DANMARKS NATIONALBANK

Appendices to the Terms and Conditions for Accounts in TARGET DKK

Appendix 1 – Technical specifications for the processing of cash transfer orders **2**

Appendix 2 – Business continuity and contingency procedures **9**

Appendix 3 – TARGET DKK operating schedule **13**

Appendix 4 – Coverage of Danmarks Nationalbank's costs for TARGET DKK and pricing model for TARGET Services **16**

Appendix 5 – Requirements for information security management and business continuity management in TARGET DKK **21**

Appendix 6 – Definitions **26**

Effective as of 22 April 2025

Appendix 1 – Technical specifications for the processing of cash transfer orders

In addition to the Terms and Conditions, the following rules apply to the processing of cash transfer orders:

1. Testing requirements for participation in TARGET DKK

Each participant must pass a series of tests to verify their technical and operational capabilities in order to participate in TARGET DKK.

2. Account numbers

Each participant's account shall be identified by a unique account number of up to 34 characters made up of five sections as follows:

Name	No. of characters	Contents

Account type	1	M = MCA
		R = RTGS DCA
		C = T2S DCA
		I = TIPS DCA
		T = RTGS AS technical account
		U = RTGS sub-account
		X = Contingency procedure account

Country code of central bank	2	ISO Country code: 3166-1
Currency code	3	DKK
BIC	11	Account holder's party BIC
Account name	Max. 17	Free text (must begin with three-character AS code)

3. Messaging rules in TARGET Services

a. Each participant shall comply with the message structure and field specifications, as defined in Part 3 of the relevant User Detailed Functional Specifications (UDFS).

b. Business application headers must be attached to all message types processed on MCAs, RTGS DCAs (including sub-accounts), RTGS AS technical accounts and T2S DCAs as listed below. If several messages are sent together as a file, a business file header must also be used.

Message Type	Description
head.001	Business application header
head.002	Business file header

4. Message types processed in TARGET Services

a. The following message types are processed on MCAs:

Message Type	Description
Administration (admi)	
admi.004	SystemEventNotification
admi.005	ReportQueryRequest
admi.007	ReceiptAcknowledgement

Cash Management (camt)	
camt.003	GetAccount
camt.004	ReturnAccount
camt.005	GetTransaction
camt.006	ReturnTransaction
camt.018	GetBusinessDayInformation
camt.019	ReturnBusinessDayInformation
camt.025	Receipt
camt.046	GetReservation
camt.047	ReturnReservation
camt.048	ModifyReservation
camt.049	DeleteReservation
camt.050	LiquidityCreditTransfer
camt.053	BankToCustomerStatement
camt.054	BankToCustomerDebitCreditNotification
Payment Clearing and Settlement (pacs)	
pacs.009	FinancialInstitutionCreditTransfer
pacs.010	FinancialInstitutionDirectDebit

b. The following message types are processed on RTGS DCAs and RTGS AS technical accounts, where applicable:

Administration (admi)	
admi.004	SystemEventNotification
admi.005	ReportQueryRequest
admi.007	ReceiptAcknowledgement
Cash Management (camt)	
camt.003	GetAccount
camt.004	ReturnAccount
camt.005	GetTransaction
camt.006	ReturnTransaction
camt.007	ModifyTransaction
camt.009	GetLimit
camt.010	ReturnLimit
camt.011	ModifyLimit
camt.012	DeleteLimit
camt.018	GetBusinessDayInformation
camt.019	ReturnBusinessDayInformation
camt.021	ReturnGeneralBusinessInformation
camt.025	Receipt
camt.029	ResolutionOfInvestigation
camt.046	GetReservation
camt.047	ReturnReservation
camt.048	ModifyReservation
camt.049	DeleteReservation
camt.050	LiquidityCreditTransfer

camt.053	BankToCustomerStatement
camt.054	BankToCustomerDebitCreditNotification
camt.056	FIToFIPaymentCancellationRequest
camt.077	BillingReport
Payment Clearing and Settlement (pacs)	
pacs.002	PaymentStatusReport
pacs.004	PaymentReturn
pacs.008	CustomerCreditTransfer
pacs.009	FinancialInstitutionCreditTransfer
pacs.010	FinancialInstitutionDirectDebit
Payment Initiation (pain)	
pain.998	ASInitiationStatus
pain.998	ASTransferNotice
pain.998	ASTransferInitiation
Account Management (acmt)	
Acmt.025	AccountQueryList
Acmt.026	AccountListReport

c. The following message types are processed on T2S DCAs:

Message Type	**Description**
Administration (admi)	
admi.005	ReportQueryRequest
admi.006	ResendRequestSystemEventNotification
admi.007	ReceiptAcknowledgement
Cash Management (camt)	
camt.003	GetAccount
camt.004	ReturnAccount
camt.005	GetTransaction
camt.006	ReturnTransaction
camt.009	GetLimit
camt.010	ReturnLimit
camt.011	ModifyLimit
camt.012	DeleteLimit
camt.018	GetBusinessDayInformation
camt.019	ReturnBusinessDayInformation
camt.024	ModifyStandingOrder
camt.025	Receipt
camt.050	LiquidityCreditTransfer
camt.051	LiquidityDebitTransfer
camt.052	BankToCustomerAccountReport
camt.053	BankToCustomerStatement
camt.054	BankToCustomerDebitCreditNotification
camt.064	LimitUtilisationJournalQuery

camt.065	LimitUtilisationJournalReport
camt.066	IntraBalanceMovementInstruction
camt.067	IntraBalanceMovementStatusAdvice
camt.068	IntraBalanceMovementConfirmation
camt.069	GetStandingOrder
camt.070	ReturnStandingOrder
camt.071	DeleteStandingOrder
camt.072	IntraBalanceMovementModificationRequest
camt.073	IntraBalanceMovementModificationRequestStatusAdvice
camt.074	IntraBalanceMovementCancellationRequest
camt.075	IntraBalanceMovementCancellationRequestStatusAdvice
camt.077	BillingReport
camt.078	IntraBalanceMovementQuery
camt.079	IntraBalanceMovementQueryResponse
camt.080	IntraBalanceModificationQuery
camt.081	IntraBalanceModificationReport
camt.082	IntraBalanceCancellationQuery
camt.083	IntraBalanceCancellationReport
camt.084	IntraBalanceMovementPostingReport
camt.085	IntraBalanceMovementPendingReport

d. The following message types are processed on TIPS DCAs:

Message Type	**Description**
Payment Clearing and Settlement (pacs)	
pacs.002	FIToFIPayment Status Report
pacs.004	PaymentReturn
pacs.008	FIToFICustomerCreditTransfer
pacs.028	FIToFIPaymentStatusRequest
Cash Management (camt)	
camt.003	GetAccount
camt.004	ReturnAccount
camt.005	GetTransaction
camt.006	ReturnTransaction
camt.011	ModifyLimit
camt.019	ReturnBusinessDayInformation
camt.025	Receipt
camt.029	ResolutionOfInvestigation
camt.050	LiquidityCreditTransfer
camt.052	BankToCustomerAccountReport
camt.053	BankToCustomerStatement
camt.054	BankToCustomerDebitCreditNotification
camt.056	FIToFIPaymentCancellationRequest
camt.077	BillingReport

Account Management (acmt)	
acmt.010	AccountRequestAcknowledgement
acmt.011	AccountRequestRejection
acmt.015	AccountExcludedMandateMaintenanceRequest
Reference data (reda)	
reda.016	PartyStatusAdviceV01
reda.022	PartyModificationRequestV01

5. Double-entry control
All cash transfer orders shall pass a double-entry control, the aim of which is to return orders that have been submitted more than once (duplicated cash transfer orders). Details can be found in Part 1, Section 3, of the relevant UDFS.

6. Validation rules and error codes
Message validation is performed in accordance with the High Value Payments Plus (HVPS+) guidelines for message validation specified by the ISO 20022 standard and the validations specific to TARGET Services. The detailed validation rules and error codes are described in the respective parts of the UDFS as follows:

a. for MCAs, Chapter 14 of the CLM UDFS

b. for RTGS DCAs, Chapter 13 in RTGS UDFS

c. for T2S DCAs, Chapter 4.1 of T2S UDFS

d. For TIPS DCAs, Chapter 4 of TIPS UDFS.

7. Predetermined settlement times and events
RTGS DCAs

a. For payment orders using the Earliest Debit Time Indicator, the message element'/FromTime/' shall be used.

b. For payment orders using the Latest Debit Time Indicator, two options shall be available.

   i. Message element 'RejectTime': If the payment order cannot be settled within the specified debit time, the order will be rejected.

   ii. Message element 'TillTime': If the payment order cannot be settled within the specified debit time, the order is not rejected but remains in the relevant queue.

In both cases, a notification is automatically sent via the GUI if a payment order with Latest Debit Time Indicator has not been settled 15 minutes prior to the time specified therein.

T2S DCAs

a. For immediate liquidity transfer orders, no specific XML tag is required.

b. Predefined liquidity transfer orders and standing liquidity transfer orders may be triggered by a specific time or event on the day of settlement:

   i. for settlement at a specified time, the 'XML tag Time(/ExctnTp/Tm/)' is used;

   ii. for settlement upon occurrence of a specific event, the XML tag '(EventType/ExctnTp/Evt/)' shall be used;

c. The validity period for standing liquidity transfer orders is indicated with the following XML tags: 'FromDate/VldtyPrd/FrDt/' and 'ToDate/VldtyPrd/ToDt/'.

8. Offsetting of cash transfer orders on RTGS DCAs
Offsetting checks and, if appropriate, extended offsetting checks (both terms as defined in paragraphs (a) and (b)) shall be carried out on cash transfer orders to facilitate the smooth settlement.

a. an offsetting check shall determine whether the payee's cash transfer orders that are at the front of the prioritised urgent queue or, if not applicable, the high priority queue, are available for offsetting against the payer's cash transfer order (hereinafter: ‘offsetting cash transfer orders’). If an offsetting cash transfer order does not provide sufficient funds for the respective payer’s cash transfer order it shall be determined whether there is sufficient available liquidity on the payer’s RTGS DCA.

b. if the offsetting check is unsuccessful, Danmarks Nationalbank may apply the extended offsetting check. An extended offsetting check determines whether offsetting cash transfer orders are available in any of the payee’s queues regardless of when they joined the queue. However, if there are cash transfer orders to other participants with higher priority, the FIFO (first-in-first-out) principle may only be used if the settlement of such an offsetting cash transfer order would result in a liquidity increase for the payee.

9. Optimisation algorithms on RTGS DCAs and sub-accounts
Four algorithms shall be applied to facilitate the smooth settlement of payment flows. Further information is available in the RTGS UDFS Part 2.

a. Under the ‘partial optimisation’ algorithm, Danmarks Nationalbank must:

   i. calculate and check the liquidity positions, limits and reservations of each relevant RTGS DCA; and

   ii. if the total liquidity position of one or more relevant RTGS DCAs is negative, extract single payment orders until the total liquidity position of each relevant RTGS DCA is positive.

   Thereafter, to the extent sufficient funds are available, Danmarks Nationalbank shall settle the relevant remaining cash transfer orders (except for the excluded payment orders in (ii)) simultaneously on the RTGS DCAs of the participants concerned.

   When extracting payment orders, Danmarks Nationalbank starts with the participant's RTGS DCA with the largest negative liquidity position and the payment order with the lowest priority at the back of the queue. The algorithm only runs for a short period of time, as determined at the discretion of Danmarks Nationalbank.

b. Under the ‘multiple optimisation’ algorithm, Danmarks Nationalbank must:

   i. compare participants' RTGS DCAs in pairs to determine whether queued payment orders can be settled within the available liquidity of the two participants' RTGS DCAs and within the limits they have specified (starting with the RTGS DCA pair with the smallest difference between the payment orders addressed to each other), and Danmarks Nationalbank reserves these payments simultaneously on the two participants' RTGS DCAs

   ii. if, in relation to a pair of RTGS DCAs as described in point (i), there is insufficient liquidity to honour the bilateral position, single payment orders are extracted until there is sufficient liquidity. In such cases, Danmarks Nationalbank settles the remaining payments, except for the excluded ones, simultaneously on the two participants' RTGS DCAs.

   After completion of the checks specified in points (i)-(ii), Danmarks Nationalbank shall check the multilateral payment positions (between the participant's RTGS DCA and other participants' RTGS DCAs for which a multilateral limit has been specified). For this purpose, the procedure described under paragraphs (i) to (ii) shall apply *mutatis mutandis*.

c. The ‘sub-account optimisation’ algorithm is used to optimise the settlement of urgent AS cash transfer orders on participants' sub-accounts. Using this algorithm, Danmarks Nationalbank calculates the total liquidity position of each participant's sub-account by determining whether the total amount of outgoing and incoming AS cash transfer orders waiting in the queue is negative or positive. If the result of these calculations and checks is positive for each relevant sub-account, Danmarks Nationalbank shall settle all payment orders simultaneously on the relevant participants' sub-accounts. If the outcome of these calculations and checks is negative, no settlement shall take place. Furthermore, this algorithm does not take account of any limits or reservations. For each settlement bank the total position is calculated and, if the positions for all settlement banks are covered, all transactions shall be settled. Transactions which are not covered are returned to the queue.

d. Cash transfer orders entered after the multiple optimisation algorithm or the partial optimisation algorithm has started may nevertheless be settled immediately if the positions and limits of the participants' affected RTGS DCAs are compatible with both the settlement of these orders and the settlement of cash transfer orders in the current optimisation procedure.

e. The partial optimisation algorithm and the multiple optimisation algorithm shall be run sequentially in that order.

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

g. 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 request is taken into account immediately.

10. Connectivity

Participants must connect to TARGET DKK using one of the following methods:

a. User-to-Application (U2A): In U2A, participants connect to a GUI so they can perform business functions based on their respective access rights. This allows users to enter and maintain static data as well as retrieve company information.

b. Application-to-Application (A2A): In A2A, software applications communicate with TARGET Services by exchanging individual messages and files based on their respective access rights and message subscription and route configuration. The A2A communication relies on XML messages, using the ISO 20022 standard where applicable, for both inbound and outbound communication.

The connection methods for TARGET Services are described in more detail in ESMIG UDFS. The relevant User Handbook (UHB) includes exhaustive information about each business function that the GUI in question provides.

11. Functional documentation description (UDFS) and user handbook

Further details and examples explaining the above rules can be found in the relevant UDFS and user handbooks for each service, as amended from time to time and published on the ECB's website.

Appendix 2 – Business continuity and contingency procedures

1. General provisions

This Appendix sets out the arrangements between Danmarks Nationalbank and participants if TARGET DKK or one or more NSPs fail or are affected by an abnormal external event, or if the failure affects any participant.

Provisions set out in this section 1 apply to MCAs, RTGS DCAs and their sub-accounts, RTGS AS technical accounts, T2S DCAs and TIPS DCAs.

1.1 Measures of business continuity and contingency processing

a. In the event that an abnormal external event occurs and/or there is a failure of TARGET DKK and/or there is a failure of one or more NSPs which affects the normal operation of TARGET DKK, Danmarks Nationalbank 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 TARGET DKK:

   i. relocating the operation of TARGET DKK to an alternative site

   ii. changing of the TARGET DKK operating schedule.

c. In relation to business continuity and contingency procedures measures, Danmarks Nationalbank has full discretion as to whether and which measures to adopt.

1.2 Incident Communication

If an event described under paragraph 1.1(a) occurs, this shall be communicated to participants via the ECB's website, if available, through the GUI(s) and, if relevant, via Danmarks Nationalbank's communication channels. In particular, communications to participants will include the following information:

a. a description of the event and its impact on TARGET Services

b. the time at which resolution of the event is expected (if known)

c. information on the measures already taken (if any)

d. the advice to participants (if any)

e. the timestamp of the communication and indication of when an update will be provided.

If an event occurs in addition to the above, e.g. in relation to SPI, this is communicated to the participants via Danmarks Nationalbank's communication channels.

1.3 Change of operating hours

a. When changing the TARGET DKK operating schedule as provided for in Part I 'General Terms and Conditions', Article 19(2), Danmarks Nationalbank may delay the TARGET DKK cut-off times for a given business day, delay the start of the following business day or change the time of any other event listed in Appendix 3.

b. The cut-off times of TARGET DKK for a given business day may be delayed if a TARGET DKK failure has occurred during that day but has been resolved before 18:00. Such a closing time delay should not normally exceed two hours and shall be announced as early as possible to participants.

c. Once a delay of the TARGET DKK cut-off times is announced, it may be delayed further, but may not be withdrawn.

1.4. Other provisions

a. In the event of a failure of Danmarks Nationalbank, some or all of its technical functions in relation to TARGET DKK may be performed by the Level 3 national central banks (4CBs) on behalf of Danmarks Nationalbank.

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

2 Business continuity and contingency procedures (RTGS DCA, RTGS AS settlement procedures and MCA)

In addition to the provisions set out in section 1, the provisions set out in this section 2 applies specifically to RTGS DCA holders, AS (retail payment systems) that make use of RTGS AS settlement procedures, and to holders of MCAs.

2.1 Relocation of the operation of TARGET DKK to an alternative site

a. The relocation of the operation of TARGET DKK to an alternative site referred to in section 1, paragraph 1(b)(i) may be to a place within the same region or in another region.

b. In the event that the operation of TARGET DKK is relocated to another region, participants shall: (i) refrain from sending new cash transfer orders to TARGET DKK; (ii) at the request of Danmarks Nationalbank, perform a reconciliation; (iii) resubmit any cash transfer orders identified as missing; and (iv) provide Danmarks Nationalbank with all relevant information in this respect.

c. Danmarks Nationalbank may take further action, including debiting and crediting participants' accounts, in order to return those participants' accounts to their status prior to the relocation.

2.2 Change of operating hours

Danmarks Nationalbank may, following a specific assessment, choose to postpone the closure of TARGET DKK.

2.3 Contingency processing

The following procedures apply to RTGS DCA holders and AS (retail payment systems) that utilise RTGS AS settlement procedures:

a. If deemed necessary to do so, Danmarks Nationalbank initiates the contingency processing of cash transfer orders using the TARGET DKK contingency solution or other means. In such cases, contingency processing shall be provided on a best efforts basis. Danmarks Nationalbank informs the participants of the start of a contingency processing via any available means of communication.

b. In contingency processing using the TARGET DKK contingency solution, payment and cash transfer orders must be submitted via ECONS II by RTGS DCA holders and authorised by Danmarks Nationalbank. All liquidity transfers in ECONS II are executed by Danmarks Nationalbank on behalf of participants upon request. In addition, an AS may submit files containing payment instructions under AS settlement procedure A, which the relevant AS authorises Danmarks Nationalbank to upload to ECONS II.

c. The following cash transfer orders are considered ‘very critical’ and Danmarks Nationalbank shall use best efforts to process them in a contingency and without undue delay:

   i. payments related to the settlement of CLS Bank International's operations, processed on CLS Settlement

   ii. central counterparty margin calls.

d. Cash transfer orders other than those listed in paragraph (c) that are required in order to avoid systemic risks are considered 'critical', and Danmarks Nationalbank may decide to initiate contingency processing in relation to them. Critical cash transfer orders include, but are not limited to:

   i. liquidity transfer orders to T2S DCAs or TIPS DCAs

   ii. liquidity transfer orders that are indispensable to the execution of very critical cash transfer orders, as referred to in paragraph (c), or to other critical cash transfer orders.

e. Cash transfer orders that have been submitted to TARGET DKK before the activation of contingency processing, but are queued, may also undergo contingency processing. In such cases, Danmarks Nationalbank endeavours to avoid the double processing of cash transfer orders, but the participants bear the risk of double processing if it occurred.

2.4 Liquidity support in TARGET DKK contingency solution (ECONS II)

a. The participant may transfer liquidity from their T2S or TIPS DCAs to their ECONS II account. If this has not been possible, the following applies:

b. In ECONS II Danmarks Nationalbank may, following a specific assessment and on the basis of criteria to be determined by Danmarks Nationalbank, offer liquidity support to each participant. Liquidity support can only be provided against collateral, cf. below.

c. For contingency procedures utilising ECONS II, participants must provide eligible assets as collateral. During contingency processing, incoming cash transfer orders may be used to fund outgoing cash transfer orders.

d. For collateralisation of eligible assets during contingency processing, one of two contingency collateral accounts is used, with Danmarks Nationalbank as owner and as the account-holding institution. These two custody accounts, a T2S account and a VP account, are both set up as omnibus (OM) accounts. During contingency processing, traditional collateral accounts cannot be used and the contingency accounts must be used in order for the participant to obtain credit.

e. The transfer of eligible assets to the contingency collateral accounts must be instructed as Free of Payment (FoP) and instructed by the participant (‘Sell’) and Danmarks Nationalbank (‘Buy’).

f. The collateral value of eligible collateral is calculated in accordance with Part IX ‘Terms and Conditions for Pledging of Collateral for Credit Facilities’. Danmarks Nationalbank may grant credit to the participant via the TARGET DKK contingency solution against collateral in the eligible assets transferred to the contingency collateral accounts.

g. Redemptions and interest on the assets registered in the contingency collateral accounts that fall due during contingency processing are paid into yield accounts registered in the name of Danmarks Nationalbank and are also pledged to Danmarks Nationalbank as collateral for credit granted by Danmarks Nationalbank to the participant.

h. Once contingency processing has been completed, the collateral on the securities accounts and the yield accounts referred to above will be maintained until the participant has repaid the liquidity support offered by Danmarks Nationalbank in ECONS II. Danmarks Nationalbank is authorised to debit the participant’s MCA in order to repay the loan. After repayment of the loan the securities are transferred to a securities account with VP Securities A/S in the form of either a VP account or an account on T2S.

i. After the end of contingency processing, the interest on the participant's current account balance will be calculated retroactively for each day the monetary policy day is closed in the contingency solution of TARGET DKK. The applicable interest rate will be the current account rate for those days. Interest shall accrue, fall due and be paid in accordance with Part I ‘General Terms and Conditions', Article 12. The interest calculation will include the participant's balances on accounts inaccessible during the contingency processing, the participant's net inflow in TARGET DKK's contingency solution and balances on accounts in TARGET DKK available during the contingency processing. No interest is paid on the credit granted under the TARGET DKK contingency processing. The consolidated account balances used for the interest calculation will be based on the the General Ledger (GL) files generated by TARGET DKK during and after contingency processing.

2.5 Failures linked to participants

a. In the event that a participant has an issue or a problem that prevents it from sending cash transfer orders to TARGET DKK, the participant in question is responsible for resolving the issue or problem using its own means. Specifically, a holder of an MCA, RTGS DCA or an AS (utilising RTGS AS settlement procedures) can use any available internal solution, the GUI function to process liquidity transfers and payment orders or make use of the backup function via the GUI (RTGS DCA and AS).

b. If the resolution means and/or solutions and functionalities used by the participant referred to in paragraph (a) are exhausted, or if they are insufficient, the participant may then request support from Danmarks Nationalbank, and Danmarks Nationalbank shall provide such support on a best effort basis. Danmarks Nationalbank decides what support it offers to the participant.

c. Further detailed contingency procedures in relation to AS (retail payment systems) are set out in agreements between Danmarks Nationalbank and the relevant AS.

3. Business continuity and contingency procedures (T2S DCA)

In addition to the provisions set out in section 1, the provisions set out in this section 3 are applicable specifically to T2S DCA holders.

3.1 Relocation of the operation of TARGET DKK to an alternative site

a. The relocation of the operation of TARGET DKK to an alternative site referred to in section 1 paragraph 1.1 (b)(i) may be to a place within the same region or in another region

b. In the event that the operation of TARGET DKK is moved to another region, participants shall: (i) refrain from sending new cash transfer orders to TARGET DKK; (ii) at the request of Danmarks Nationalbank, perform a reconciliation; (iii) resubmit the cash transfer orders identified as missing; and (iv) provide Danmarks Nationalbank with all relevant information in this respect.

c. Danmarks Nationalbank may take further actions, including debiting and crediting participants' accounts, in order to bring participants'account balances to the status they had prior to the relocation.

3.2 Failures linked to participants

a. In the event that a T2S DCA holder has an issue or a problem that prevents it from sending cash transfer orders to TARGET DKK, the participant in question is responsible for resolving the matter using its own means.

b. If the resolution means and/or solutions and functionalities used by the participant referred to in paragraph (a) are exhausted, or if they are insufficient, the participant may then request support from Danmarks Nationalbank and Danmarks Nationalbank shall provide such support on a best effort basis. Danmarks Nationalbank decides what support it offers to the participant.

Appendix 3 – TARGET DKK operating schedule

1. Business days for transactions settled in TARGET Services are always the business day on which the system is operating for the respective currency. The system can work with different business days for different currencies.
2. Business days with settlement in Danish kroner: All days except Saturday, Sunday, New Year's Day, Maundy Thursday, Good Friday, Easter Monday, Ascension Day, the day after Ascension Day, Whit Monday, Constitution Day, Christmas Eve, Christmas Day, Boxing Day and 31 December.
3. TIPS DCAs are operational on every calendar day. All other account types are in operation on business days with settlement in Danish kroner.
4. A business day is opened during the evening of the previous business day.
5. The different periods during a business day and the specific operational events relevant for MCAs, RTGS DCAs (including RTGS AS technical accounts and sub-accounts), T2S DCAs and TIPS DCAs are shown in the following table:

HH:MM	MCAs	RTGS DCAs	T2S DCAs	TIPS DCAs
Approx. 18:45	Start of business day: Change of value date	Start of business day: Change of value date	Start of business day: Change of value date Preparation of night-time settlement	Processing of instant payment orders No liquidity transfers between TIPS DCAs and other TARGET DKK accounts
19:00	Settlement of CBOs Processing of automated and rule-based liquidity transfer orders		Deadline for acceptance of CMS data feeds (loan values) Preparation of night-time settlement	
19:30	Opening of the monetary policy day Settlement of CBOs Processing of standing liquidity transfer orders Processing of automated, rule-based and immediate liquidity transfer orders	Opening of the monetary policy day Settlement of AS transfer orders Processing of standing liquidity transfer orders Processing of automated, rule-based and immediate liquidity transfer orders	Opening of the monetary policy day	Start of the monetary policy day Processing of instant payment orders Processing of liquidity transfer orders between TIPS DCAs and MCAs and RTGS DCAs
20:00			Night-time settlement cycles	Processing of instant payment orders Processing of liquidity transfer orders between TIPS DCAs and other TARGET DKK accounts
02:30		Settlement of AS transfer orders Processing of automated, rule-based and immediate liquidity transfer orders		
02:30	Mandatory maintenance window until 02:30 on business days after the closing day, including every	Mandatory maintenance window until 02:30 on business days after the closing day, including every	Mandatory maintenance window until 02:30 on business days after the closing day, including every business day Monday	Processing of instant payment orders No liquidity transfer orders between TIPS DCAs and other

	business day Monday Optional maintenance window (if needed) from 03:00-05:00 on business days	business day Monday Optional maintenance window (if needed) from 03:00-05:00 on business days	Optional maintenance window (if needed) from 03:00-05:00 on business days	TARGET DKK accounts
Reopening time*	Settlement of CBOs Processing of automated, rule-based and immediate liquidity transfer orders	Settlement of AS transfer orders Processing of automated, rule-based and immediate liquidity transfer orders	Night-time settlement cycles	Processing of instant payment orders Processing of liquidity transfer orders between TIPS DCAs and other TARGET DKK accounts
05:00			Day trade/Real-time settlement: Preparation of real-time settlement. Time slots for partial settlement are 08:00, 10:00, 12:00, 14:00 and 15:30 (or 30 minutes before the start of the DvP cut-off time)	
07:00		Processing of customer and interbank payment orders		
16:00			Cut-off time for DvP orders	
16:30		Cut-off time for AS transfer orders	Automatic auto-collateralisation reimbursement, followed by the optional cash sweep	
16:40			Cut-off time for CBO	
16:45	Cut-off time for liquidity transfer orders to T2S DCAs	Cut-off time for liquidity transfer orders to T2S DCAs	Cut-off time for liquidity transfer orders followed by the mandatory cash sweep	Processing of instant payment orders Processing of liquidity transfer orders between TIPS DCAs and MCAs and RTGS DCAs Blocking of liquidity transfer orders from TIPS DCAs to T2S DCAs No liquidity transfer orders between T2S DCAs and TIPS DCAs are processed during this period
17:00	Blocking for liquidity transfer orders	Blocking for interbank and customer payment orders and liquidity transfer orders and AS transfer orders Blocking for CB: interbank payment orders		Processing of instant payment orders Blocking of liquidity transfer orders between TIPS DCAs and TARGET DKK accounts No liquidity transfer orders between TIPS DCAs and other TARGET DKK accounts are processed during this period
17:00	Closing of the monetary policy day (intraday loans to be	Closing of the monetary policy day (intraday loans to be	Closing of the monetary policy day (intraday loans to be	Closing of the monetary policy day (intraday loans to

	covered)	covered)	covered)	be covered)
17:00-18:00	DKK Central Bank Period	DKK Central Bank Period	DKK Central Bank Period	DKK Central Bank Period Processing of instant payment orders No liquidity transfer orders between TIPS DCAs and other TARGET DKK accounts are processed during this period
18:00	Blocking for CB: Liquidity transfer orders. CBOs. Credit line modifications. Calculation of current account balances for interest calculation	Blocking for CB: Liquidity transfers Calculation of current account balances for interest calculation	Cut-off time for FOP Finalising the processing of T2S settlement Recycling and Purging End-of-day reporting and statements	Change of business day Calculation of current account balances for interest calculation. Processing of instant payment orders No liquidity transfer orders between TIPS DCAs and other TARGET DKK accounts are processed during this period
18:40	End of business day	End of business day	End of business day	

SPI service windows
Danmarks Nationalbank can organise service windows in systems on non-business days and on business days between 19:00-07:00. However, service windows may exceptionally occur at other times. Danmarks Nationalbank does not send out separate information about the organisation of service windows unless it is deemed necessary in the given situation.

Opening hours may change if business continuity procedures are implemented, in accordance with Appendix 2. On the last day of a Eurosystem minimum reserve period, the cut-off times of 18:40, 18:45, 19:00 and 19:30 for MCAs and RTGS DCAs (as well as for RTGS AS technical and sub-accounts) will be 15 minutes later.

Appendix 4 – Coverage of Danmarks Nationalbank's costs for TARGET DKK and pricing model for TARGET Services

1. General

1. The following services are not included in the services offered by Danmarks Nationalbank and are charged by the relevant service providers in accordance with their terms and conditions:

   i. services offered by NSPs

   ii. non-cash related T2S services.

2. Co-managees are not charged by Danmarks Nationalbank, neither in relation to the recovery of Danmarks Nationalbank's costs for TARGET DKK nor in relation to the use of TARGET Services. The co-manager's charging of co-managees is a matter between the two parties and is of no concern to Danmarks Nationalbank.

2. Coverage of Danmarks Nationalbank's costs for TARGET DKK

1. Coverage of Danmarks Nationalbank's running costs for TARGET DKK

   All direct participants pay a monthly fee, which is set with a view to user funding of both the operation and further development of the systems that support TARGET DKK. The fee shall be determined by Danmarks Nationalbank for 12 months at a time and shall be recalculated each year with effect from 1 January. The fee is charged in arrears on the eleventh TARGET business day (in accordance with the calendar for TARGET closing days set out by the ECB) each month. If the eleventh TARGET business day is not a business day in TARGET DKK, debiting takes place on the next business day in TARGET DKK.

   The fee is calculated by Danmarks Nationalbank calculating the year's total costs to be financed by the participants and calculating the basis for distributing the costs among the participants.

   The basis of distribution is preferably based on the number and amount of each participant's RTGS transactions in the previous calendar year. The fee will be a minimum of kr. 1,000 per month.

   A detailed overview of the principles for the participants' coverage of Danmarks Nationalbank's running costs for TARGET DKK can be found on Danmarks Nationalbank's website.

2. Coverage of Danmarks Nationalbank's costs for the development of TARGET DKK

   Costs for the initial development of TARGET DKK were paid as a lump sum by the institutions participating in TARGET DKK at the time of commissioning. Institutions that subsequently become participants in TARGET DKK are charged a lump sum to cover the institution's share of the initial development costs. Danmarks Nationalbank's income from this will be included in the calculation of the amount charged to participants via the monthly fee the following year. The general framework for determining the amount is described on Danmarks Nationalbank's website.

3. Changes

   Danmarks Nationalbank may change the rules and principles for the participants' recovery of Danmarks Nationalbank's costs for TARGET DKK at any time and without notice.

3. Pricing models for TARGET Services

1. A participant wishing to change its choice of pricing model must notify Danmarks Nationalbank no later than the twentieth calendar day of the month (or, if this date is not a business day, the first business day thereafter), so that the change can be taken into account in the following month.

2. All prices are quoted in euros but will be invoiced to participants in Danish kroner. The conversion is made using the exchange rate published on the ECB's website on the third business day of the month.

4. Fee for MCA holders

1. MCAs and transactions settled on them shall not incur fees.

5. Fees for RTGS DCA holders

1. RTGS DCA holders can choose between two of the following pricing models:

a. a monthly fee, plus a fixed transaction fee per payment order (debit entry);

Monthly fee	**EUR 150**
Transaction fee per payment order	EUR 0.80

b. a monthly fee, plus a transaction fee based on the volume of payment orders (debit entry) and calculated on a cumulative basis as set out in the following table. For participants in a billing group the monthly volume of payment orders (debit entry) for all participants in that group shall be aggregated.

Monthly fee			**EUR 1 875**
			Monthly volume of payment orders
Band	**From**	**To**	**Transaction fee per payment order (EUR)**
1.	1	10,000	0.60
2.	10,001	25,000	0.50
3.	25,001	50,000	0.40
4.	50,001	75,000	0.20
5.	75,001	100,000	0.125
6.	100,001	150,000	0.08
7.	over 150,000		0.05

2. Liquidity transfer orders from RTGS DCAs to sub-accounts, to MCAs, or to RTGS DCAs held by the same participant or by participants located in the same banking group are free of charge.

3. Liquidity transfer orders from RTGS DCAs to MCAs or RTGS DCAs held by participants not belonging to the same banking group shall incur a charge of EUR 0.80 per transaction (debit entry).

4. Liquidity transfer orders from RTGS DCAs to T2S DCAs or TIPS DCAs shall be free of charge.

5. Cash transfer orders from an RTGS DCA to an AS account shall not be charged to the RTGS DCA holder.

6. The following fees shall apply to RTGS DCA holders:

Service	**Monthly fee (EUR)**
Addressable BIC code holder (correspondents)	20
Unpublished BIC	30
Multi-addressee access (based on BIC 8)	80

6. Fees for AS when using the payment procedures in RTGS

Fees are charged per ancillary system regardless of the number and type of accounts. AS operators operating more than one system will be charged for each system.

1. ASs that use RTGS AS payment procedures or have been granted an exemption to settle on an RTGS DCA must choose one of the following two pricing models:

a. a monthly fee, plus a fixed transaction fee per cash transfer order;

Monthly fee		**EUR 300**
Transfer fee per cash transfer order		EUR 1.60

b. a monthly fee, plus a transaction fee based on the volume of cash transfer orders and calculated on a cumulative basis, as shown in the following table:

Monthly fee			EUR 3 750
Monthly volume of cash transfer orders			
Band	From	To	Transaction fee per cash transfer order (EUR)
1.	1	5,000	1.20
2.	5,001	12,500	1.00
3.	12,501	25,000	0.80
4.	25,001	50,000	0.40
5.	over 50,000		0.25

Cash transfer orders between an RTGS DCA and an AS account are charged to the relevant AS according to the pricing model selected by the ancillary system.

2. In addition to the fees listed above, each AS shall be subject to fixed fees as shown in the following table:

A. Fixed fee I		
Monthly fee per AS		EUR 2,000
B. Fixed fee II (based on the underlying gross value)		
Size (EUR million/day)	**Annual fee (EUR)**	**Monthly fee (EUR)**
from 0 to 999.99	10,000	833
from 1,000 to 2,499.99	20,000	1,667
from 2,500 to 4,999.99	40,000	3,334
from 5,000 to 9,999.99	60,000	5,000
from 10 000 to 49 999.99	80,000	6,666
from 50,000 to 499,999.99	100,000	8,333
500,000 and above	200,000	16,667

7. Fees for T2S DCA holders

1. The following fees shall be charged for the operation of T2S DCAs:

Item	**Applied rule**	**Fee per item (EUR)**
Liquidity transfer orders between T2S DCAs	Per transfer for the debited T2S DCA.	0.141
Intra-balance movements	Any successfully executed intra-balance movement (i.e. blocking, unblocking, reservation of liquidity, etc.).	0.094
A2A queries	Per business item within each A2A query generated.	0.007
A2A reports	Per business item within each generated A2A report,	
including A2A reports as a result of U2A queries.	0.004	
Messages bundled into a file	Per message in each file containing bundled messages.	0.004
Transmission	Each transmission per T2S party (both inbound and outbound) will be counted and charged for (except for technical acknowledgement messages).	0.012
U2A queries	Any executed query search function.	0.100
Fee per T2S DCA	Any T2S DCA existing at any time during the monthly billing period	
Currently no fee. For regular evaluation.	0.000	
Auto-collateralisation	Issue or return of auto-collateralisation.	0.000

2. Liquidity transfer orders from a T2S DCA to an RTGS DCA, a TIPS DCA or an MCA are free of charge.

8. Fees for TIPS DCA holders

1. The following fees are charged for the operation of TIPS DCAs:

a. For each TIPS DCA, a fixed monthly fee of EUR 800 is charged to the TIPS DCA holder. This fixed fee includes one BIC, which shall be a reachable party in TIPS and designated for the use of the TIPS DCA holder.

b. For each additional reachable party, up to a maximum of 50, designated by the TIPS DCA holder, a fixed monthly fee of EUR 20 is charged to the designating TIPS DCA holder. There is no charge for any subsequent reachable parties designated.

c. For each instant payment order or positive recall answer accepted by Danmarks Nationalbank pursuant to Article 17 of Part I 'General Terms and Conditions', a fee of EUR 0.001 shall be charged to both the holder of the TIPS DCA to be debited and the holder of the TIPS DCA to be credited, irrespective of whether or not the instant payment order or positive recall answer is settled.

d. No fee is charged for liquidity transfer orders from TIPS DCAs to MCAs, RTGS DCAs, sub-accounts or T2S DCAs.

Appendix 5 – Requirements for information security management and business continuity management in TARGET DKK

MCA holders, T2S DCA holders and TIPS DCA holders
These requirements regarding information security management shall not apply to MCA holders, T2S DCA holders and TIPS DCA holders.

RTGS DCA holders and AS
The requirements set out in section 1 of this Appendix (information security management) are applicable to all RTGS DCA and AS holders, except when an RTGS DCA or AS holder can demonstrate that a specific requirement is not applicable. In determining the scope of the requirements of the infrastructure, the participant shall identify the elements that form part of the payment transaction chain. Specifically, the payment transaction chain begins at a point of entry, i.e. a system involved in creating transactions (e.g. workstations, front office and back office applications, middleware), and ends at the system responsible for sending the message to the NSP (Network Service Provider).

The requirements set out in section 2 of this Appendix (business continuity) apply to holders of RTGS DCAs and ASs designated by Danmarks Nationalbank as important for the smooth functioning of the TARGET system.

1. Managing information security

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 processing facilities should not be reduced by the introduction of and/or reliance on one or more external parties or the products/services they provide. 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 to 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, business processes and underlying information systems, such as operating systems, infrastructures, business applications, standard products, services and user-developed applications, within the scope of the payment transaction chain shall be included and shall have a designated owner. The responsibility for the maintenance and operation of appropriate controls in the business process-

es 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 asset classification
Information assets are classified according to their critical importance to the participant's seamless provision of the service. 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
Facilities for processing of critical or sensitive data shall be located in secure areas and be protected by designated security areas with adequate security barriers and access control. 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 also be 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 plug-ins) 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 implemented in conjunction with the exchange of information with TARGET (e.g. software received from a service agency) must be used in accordance with a formal agreement with the third party.

Requirement 1.9: Access control

Access to information assets must be justified by business requirements (need-to-know) and according to the established framework of company policies (including the information security policy). Clear rules for access control must be established based on the principle of least privilege to accurately reflect the needs of the corresponding business and IT processes. Logical access controls (e.g. for backup management) should, where applicable, be consistent with physical access controls, unless appropriate compensating controls (e.g. encryption, anonymisation of personal data) are in place.

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.

Particular attention shall be paid, where applicable, to the granting of access rights of such a critical nature that the abuse of these access rights may have serious negative consequences for the participant's operations (e.g. access rights authorising 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 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 for the use of cryptographic controls to protect the confidentiality, authenticity and integrity of information must be developed and implemented. A key management policy shall be established to support the use of cryptographic controls.

There shall be a policy for viewing confidential information on screen or in print (e.g. a screen lock and clean desk policy) to mitigate 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.

Adequate 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 the data flows and the level of risk of the network zones in the organisation. There shall be specific controls to protect sensitive data 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 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 third-party supplier 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 the 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 of security incidents and vulnerabilities, roles, responsibilities and procedures at the enterprise and technical level must be defined and tested to ensure a fast, efficient and secure recovery from information security incidents, including scenarios with cyber-related cause (e.g. fraud pursued by an outside attacker or 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 and 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 im-

plemented 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 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.

2. Business continuity management

The following requirements relate to business continuity management. Each TARGET DKK participant must have a business continuity strategy that fulfils the following requirements:

Requirement 2.1:
Business continuity plans shall be developed and procedures for maintaining them shall be 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 interrupted.

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.

Appendix 6 – Definitions

1. ‘4CB’: Deutsche Bundesbank, Banco de España, Banque de France and Banca d’Italia jointly in their capacity as the national central banks responsible for building, maintaining and operating TARGET services in accordance with the relevant agreements and decisions taken by the Governing Council of the ECB

2. ‘addressable BIC holder’: an entity that: (a) has a Business Identifier Code (BIC); and (b) is a correspondent or customer of an RTGS DCA holder or a branch of an RTGS DCA holder and is able to submit payment orders to and receive payments from TARGET DKK via that RTGS DCA holder

3. ‘settlement bank’: a holder of an RTGS DCA whose RTGS DCA or sub-account is used to settle AS transfer orders submitted by an AS using the RTGS AS settlement procedure

4. ‘settlement bank account group (SBAG)’: a list of RTGS DCAs and/or sub-accounts established in conjunction with the settlement of an ancillary system using the RTGS AS settlement procedure

5. ‘ancillary system (AS)’: a system operated by an entity established in the European Union or in the EEA and subject to supervision and/or oversight by a competent authority, in which payments and/or financial instruments are exchanged and/or cleared or recorded with (a) the monetary obligations resulting in transfer orders settled in TARGET DKK

6. ‘ancillary system settlement procedure, AS settlement procedure’: an RTGS AS settlement procedure

7. ‘ancillary system transfer order, AS transfer order’: a cash transfer order initiated by an ancillary system for the purpose of an RTGS ancillary system settlement procedure

8. ‘recall request’: a message from an RTGS DCA holder or a TIPS DCA holder requesting a recall of a settled payment order or an instant payment order, respectively

9. ‘automated liquidity transfer order’: a liquidity transfer order that is generated automatically to transfer funds from a designated RTGS DCA to the participant’s MCA in the event that there are insufficient funds in that MCA to settle central bank operations

10. ‘business day’: a day on which MCAs, RTGS DCAs or T2S DCAs are available for the settlement of cash transfer orders

11. ‘banking group’:

a. 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 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 combination of credit institutions referred to in paragraph (a)(i) or (ii) where a parent company does not present consolidated financial statements in accordance with IAS 27 but may be able to meet the criteria as defined in IAS 27 for inclusion in consolidated financial statements subject to verification by Danmarks Nationalbank

c. a bilateral or multilateral network of credit institutions which is: (i) organised through a statutory framework defining the affiliation of credit institutions to such a network; or (ii) characterised by self-organised cooperation mechanisms (promoting, supporting and representing the business interests of its members) and/or economic solidarity going beyond the usual cooperation between credit institutions, whereby such cooperation and solidarity are permitted by the articles of association or statutes of credit institutions or established by virtue of separate agreements, and in each case referred to in paragraphs (c)(i) and (c)(ii), Danmarks Nationalbank has approved the application to be considered a banking group

12. 'eligible securities': eligible securities as defined in Part IX 'Terms and Conditions for Pledging of Collateral for Credit Facilities', Article 4(1)(a)
13. 'payer': except where used in Part I 'General Terms and Conditions', Article 29, a participant whose MCA or DCA is debited as a result of a cash transfer order being settled
14. 'payee': except where used in Part I 'General Terms and Conditions', Article 29, a participant whose MCA or DCA is credited as a result of a cash transfer order being settled
15. 'payment order': any instruction from a participant or a party acting on its behalf to make a sum of money available to a recipient from one account by posting an entry on another account, and which is not an AS transfer order, a liquidity transfer order, an instant payment order or a positive recall answer
16. 'central bank operation': any payment order or liquidity transfer order initiated by Danmarks Nationalbank on an MCA that has been opened in TARGET DKK
17. 'currency participation agreements': the agreements concluded between the Eurosystem and Danmarks Nationalbank on Danmarks Nationalbank's participation in T2, T2S and TIPS with Danish kroner
18. 'dedicated cash account (DCA)': an RTGS DCA, a T2S DCA or a TIPS DCA
19. 'participant': (a) an entity that has at least one MCA and possibly one or more additional DCAs in TARGET Services; or (b) an AS
20. 'The European System of Central Banks': The ECB and the national central banks in the EU whether they have adopted the euro or not
21. 'available liquidity': a credit balance on a participant's account and, if applicable, any intraday credit granted to the MCA that has not yet been utilised or, if applicable, has been reduced by an amount used to reserve liquidity or block funds on MCAs or DCAs
22. 'ECB': The European Central Bank
23. 'Eurosystem': ECB and the national central banks of a member state whose currency is the euro
24. 'current account balance': the sum of the credit balance/utilised intraday credit on the primary MCA and the balance on the participant's other accounts, other than cash deposit accounts, and any balance on the separate MCA, registered in the name of Sveriges Riksbank or Norges Bank, opened for the participant's use of cash collateral in Danish kroner in the SCP scheme
25. 'current account limit': the current ceiling for a monetary policy counterparty's current account balance at 17:00, where the aggregate current account limit of the monetary policy counterparties is equal to the sum of the individual current account limits
26. 'insolvency proceedings': insolvency proceedings as defined in Article 2(j) of 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
27. 'instructing party': an entity that has been designated as such by a TIPS DCA holder and is authorised to submit instant payment orders or liquidity transfer orders and/or receive instant payment orders or liquidity transfer orders on behalf of that account holder or a reachable party of that account holder in conjunction with the holder of the relevant account
28. 'intraday credit': credit granted for a period of time within one business day

29. ‘account monitoring group’: a group consisting of two or more MCAs and/or DCAs, where one participant, the lead party, has an overview of the balance of each TARGET account in the group

30. ‘credit institution’: either (a) a credit institution as defined in Article 4(1)(1) of Regulation (EU) 575/2013 of the European Parliament and of the Council and Article 5(1)(2) of the Danish Financial Business Act (Consolidated Act No 406 of 29 March 2022) that is subject to supervision by a competent authority; or (b) another credit institution as defined in Article 123(2) of the treaty that is subject to supervision of a standard comparable to supervision by a competent authority

31. ‘credit memorandum balance (CMB)’: a limit set by the T2S DCA holder or TIPS DCA holder on the use of liquidity by a specific reachable party

32. ‘liquidity transfer order’: a cash transfer order to transfer a specified amount of funds for liquidity management purposes

33. ‘event of default’: an impending event or event that has already occurred, the occurrence of which may involve a risk of a participant's failure to fulfil its obligations under these Terms and Conditions or other rules, including where

a. the participant no longer fulfils the eligibility criteria set out in Article 4 of Part I 'General Terms and Conditions' or the requirements set out in Article 5(2)(a) of Part I 'General Terms and Conditions'.

b. insolvency proceedings are opened regarding the participant

c. an application is made for the proceedings referred to in (b)

d. the participant issues a written declaration of its inability to pay all or part of its debts or its inability to fulfil its obligations in connection with intraday credit

e. the participant enters into a voluntary general agreement or scheme with its creditors

f. the participant is, or is deemed to be, insolvent or unable to pay its debts

g. the participant's credit balance on any of its TARGET DKK accounts or all or a substantial part of the participant's assets are frozen, subject to distress levy, seized or subject to any other measure intended to protect the public interest or the participant's creditors

h. any material representation or statement made by the participant prior to the conclusion of the contract or presumed to have been made by the participant under applicable law is incorrect or untrue

i. all or a substantial part of the participant's assets are assigned

34. ‘NCT Inst (Nordic Payments Council's NPC Instant Credit Transfer Scheme)’: an automated, open standard scheme providing a set of rules that NPC Inst participants must comply with, and enabling payment service providers to offer an automated, instant credit transfer product in Danish kroner

35. ‘network service provider’ (NSP): a company that has been granted a licence by the Eurosystem to provide connectivity services via the access gateway for financial market infrastructures to the TARGET services

36. ‘contingency solution’: the functionality that enables Danmarks Nationalbank and participants to process cash transfer orders in the event that the normal operation of MCAs and/or RTGS DCAs and/or RTGS AS technical accounts is not possible

37. ‘cash transfer order’: any instruction given by a participant or a party acting on its behalf to make a sum of money available to a recipient from one account by posting an entry on another account, and which is an AS transfer order, a liquidity transfer order, an instant payment order, a positive recall answer or a payment order

38. ‘monetary policy instruments’: interest-bearing current account deposits, monetary policy loans and certificates of deposit

39. ‘positive recall answer: in accordance with the NPC Inst scheme, a cash transfer order initiated by the recipient of a recall request in response to a recall request in favour of the sender of that recall request

40. ‘primary MCA’: the MCA that a participant holding multiple MCAs has agreed with Danmarks Nationalbank is the participant's primary MCA

41. ‘receiving custody account’: a T2S custody account opened with VP Securities A/S in the name of the participant, which is used in connection with the raising of T2S auto-collateralisation loans and which the account holder has pledged to Danmarks Nationalbank

42. ‘rule-based liquidity transfer order’: a liquidity transfer order that has been triggered as a result of: (a) the balance on an MCA or RTGS DCA account exceeding a predefined floor or ceiling; or (b) insufficient funds being available to cover urgent queued payment orders or high priority payment orders on an RTGS DCA

43. ‘regular custody account’: a T2S custody account opened with VP Securities A/S in the name of the participant, which is used in connection with the raising of intraday loans in TARGET DKK for the redemption of T2S auto-collateralisation loans and which the account holder has pledged to Danmarks Nationalbank

44. ‘capacity opinion’: a legal opinion containing an assessment of the legal capacity of a participant to assume and fulfil its obligations

45. ‘RTGS AS settlement procedure (real-time gross settlement ancillary system settlement procedure)": one of two special predefined services for the submission and settlement of AS transfer orders related to the settlement of AS on RTGS DCAs, sub-accounts and RTGS AS technical accounts

46. ‘RTGS AS technical account (real-time gross settlement ancillary system technical account)’: an account held by an AS and used in connection with an RTGS AS settlement procedure

47. ‘security officer’: a person authorised by the authorised signatories of an account holder

48. ‘instant payment order’: in accordance with the Nordic Payments Council's Instant Credit Transfer Scheme (NPC Inst), a cash transfer order that can be executed 24 hours a day, every day of the year with immediate or near-immediate processing and notification to the payer, and includes instant payment orders from a TIPS DCA to a TIPS DCA

49. ‘suspension’: the temporary suspension of a participant's rights and obligations for a period of time to be determined by Danmarks Nationalbank

50. ‘T2S auto-collateralisation loan’: an intraday loan in Danish kroner granted by Danmarks Nationalbank on T2S, where a participant has insufficient funds in the T2S DCA to settle transactions or make corporate action payments on T2S, and where the loan is collateralised by the securities being purchased or securities transferred from one of the collateral-providing custody accounts specified by the participant to the participant's receiving custody account pledged to Danmarks Nationalbank

51. ‘TARGET2-Securities, T2S’: the hardware, software and other components of the technical infrastructure through which the Eurosystem provides services to the central securities depositories and Eurosystem central banks that enable the basic, neutral and borderless settlement of securities transactions in central bank money on a delivery versus payment basis

52. ‘reachable party’: an entity that (a) holds a Business Identifier Code (BIC); (b) is designated as such by a TIPS DCA holder; (c) is a correspondent, customer or branch of a TIPS DCA holder; and (d) is addressable through TIPS and able to

submit cash transfer orders and receive cash transfer orders either through the TIPS DCA holder or directly with the authorisation of the TIPS DCA holder

53. ‘non-settled cash transfer order’: a cash transfer order that is not settled on the business day on which it is accepted

54. ‘broadcast message’: information that is made available to all or groups or a selected group of participants simultaneously

55. ‘Business Identifier Code, BIC’: a code as defined by ISO Standard No. 9362