans to close any identified gap shall be prepared and followed-up in a timely fashion.

Requirement 1.11: Information security in supplier[3] relationships
To ensure protection of the participant's internal information systems that are accessible by suppliers, information security requirements for mitigating the risks associated with supplier's access shall be documented and formally agreed upon with the supplier.

Requirement 1.12: Management of information security incidents and improvements
To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses, roles, responsibilities and procedures, at business and technical level, shall be established and tested to ensure a quick, effective and orderly and safely recover from information security incidents including scenarios related to a cyber-related cause (e.g. a fraud pursued by an external attacker or by an insider). Personnel involved in these procedures shall be adequately trained.

Requirement 1.13: Technical compliance review
A participant's internal information systems (e.g. back office systems, internal networks and external network connectivity) shall be regularly assessed for compliance with the organisation's established framework of policies (e.g. information security policy, cryptographic control policy).

Requirement 1.14: Virtualisation
Guest virtual machines shall comply with all the security controls that are set for physical hardware and systems (e.g. hardening, logging). Controls relating to hypervisors must include: hardening of the hypervisor and the hosting operating system, regular patching, strict separation of different environments (e.g. production and development). Centralised management, logging and monitoring as well as managing of access rights, in particular for high privileged accounts, shall be implemented

[3] A supplier in the context of this exercise should be understood as any third party (and its personnel) which is under contract (agreement), with the institution, to provide a service and under the service agreement the third party (and its personnel) is granted access, either remotely or on site, to information and/or information systems and/or information processing facilities of the institution in scope or associated to the scope covered under the exercise of the TARGET2 self-certification.

based on a risk assessment. Guest virtual machines managed by the same hypervisor shall have a similar risk profile.

Requirement 1.15: Cloud computing
The usage of public and/or hybrid cloud solutions in the Payment Transaction Chain must be based on a formal risk assessment, taking into account the technical controls and the contractual clauses related to the cloud solution.
If hybrid cloud solutions are used, it is understood that the criticality level of the overall system is the highest one of the connected systems. All on-premises components of the hybrid solutions must be segregated from the other on-premises systems.

Business continuity management (applicable only to critical participants)
The following requirements (2.1 to 2.6) relate to business continuity management. Each TARGET2 participant classified by the Eurosystem as being critical for the smooth functioning of the TARGET2 system shall have a business continuity strategy in place comprising the following elements.

Requirement 2.1: Business continuity plans shall be developed and procedures for maintaining them are in place.

Requirement 2.2: An alternate operational site shall be available.

Requirement 2.3: The risk profile of the alternate site shall be different from that of the primary site, in order to avoid that both sites are affected by the same event at the same time. For example, the alternate site shall be on a different power grid and central telecommunication circuit from those of the primary business location.

Requirement 2.4: In the event of a major operational disruption rendering the primary site inaccessible and/or critical staff unavailable, the critical participant shall be able to resume normal operations from the alternate site, where it shall be possible to properly close the business day and open the following business day(s).

Requirement 2.5: Procedures shall be in place to ensure that the processing of transactions is resumed from the alternate site within a reasonable timeframe after the initial disruption of service and commensurate to the criticality of the business that was disrupted.

Requirement 2.6: The ability to cope with operational disruptions shall be tested at least once a year and critical staff shall be aptly trained. The maximum period between tests shall not exceed one year.'.