

RETNINGSLINJER

DEN EUROPÆISKE CENTRALBANKS RETNINGSLINJE

af 15. september 2010

om ændring af retningslinje ECB/2007/2 om TARGET2 (Trans-European Automated Real-time Gross settlement Express Transfer system)

(ECB/2010/12)

(2010/593/EU)

STYRELSESRÅDET FOR DEN EUROPÆISKE CENTRALBANK HAR —

opbygget og fungerer på grundlag af den fælles platform, hvor alle betalingsordrer sendes igennem, behandles og hvor betalinger til sidst modtages på samme tekniske måde.»

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 127, stk. 2,

under henvisning til statuten for Det Europæiske System af Centralbanker og Den Europæiske Centralbank, særlig artikel 3.1, artikel 17, 18 og 22, og

2. Artikel 2 ændres således:

ud fra følgende betragtninger:

a) Følgende definitioner affattes således:

(1) Styrelsesrådet for Den Europæiske Centralbank har vedtaget retningslinje ECB/2007/2 af 26. april 2007 om TARGET2-systemet (Trans-European Automated Real-time Gross settlement Express Transfer) ⁽¹⁾, som regulerer TARGET2-systemet, der er karakteriseret ved en fælles teknisk infrastruktur, benævnt den fælles platform (SSP).

»— »deltagende national centralbank«: den nationale centralbank i en medlemsstat, der har indført euroen«

(2) Der er behov for at ændre retningslinje ECB/2007/2 for: a) at tage højde for opdateringerne med henblik på lanceringen af TARGET2 4.0, navnlig for at give deltagerne mulighed for at få adgang til en eller flere PM-konti via internetbaseret adgang, og b) at afspejle en række tekniske ændringer efter traktaten om Den Europæiske Unions funktionsmådes ikrafttræden samt tydeliggøre nogle spørgsmål —

»— »adresserbar BIC-kode-indehaver«: en enhed som: a) er indehaver af en virksomhedsidentifikationskode (Business Identifier Code) (BIC), b) ikke er anerkendt som indirekte deltager og c) er kunde hos en direkte deltager eller hos en filial af en direkte eller indirekte deltager samt er i stand til at sende betalingsordrer til og modtage betalinger fra et TARGET2 delysnet via den direkte deltager«

b) »— »bankidentifikationskode (BIC)«: en kode som defineret ved ISO Standard nr. 9362« erstattes af følgende: »— »virksomhedsidentifikationskode (BIC) (Business Identifier Code) (BIC)«: en kode som defineret ved ISO Standard nr. 9362«.

VEDTAGET FØLGENDE RETNINGSLINJE:

Artikel 1

Retningslinje ECB/2007/2 ændres således:

1. Artikel 1, stk. 1, affattes således:

»1. TARGET2 yder realtidsbruttoafvikling af betalinger i euro, med afvikling i centralbankpenge. Systemet er

c) Der tilføjes følgende definitioner:

»— »internetbaseret adgang«: hvor deltageren har valgt en PM-konto, som der kun er adgang til via internettet, og deltageren afgiver betalingsmeddelelser eller kontrolmeddelelser til TARGET2 ved brug af internettet«

⁽¹⁾ 1. EUT L 237 af 8.9.2007, s. 1.

»— »certificeringsmyndigheder«: en eller flere centralbanker, som Styrelsesrådet har udnævnt hertil, der på Eurosystemets vegne kan udstede, forvalte, tilbagekalde og forny elektroniske certifikater«

»— »elektroniske certifikater« eller »certifikater«: en elektronisk fil, udstedt af certificeringsmyndighederne, der knytter en identitet til en offentlig nøgle, og som anvendes til følgende: at kontrollere, at en offentlig nøgle tilhører en person; til at bekræfte indehaverens identitet, til at kontrollere en underskrift fra denne person; og til at kryptere en meddelelse adresseret til denne person. Certifikater opbevares på en fysisk anordning såsom et chipkort eller en USB-nøgle, og henvisninger til certifikater omfatter sådanne fysiske anordninger. Certifikaterne er en del af kontrolprocessen af deltagerne, der har adgang til TARGET2 via internettet og afgiver betalingsmeddelelser eller kontrolmeddelelser«

»— »indehaver af certifikat«: en navngivet person, der af en TARGET2-deltager er identificeret og udpeget som indehaver af tilladelse til at have internetbaseret adgang til deltagerens TARGET2-konto. Dennes anmodning om certifikater er først kontrolleret af deltagerens hjemme-centralbank og sendt til certificeringsmyndighederne, som herefter har udleveret certifikater, som knytter de beviser, som identificerer deltageren, til den offentlige nøgle«

»— »harmoniserede vilkår«: vilkårene fastsat i bilag II og V.«

3. Artikel 6, stk. 1 og 2, affattes således:

»1. Alle deltagende nationale centralbanker indfører et regelsæt til gennemførelse af de harmoniserede vilkår for deltagelse i TARGET2, som er anført i bilag II, og de supplerende og ændrede harmoniserede vilkår for deltagelse i TARGET2 ved anvendelse af internetbaseret adgang, som er anført i bilag V. Disse regelsæt regulerer alene forholdet mellem den pågældende deltagende nationalbank og dens deltagere for så vidt angår behandlingen af betalinger i PM-modulet. Adgang til en PM-konto kan ske enten ved internetbaseret adgang eller via netværksleverandøren. Disse to metoder til adgang til en PM-konto udelukker hinanden, selv om en deltager kan vælge at have en eller flere PM-konti, som der hver især enten er adgang til via internettet eller netværksleverandøren.

2. ECB vedtager betingelser og vilkår for TARGET2-ECB ved at gennemføre bilag II, idet TARGET2-ECB dog kun skal

levere tjenester til clearing- og afviklingsorganisationer, herunder enheder etableret uden for EØS, under forudsætning af at de er undergivet overvågning af en kompetent myndighed, og at deres adgang til TARGET2-ECB er godkendt af Styrelsesrådet.«

4. Artikel 8, stk. 1, affattes således:

»1. Eurosystemets centralbanker yder pengeoverførselstjenester i centralbankpenge til afviklingssystemer i PM-modulet med adgang via netværksleverandøren eller, i overgangsperioden og såfremt relevant, til hjemmekonti. Disse tjenesteydelser reguleres af bilaterale ordninger mellem Eurosystemets centralbanker og de pågældende afviklingssystemer.«

5. Artikel 10, stk. 1, affattes således:

»1. Styrelsesrådet fastlægger sikkerhedspolitikken og kravene til sikkerhed og overvågning for SSP samt i overgangsperioden for den tekniske infrastruktur for hjemmekonti. Styrelsesrådet fastlægger desuden principperne for sikkerheden i forbindelse med certifikater anvendt til internetbaseret adgang.«

6. Artikel 16, stk. 2, affattes således:

»2. De deltagende nationale centralbanker skal senest den 31. juli 2007 eller en dato, som angives nærmere af Styrelsesrådet, fremsende til ECB de foranstaltninger, hvormed de tilsigter at følge denne retningslinje.«

7. Bilagene retningslinje ECB/2007/2 ændres i overensstemmelse med bilag I til denne retningslinje.

8. Bilag V tilføjes til retningslinje ECB/2007/2 i overensstemmelse med bilag II til denne retningslinje.

Artikel 2

Ikrafttræden

Denne retningslinje træder i kraft to dage efter dens vedtagelse. Den finder anvendelse fra den 22. november 2010.

*Artikel 3***Adressater og gennemførelsesbestemmelser**

1. Denne retningslinje er rettet til alle centralbanker i Eurosystemet.
2. De deltagende nationale centralbanker skal senest den 7. oktober 2010 fremsende til ECB de foranstaltninger, hvormed de tilsigter at følge denne retningslinje.

Udfærdiget i Frankfurt am Main, den 15. september 2010.

For ECB's Styrelsesråd
Jean-Claude TRICHET
Formand for ECB

BILAG I

1. Bilag I til retningslinje ECB/2007/2 ændres således:

I bilag I affattes tabellens punkt 7 således:

»7. Drift		
— Ledelse af alvorlige krisesituationer	— Ledelse mht ansvar for system-ejer	— Ledelse af systemet på grundlag af de aftaler, som er angivet i artikel 5, stk. 6, i denne retningslinje«
— Tilladelse til etablering og drift af TARGET2-simulator	— Varetagelse af kontakter med brugere på europæisk plan (med forbehold af eneansvar for centralbanker i Eurosystemet for forretningsforbindelse til deres kunder) og overvågning af daglig brugeraktivitet fra et forretnings-synspunkt (opgave for centralbanker i Eurosystemet)	
— Udnævnelse af certificeringsmyndigheder til internetbaseret adgang	— Overvågning af forretningsudviklingen	
— Beskrivelse af sikkerhedspolitikker, krav og kontrol vedrørende SSP	— Budgetlægning, finansiering, fakturering (opgaver for centralbanker i Eurosystemet) og andre administrative opgaver	
— Fastlæggelse af principper gældende for sikkerheden i forbindelse med certifikater til anvendelse ved internetbaseret adgang		

2. Bilag II til retningslinje ECB/2007/2 ændres således:

1) Artikel 1 ændres således:

a) Følgende definitioner affattes således:

— »adresserbar BIC-kode-indehaver (addressable BIC holder)«: en enhed som: a) er indehaver af en virksomhedsidentifikationskode (Business Identifier Code) (BIC), b) ikke er anerkendt som indirekte deltager og c) er kunde hos en direkte deltager eller hos en filial af en direkte eller indirekte deltager samt er i stand til at sende betalingsordrer til og modtage betalinger fra et TARGET2 delsystem via den direkte deltager«

— »kreditinstitut (credit institution)«: enten: a) et kreditinstitut som defineret i [indsæt de nationale lovbestemmelser, der gennemfører artikel 4, stk. 1, litra a), og — såfremt relevant — artikel 2 i bankdirektivet], der er underlagt tilsyn af en kompetent national myndighed, eller b) et andet kreditinstitut som defineret i artikel 123, stk. 2, i traktaten om Den Europæiske Unions funktionsmåde, som er underlagt kontrol efter standarder, som er sammenlignelige med tilsyn af en kompetent national myndighed«

— »organ inden for den offentlige sektor (public sector body)«: en enhed inden for den »offentlige sektor« som defineret i artikel 3 i Rådets forordning (EF) nr. 3603/93 af 13. december 1993 om fastlæggelse af definitioner med henblik på gennemførelse af forbuddene i traktatens artikel 104 og artikel 104 B, stk.1 (*)

(*) EFT L 332 af 31.12.1993, s. 1.«

b) — »bankidentifikationskode (Bank Identifier Code, (BIC))«: en kode som defineret ved ISO Standard nr. 9362« affattes således: — »virksomhedsidentifikationskode (Business Identifier Code) (BIC)«: en kode som defineret ved ISO Standard nr. 9362«.

c) Følgende definition indsættes:

— »User Detailed Functional Specifications (UDFS)«: den senest opdaterede udgave af UDFS, den tekniske dokumentation, der indeholder detaljerede angivelser af, hvordan en deltager interagerer med TARGET2.«

2) Artikel 4 ændres således:

a) Stk. 1 affattes således:

»1. Følgende typer af enheder kan godkendes som direkte deltagere i TARGET2 [indsæt centralbank/landereference]:

- a) kreditinstitutter, som har deres hjemsted i EØS, herunder hvor de handler gennem en filial, som er etableret i EØS
- b) kreditinstitutter, som har deres hjemsted uden for EØS, forudsat at de handler gennem en filial, som er etableret i EØS, og
- c) Nationale centralbanker i EU-medlemsstater samt ECB

forudsat at de i litra a) og b) omhandlede enheder ikke er omfattet af restriktive foranstaltninger vedtaget af Rådet for Den Europæiske Union eller medlemsstaterne i henhold til artikel 65, stk. 1, litra b), artikel 75 eller artikel 215 i traktaten om Den Europæiske Unions funktionsmåde, hvis gennemførelse [centralbank/landereference], efter at have underrettet ECB, anses for uforenelig med den effektive funktion af TARGET2.«

- b) I artikel 4, stk. 2, litra e), erstattes ordene »Det Europæiske Fællesskab« med Unionen og »fællesskabslovgivning« med »EU-lovgivning«.

3) Artikel 32, stk. 4, affattes således:

»4. [indsæt centralbankens navn] skal opbevare fuldstændige fortegnelser over deltagernes indgivne betalingsordrer og modtagne betalinger i [indsæt det tidsrum, der kræves i den relevante nationale lovgivning] fra det tidspunkt, hvor disse betalingsordrer er afgivet, og betalinger modtaget, forudsat at disse fuldstændige fortegnelser omfatter mindst fem år for alle deltagere i TARGET2, som er genstand for konstant overvågen i henhold til restriktive foranstaltninger vedtaget af Rådet for Den Europæiske Union eller medlemsstater eller længere, såfremt dette kræves af specifikke lovbestemmelser.«

4) Artikel 34, stk. 2, ændres således:

- a) I litra d) udgår ordene »og/eller«, og de tilføjes til litra e).

- b) Som litra f) indsættes:

»f) en national centralbank suspenderer eller bringer deltagerens adgang til intradagkredit til ophør i henhold til punkt 12 i bilag III.«

5) I artikel 38, stk. 2, erstattes ordet »Fællesskabet« af ordet »Unionen«.

6) Artikel 39, stk. 1, affattes således:

»1. Deltagere anses for at være bekendt med og skal handle i overensstemmelse med alle forpligtelser, der påhviler dem i forbindelse med lovgivning om personbeskyttelse, forebyggelse af hvidvaskning, finansiering af terrorisme, spredningsfølsomme nukleare aktiviteter og udvikling af fremføringssystemer til kernevåben, i særdeleshed for så vidt angår gennemførelse af egnede foranstaltninger angående betalinger, som debiteres eller krediteres deres PM-konti. Inden deltagere indgår kontraktforhold med tjenesteleverandøren, skal de endvidere gøre sig bekendt med dennes politik for indhentning af data.«

7) I artikel 40, stk. 1, erstattes ordet »SWIFT« af ordet »BIC«.

8) Artikel 44, stk. 2, erstattes af følgende:

»2. Uden at det berører Den Europæiske Unions Domstols kompetence hører enhver tvist, der opstår som følge af omstændigheder, der har tilknytning til det i stk. 1 nævnte forhold, under den eksklusive kompetence for de kompetente domstole i [indsæt den nationale centralbanks hovedsæde].«

9) I tillæg I affattes de sidste tre rækker i tabellen i afsnit 2, punkt1, således:

»MT 900	Valgfri	Bekræftelse på debitering/ændring af kreditlinje
MT 910	Valgfri	Bekræftelse på kreditering/ændring af kreditlinje
MT 940/950	Valgfri	(Kunde-) kontoudtog«

10) I tillæg V affattes den sidste række i tabellen i afsnit 3 således:

»1.00 – 7.00	Natafvikling i afviklingssystemet (kun for afviklingsprocedure 6)«
--------------	--

3. Bilag III til retningslinje ECB/2007/2 ændres således:

1) Følgende definitioner affattes således:

- »— »kreditinstitut (credit institution)«: enten: a) et kreditinstitut som defineret i artikel 2 og artikel 4, stk. 1, litra a), i bankdirektivet, som gennemført i national lovgivning, der er undergivet tilsyn af en kompetent national myndighed, eller b) et andet kreditinstitut som defineret i artikel 123, stk. 2, i traktaten om Den Europæiske Unions funktionsmåde, som er underlagt kontrol efter standarder, som er sammenlignelige med tilsyn af en kompetent national myndighed«
- »— »organ inden for den offentlige sektor (public sector body)«: en enhed inden for den »offentlige sektor« som defineret i artikel 3 i Rådets forordning (EF) nr. 3603/93 af 13. december 1993 om fastlæggelse af definitioner med henblik på gennemførelse af forbuddene i traktatens artikel 104 og artikel 104 B, stk.1 (*)

(*) EFT L 332 af 31.12.1993, s. 1.«

»— »misligholdelse«: en forestående eller allerede indtruffet hændelse, hvis indtræden kan udgøre en risiko for en enheds manglende opfyldelse af sine forpligtelser i henhold til de nationale regelsæt, som gennemfører denne retningslinje, eller eventuelle andre regler (herunder regler angivet af Styrelsesrådet vedrørende Eurosystemets pengepolitiske operationer), der gælder for forholdet mellem denne enhed og en national centralbank i Eurosystemet, herunder:

- a) hvor en enhed ikke længere opfylder adgangsbetingelserne og/eller de tekniske krav anført i bilag II og, eventuelt, bilag V
- b) indledning af insolvensbehandling vedrørende en enhed
- c) indgivelse af begæring om en behandling, som er angivet i litra b)
- d) en enheds udstedelse af en skriftlig erklæring om manglende betalingsevne vedrørende al eller en del af sin gæld eller manglende evne til at opfylde sine forpligtelser i forbindelse med intradag-kredit
- e) en enheds indgåelse af en frivillig generel aftale eller ordning med sine kreditorer
- f) hvor enheden er eller af den relevante deltagende nationale centralbank bedømmes at være insolvent eller ude af stand til at betale sin gæld
- g) hvor enhedens positive saldo på dennes PM-konto eller alle eller en væsentlig del af enhedens aktiver er indefrosset, omfattet af arrest, udlæg, beslaglagt eller omfattet af nogen anden foranstaltning, som har til formål at beskytte offentlige interesser eller enhedens kreditorer
- h) hvor enhedens deltagelse i et andet TARGET2-delsystem og/eller i et afviklingssystem er blevet suspenderet eller ophævet
- i) hvor en tilsikring eller en erklæring, som er afgivet af enheden forud for kontraktindgåelsen eller efter gældende lov forudsættes at være fremsat af enheden, er ukorrekt eller usand, eller
- j) overdragelse af alle eller en væsentlig del af enhedens aktiver.«

2) Punkt 1 affattes således:

»1. En deltagende national centralbank skal yde intradag-kredit til de enheder, som er angivet i punkt 2 nedenfor, og som har en konto hos den relevante deltagende nationale centralbank, forudsat at disse enheder ikke er omfattet af restriktive foranstaltninger som vedtaget af Rådet for Den Europæiske Union eller medlemsstaterne i henhold til artikel 65, stk. 1, litra b), artikel 75 eller artikel 215 i traktaten om Den Europæiske Unions funktionsmåde, hvis gennemførelse [centralbank/landereference], efter at have underrettet ECB, anser for uforenelig med den effektive funktion af TARGET2. Intradag-kredit må dog ikke ydes til en enhed, der er oprettet i et andet land end den medlemsstat, hvor den deltagende nationale centralbanks hovedsæde, hos hvilken enheden har en konto, er beliggende.«

3) Punkt 4 affattes således:

- »4. Intradag-kredit skal baseres på godkendt sikkerhed og ydes som intradag-overtræk med sikkerhedsstillelse og/eller intradag genkøbs-transaktioner i overensstemmelse med de supplerende fælles minimumsregnskaber (herunder de tilfælde af misligholdelse, som er anført heri, samt deres respektive konsekvenser), som Styrelsesrådet fastsætter med hensyn til Eurosystemets pengepolitiske operationer. Godkendt sikkerhed skal bestå af de samme aktiver og instrumenter som er godkendte aktiver med hensyn til Eurosystemets pengepolitiske operationer, og er underlagt samme regler for værdiansættelse og risikokontrol, som er foreskrevet i bilag I til retningslinje ECB/2000/7.«

4) Punkt 12 affattes således:

- »12. a) Deltagende centralbanker skal suspendere eller ophæve adgang til intradag-kredit, såfremt et af følgende tilfælde af misligholdelse indtræder:
- i) den pågældende enheds konto hos den deltagende nationale centralbank er suspenderet eller lukket
 - ii) enheden opfylder ikke længere en af betingelserne angivet i dette bilag for bevilling af intradag-kredit
 - iii) en kompetent retslig eller anden myndighed træffer beslutning om over for enheden at iværksætte en likvidationsprocedure eller udnævne en kurator eller en tilsvarende person eller iværksætte en anden tilsvarende procedure
 - iv) enheden er genstand for indefrysning af midler og/eller andre foranstaltninger truffet af Unionen, der begrænser enhedens mulighed for anvendelse af sine midler, eller
- b) deltagende nationale centralbanker kan suspendere eller ophæve adgang til intradag-kredit, hvis en national centralbank suspenderer eller ophæver deltagerens deltagelse i TARGET2 i henhold til artikel 34, stk. 2, litra b)-e), i bilag II, eller hvis der indtræffer et eller flere tilfælde af misligholdelse (bortset fra dem, der er nævnt i artikel 34, stk. 2, litra a)), eller
- c) hvis Eurosystemet af forsigtighedshensyn eller af andre årsager suspenderer eller indskrænker eller ekskluderer modparters adgang til pengepolitiske instrumenter i overensstemmelse med afsnit 2.4 i bilag I til retningslinje ECB/2000/7, skal deltagende nationale centralbanker gennemføre denne suspension eller indskrænkning eller eksklusion vedrørende adgang til intradag-kredit i overensstemmelse med de kontraktmæssige eller lovgivningsmæssige bestemmelser, som den pågældende nationale centralbank anvender.«

4. Bilag IV til retningslinje ECB/2007/2 ændres således:

1) Punkt 9, nr. 4, affattes således:

- »4) Afviklingsbanker og afviklingssystemer skal have adgang til information via ICM-modulet. Afviklingssystemerne skal underrettes om afslutning eller svigt af afviklingen. Hvis afviklingssystemet igangsætter likviditetsoverførslen fra skyggekontoen til afviklingsbankens PM-konto, skal de afviklingsbanker, der har adgang til TARGET2 via netværksleverandøren, have meddelelse om krediteringen via en SWIFT MT 202-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«

2) Punkt 10, nr. 4, affattes således:

- »4) Afviklingsbankerne og afviklingssystemerne skal have adgang til information via ICM-modulet. Afviklingssystemerne skal underrettes om afslutning eller svigt af afviklingen med en meddelelse på ICM-modulet. Afviklingsbanker, der har adgang til TARGET2 via netværksleverandøren, skal efter anmodning have underretning om en afsluttet afvikling via en SWIFT MT 900 eller MT 910-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«

3) Punkt 11, nr. 5, affattes således:

- »5) Afviklingsbankerne og afviklingssystemerne skal have adgang til information via ICM-modulet. Afviklingssystemerne skal underrettes om afslutning eller svigt af gennemførelse af afviklingen. Der kan vælges enkelt eller en global notifikation. Afviklingsbanker skal efter anmodning underrettes om vellykket afvikling via en SWIFT MT 900 eller MT 910-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«

- 4) Punkt 12, nr. 9, affattes således:
- »9) Afviklingsbankerne og afviklingssystemerne skal have adgang til information via ICM-modulet. Afviklingssystemerne skal underrettes om afslutning eller svigt af afviklingen. Afviklingsbanker skal efter anmodning underrettes om vellykket afvikling via en SWIFT MT 900 eller MT 910-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«
- 5) Punkt 13, nr. 3, affattes således:
- »3) Afviklingsbankerne og afviklingssystemerne skal have adgang til information via ICM-modulet. Afviklingssystemerne skal underrettes om afslutning eller svigt af afviklingen. Afviklingsbanker skal efter anmodning underrettes om vellykket afvikling via en SWIFT MT 900 eller MT 910-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«
- 6) Punkt 14, nr. 2, affattes således:
- »2) Efter anmodning underrettes afviklingsbanker via en SWIFT MT 900 eller en MT 910-meddelelse og deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet om krediteringen og debiteringen af deres PM-konti og, hvis relevant, af deres afviklingskonti.«
- 7) Punkt 14, nr. 7), litra c), affattes således:
- »c) SWIFT-ordrer, som går via en MT 202-meddelelse eller ved automatisk »mapping« til MT 202 fra skærmene for deltagere, der anvender internetbaseret adgang, som kun kan afgives under forløbet af afviklingsprocedure 6 og kun under dagbehandling. Disse ordrer afvikles straks.«
- 8) I punkt 14, nr. 12, affattes andet afsnit således:
- »Det afviklingssystem, der har iværksat betalingsinstruksen, og det andet afviklingssystem skal underrettes, når afviklingen er gennemført. Afviklingsbanker skal efter anmodning underrettes om vellykket afvikling via en SWIFT MT 900 eller MT 910-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«
- 9) I punkt 14, nr. 13, affattes andet afsnit således:
- »Det afviklingssystem, der har iværksat betalingsinstruksen, og det andet afviklingssystem skal underrettes, når afviklingen er gennemført. Afviklingsbanker skal efter anmodning underrettes om vellykket afvikling via en SWIFT MT 900 eller MT 910-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«
- 10) I punkt 14, nr. 17, affattes andet afsnit således:
- »Det afviklingssystem, der har iværksat betalingsinstruksen, og det andet afviklingssystem skal underrettes, når afviklingen er gennemført. Afviklingsbanker skal efter anmodning underrettes om vellykket afvikling via en SWIFT MT 900 eller MT 910-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«
- 11) I punkt 14, nr. 18, affattes andet afsnit således:
- »Det afviklingssystem, der har iværksat betalingsinstruksen, og det andet afviklingssystem skal underrettes, når afviklingen er gennemført. Afviklingsbanker skal efter anmodning underrettes om vellykket afvikling via en SWIFT MT 900 eller MT 910-meddelelse. Deltagere, som anvender internetbaseret adgang, underrettes ved en meddelelse på ICM-modulet.«
-

BILAG II

Følgende indsættes som bilag V:

»BILAG V

SUPLERENDE OG ÆNDRERE HARMONISEREDE VILKÅR FOR DELTAGELSE I TARGET2 VED ANVENDELSE AF INTERNETBASERET ADGANG

Artikel 1

Anvendelsesområde

Vilkårene angivet i bilag II finder anvendelse på deltagere, der anvender internetbaseret adgang til en eller flere PM-konti, som er omfattet af bestemmelserne i dette bilag.

Artikel 2

Definitioner

Definitionerne i bilag II gælder ligeledes for dette bilag. Desuden forstås i dette bilag ved:

- »certificeringsmyndigheder«: en eller flere nationale centralbanker, som Styrelsesrådet har udnævnt hertil, hvorved de på Eurosystemets vegne kan udstede, forvalte, tilbagekalde og forny elektroniske certifikater
- »elektroniske certifikater« eller »certifikater«: en elektronisk fil, udstedt af certificeringsmyndighederne, der knytter en identitet til en offentlig nøgle, og som anvendes til: at kontrollere, at en offentlig nøgle tilhører en person, til at bekræfte indehaverens identitet, til at kontrollere en underskrift fra denne person eller til at kryptere en meddelelse adresseret til denne person. Certifikater opbevares på en fysisk anordning såsom et chipkort eller en USB-nøgle, og henvisninger til certifikater omfatter sådanne fysiske anordninger. Certifikaterne er en del af identitetprocessen ved deltagere, der har adgang til TARGET2 via internettet og afgiver betalingsmeddelelser eller kontrolmeddelelser
- »indehaver af certifikat«: en navngivet person, der af en TARGET2-deltager er identificeret og udpeget som indehaver af en tilladelse til at have internetbaseret adgang til deltagerens TARGET2-konto. Dennes anmodning om certifikater er først kontrolleret af deltagerens hjemmecentralbank og sendt til certificeringsmyndighederne, som herefter har udleveret certifikater, som knytter de beviser, som identificerer deltageren, til den offentlige nøgle
- »internetbaseret adgang«: hvor deltageren har valgt en PM-konto, som der kun er adgang til via internettet, og deltageren afgiver betalingsmeddelelser eller kontrolmeddelelser til TARGET2 ved brug af internettet
- »internetudbyder«: det selskab eller den organisation, dvs. den portal, som TARGET2-deltageren anvender for at få adgang til sin TARGET2-konto ved anvendelse af internetbaseret adgang.

Artikel 3

Uanvendelige bestemmelser

Følgende bestemmelser i bilag II finder ikke anvendelse vedrørende internetbaseret adgang:

Artikel 4, stk. 1, litra c), samt stk. 2, litra d), artikel 5, stk. 2, 3 og 4, artikel 6 og 7, artikel 11, stk. 8, artikel 14, stk. 1, litra a), artikel 17, stk. 2, artikel 23-26, artikel 41 og tillæg I, VI og VII.

Artikel 4

Supplerende og ændrede bestemmelser

Følgende bestemmelser i bilag II finder anvendelse vedrørende internetbaseret adgang som ændret som følger:

1) Artikel 2, stk. 1, affattes således:

»1. Følgende tillæg udgør en integrerende del af disse vilkår og finder anvendelse for deltagere, der har adgang til en PM-konto ved anvendelse af internetbaseret adgang:

Tillæg IA til bilag V: Tekniske specifikationer for behandling af betalingsordrer for internetbaseret adgang

Tillæg IIA til bilag V: Gebyrer og fakturering for internetbaseret adgang

Tillæg II: TARGET2 kompensationsordning

Tillæg III: Standard for afgivelse af responsa (legal opinion)

Tillæg IV, dog ikke stk. 7, litra b): Driftskontinuitet og nødprocedurer

Tillæg V: Driftsplan«

2) Artikel 3 ændres således:

a) Stk. 4 affattes således:

»4. [indsæt centralbankens navn] er leverandøren af ydelser i medfør af disse vilkår. Handlinger og undladelser fra centralbankerne, der er SSP leverandører, og/eller certificeringsmyndighederne skal anses som handlinger og undladelser begået af [indsæt centralbankens navn], og denne påtager sig ansvaret herfor i overensstemmelse med artikel 31 nedenfor. Deltagelse i henhold til disse vilkår udgør intet aftaleforhold mellem deltagerne og de centralbanker, som er SSP leverandører, når sidstnævnte handler i egenskab heraf. Instrukser, meddelelser og information, som en deltager modtager fra eller sender til den fælles platform vedrørende ydelser, som leveres ifølge disse vilkår, anses for modtaget fra og sendt til [indsæt centralbankens navn].«

b) Stk. 6 affattes således:

»6. Deltagelse i TARGET2 sker via deltagelse i et TARGET2 delsystem. Disse vilkår beskriver de gensidige rettigheder og forpligtelser for deltagere i TARGET2-[indsæt centralbank/landereference] og [indsæt centralbankens navn]. Reglerne for behandling af betalingsordrer (afsnit IV) omfatter alle betalingsordrer afgivet af eller betalinger modtaget af alle TARGET2-deltagere og gælder med forbehold af bilag V.«

3) Artikel 4, stk. 2, litra e), erstattes af følgende:

»e) kreditinstitutter eller en enhed opregnet under litra a)-c), og i begge tilfælde, hvor disse er etableret i et land, med hvilket Unionen har indgået en monetær aftale, der giver adgang for alle disse enheder til betalingssystemer i Unionen på de betingelser, som er fastsat i den monetære aftale, og forudsat det retlige system, som gælder i landet, svarer til den relevante EU-lovgivning.«

4) Artikel 8 ændres således:

a) stk. 1, litra a), punkt i), affattes således:

»1. For at kunne åbne en PM-konto i TARGET2-[indsæt centralbank/landereference], hvortil der er adgang over internettet, skal ansøgeren:

a) opfylde følgende tekniske krav:

i) installere, lede, drive og overvåge og sikre sikkerheden i den påkrævede IT-infrastruktur til opkobling til TARGET2-[indsæt centralbank/landereference] og afgive betalingsordrer til dette i overensstemmelse med de tekniske specifikationer i tillæg IA til bilag V. I forbindelse hermed kan ansøgeren om deltagelse inddrage tredjeparter, men bærer desuagtet selv ansvaret, og«

b) som stk. 1, litra c), indsættes:

»c) anføre, at de ønsker at have adgang til deres konto via internettet, og ansøge om en separat PM-konto i TARGET2, hvis de desuden ønsker adgang til TARGET2 via netværksleverandøren. Ansøgerne skal fremsende en korrekt udfyldt ansøgningsformular om udstedelse af de elektroniske certifikater, som kræves, for at de kan få adgang til TARGET2 med internetbaseret adgang.«

5) Artikel 9 ændres således:

a) Stk. 3 affattes således:

»3. Deltagere, der anvender internetbaseret adgang, må kun se TARGET2-registret online og må ikke distribuere det hverken internt eller eksternt.«

b) Stk. 5 affattes således:

»5. Deltagere anerkender, at [indsæt centralbankens navn] og andre centralbanker kan offentliggøre deltagernes navne og BIC-koder.«

6) Artikel 10 ændres således:

a) Stk. 1 og 2 affattes således:

»1. [indsæt centralbankens navn] skal tilbyde den i bilag V omhandlede internetbaserede adgang. Medmindre andet er bestemt i disse vilkår eller krævet i henhold til lov, skal [indsæt centralbankens navn] anvende alle til rådighed stående rimelige midler for at opfylde sine forpligtelser i henhold til disse vilkår, men uden at garantere et resultat.

2. Deltagere, der anvender internetbaseret adgang til TARGET2, betaler de gebyrer, som er fastsat i tillæg IIA til bilag V.«

b) Følgende indsættes som stk. 5:

»5. Deltagere skal både:

a) på alle bankdage, med regelmæssige mellemrum, aktivt kontrollere alle de informationer, som foreligger til dem på ICM-modulet, især informationer vedrørende vigtige systemrelaterede hændelser (f.eks. meddelelser vedrørende afvikling af afviklingssystemer) og hændelser vedrørende eksklusion eller suspension af en deltager. [indsæt centralbankens navn] kan ikke holdes ansvarlig for tab, direkte eller indirekte, som skyldes, at en deltager har undladt at foretage denne kontrol, og

b) til enhver tid både sikre overholdelse af sikkerhedskravene anført i tillæg IA til bilag V, navnlig hvad angår opbevaring af certifikater, og anvende regler og procedurer med henblik på at sikre, at indehavere af certifikater er bekendt med deres ansvar med hensyn til beskyttelsen af certifikaterne.«

7) Artikel 11 ændres således:

a) Følgende indsættes som stk. 5a:

»5a. Deltagere er ansvarlige for en rettidig ajourføring af blanketter til udstedelse af elektroniske certifikater, som kræves, for at der kan gives adgang til TARGET2 ved anvendelse af internetbaseret adgang, og for fremsendelsen af nye blanketter til udstedelse af sådanne elektroniske certifikater til [indsæt centralbankens navn]. Deltagere er ansvarlige for kontrol af nøjagtigheden af de oplysninger, som angår dem og som [indsæt centralbankens navn] har indlagt i TARGET2-[indsæt centralbank/landereference].«

b) Stk. 6 affattes således:

»6. [indsæt centralbankens navn] anses for at have fuldmagt til at udlevere alle oplysninger om deltagere, som certificeringsmyndighederne måtte have behov for, til disse myndigheder.«

8) Artikel 12, stk. 7, affattes således:

»7. [indsæt centralbankens navn] skal stille en daglig kontoopgørelse til rådighed for deltagere, som har valgt denne service.«

9) Artikel 13, litra b), affattes således:

»b) debiteringsinstrukser modtaget på grundlag af en debiteringsfuldmagt. Deltagere, der anvender internetbaseret adgang, må ikke kunne sende debiteringsinstrukser fra deres PM-konto, og«

10) Artikel 14, stk. 1, litra b) erstattes af følgende:

»b) betalingsmeddelelsen opfylder formateringsreglerne for TARGET2 [indsæt centralbank/landereference], herunder dobbeltordrekontrol beskrevet i tillæg IA til bilag V, og«

11) Artikel 16, stk. 2, affattes således:

»2. Deltagere, der anvender internetbaseret adgang, må ikke anvende AL-gruppefunktionaliteten vedrørende deres PM-konto med internetadgang, og må heller ikke kombinere deres PM-konto med internetadgang med eventuelle andre TARGET2-konti, som de er indehavere af. Der kan kun sættes limits i relation til en AL-gruppe som helhed. Der kan ikke sættes limits i relation til en enkelt PM-konto tilhørende et AL-gruppemedlem.«

12) Artikel 18, stk. 3, affattes således:

»3. Når Latest Debit Time Indicator anvendes, returneres den accepterede betalingsordre som uafviklet, hvis den ikke kan afvikles på det angivne debiteringstidspunkt. 15 minutter før det fastsatte debiteringstidspunkt skal den ordregivende deltager informeres via ICM-modulet i stedet for at få sendt en automatisk meddelelse via ICM-modulet. Den ordregivende deltager kan også anvende Latest Debit Time Indicator alene som en advarselsindikator. I disse tilfælde returneres den pågældende betalingsordre ikke.«

13) Artikel 21, stk. 4, affattes således:

»4. På anmodning fra en betaler kan [indsæt centralbankens navn] beslutte at ændre en meget hastende betalingsordres placering i køen (bortset fra meget hastende betalingsordrer i forbindelse med afviklingsprocedure 5 og 6), forudsat at denne ændring ikke påvirker den smidige afvikling i afviklingssystemer i TARGET2 eller på anden måde giver anledning til systemisk risiko.«

14) Artikel 28 ændres således:

a) Stk. 1 affattes således:

»1. Deltagere, der anvender internetbaseret adgang, skal indføre tilstrækkelige sikkerhedskontroller, især de sikkerhedskontroller, der er angivet i tillæg IA til bilag V, til beskyttelse af deres systemer mod uautoriseret adgang og benyttelse. Deltagerne er eneansvarlige for en tilstrækkelig beskyttelse af fortrolighed, pålidelighed og tilgængelighed vedrørende deres systemer.«

b) Følgende indsættes som stk. 4:

»4. Deltagere, der anvender internetbaseret adgang, skal straks informere [indsæt centralbankens navn] om enhver hændelse, der kan påvirke certifikaternes gyldighed, især de i tillæg IA til bilag V anførte hændelser, herunder uden begrænsninger ethvert tab eller misbrug.«

15) Artikel 29 erstattes af følgende:

»Artikel 29

Anvendelse af CM-modulet

1. ICM-modulet:

- a) giver deltagerne mulighed for at indgive betalinger
- b) giver deltagerne mulighed for adgang til information vedrørende deres konti og til styring af likviditet
- c) kan anvendes til at iværksætte likviditetsoverførselsordrer, og
- d) giver deltagerne adgang til systemmeddelelser.

2. Tillæg IA til bilag V indeholder yderligere tekniske detaljer om ICM-modulet, som anvendes i forbindelse med internetbaseret adgang«.

16) Artikel 32 ændres således:

a) Stk. 1 affattes således:

»1. Medmindre andet er bestemt i disse Vilkår stilles alle betalingsmeddelelser og meddelelser forbundet med betalingsbehandling i forbindelse med TARGET2, som f.eks. bekræftelser på debiteringer og krediteringer, og saldomeddelelser mellem [indsæt centralbankens navn] og deltagerne til rådighed for deltageren på ICM-modulet.«

b) Stk. 3 affattes således:

»3. Hvis en deltagers forbindelse svigter, skal deltageren anvende de alternative måder til overførsel af meddelelser, der er fastlagt i tillæg IA til bilag V. I disse tilfælde skal den gemte eller udprintede version af meddelelsen, som fremskaffes af [indsæt centralbankens navn], accepteres som dokumentation.«

17) Artikel 34, stk. 4, litra c), affattes således:

- »c) Så snart en sådan ICM-meddelelse er modtaget af deltagere, der anvender internetbaseret adgang, skal disse anses for at være underrettet om ophøret/suspenderingen af den pågældende deltagers deltagelse i TARGET2-[indsæt centralbank/landereference] eller et andet TARGET2-delsystem. Deltagerne bærer ethvert tab, der opstår som følge af afgivelse af en betalingsordre til deltagere, hvis deltagelse er suspenderet eller ophørt, såfremt denne betalingsordre blev indført i TARGET2-[indsæt centralbank/landereference], efter at ICM-meddelelsen blev stillet til rådighed.«

18) Artikel 39, stk. 1, affattes således:

- »1. Deltagere anses for at være bekendt med og skal handle i overensstemmelse med alle forpligtelser, der påhviler dem i forbindelse med lovgivning om personbeskyttelse, forebyggelse af hvidvaskning af penge og finansiering af terrorisme, spredningsfølsomme nukleare aktiviteter og udvikling af fremføringssystemer til kernevåben, i særdeleshed for så vidt angår gennemførelse af egnede foranstaltninger angående betalinger, som debiteres eller krediteres deres PM-konti. Inden deltagere, der anvender internetbaseret adgang, indgår kontraktforhold med en internetudbyder, skal de gøre sig bekendt med dennes politik for indhentning af data.«

19) Artikel 40, stk. 1, affattes således:

- »1. Medmindre andet er bestemt i disse vilkår, skal alle påkrævede eller tilladte meddelelser i henhold til disse vilkår sendes ved anbefalet brev, pr. telefax eller på anden måde skriftligt. Meddelelser til [indsæt centralbankens navn] sendes til lederen af [indsæt betalingssystemafdelingen eller den relevante centralbankenhed] i [indsæt centralbankens navn], [medtag den relevante adressat i centralbanken] eller til [indsæt centralbankens BIC-adresse]. Meddelelser til deltageren skal stiles til denne på den adresse, det faxnummer eller den SWIFT-adresse, som deltageren til enhver tid meddeler [indsæt centralbankens navn].«

20) Artikel 45 erstattes af følgende:

»Artikel 45

Gyldighed af enkelte bestemmelser

Hvis en bestemmelse i disse vilkår eller bilag V er eller bliver ugyldig, påvirker dette ikke gyldigheden af alle øvrige bestemmelser i vilkårene.«

Tillæg IA

TEKNISKE SPECIFIKATIONER FOR BEHANDLING AF BETALINGSORDRER FOR INTERNETBASERET ADGANG

I tillæg til de ensartede vilkår gælder følgende regler for behandlingen af betalingsordrer for internetbaseret adgang:

1. Tekniske krav for deltagelse i TARGET2 [indsæt centralbankens landerreference] med hensyn til infrastruktur, netværk og formater

- 1) Alle deltagere, der anvender internetbaseret adgang skal forbindes med ICM i TARGET2 ved hjælp af en lokal klient, operativsystem og internet browser som angivet i bilaget »Internetbaseret adgang — Systemkrav til internetadgang« i »User Detailed Functional Specifications« (UDFS) med de definerede opsætninger. Hver deltagers PM-konto identificeres ved en otte- eller 11-ciffer BIC-kode. Endvidere skal hver deltager bestå en række test til efterprøvning af dennes tekniske og operationelle formåen, for at få adgang som deltager i TARGET2 [centralbanken/landerreference].
- 2) Til brug for afgivelse af betalingsordrer og udveksling af betalingsmeddelelser i betalingsmodulet (Payments Module) anvendes TARGET2-plattformen BIC, TRGTXPMLVP, som meddelelsens afsender/modtager. Betalingsordrer afsendt til en deltager, der anvender internetbaseret adgang, bør angive den modtagende deltager i feltet til modtagende institution. Betalingsordrer afsendt af en deltager, der anvender internetbaseret adgang, angiver denne deltager som afgivende institution.
- 3) Deltagere der anvender internetbaseret adgang skal benytte public key infrastructure services som angivet i »User Manual Internetbased Access for the public-key certification service«.

2. Betalingsmeddelelestyper

- 1) Internetbaserede deltagere kan foretage følgende typer af betalinger:
 - a) kundebetaling, dvs kreditoverførsler, hvor den afgivende og/eller modtagende kunde ikke er en finansiel institution
 - b) kundebetaling, STP, dvs kreditoverførsler, hvor den afgivende og/eller modtagende kunde ikke er en finansiel institution, udført i »straight through processing mode«
 - c) bank-til-bank overførsler med anmodning om flytning af midler mellem finansielle institutioner
 - d) dækningsbetalinger med anmodning om flytning af midler mellem finansielle institutioner, der står i forbindelse med en underliggende kundes kreditoverførsel.

Derudover kan deltagere med internetbaseret adgang til en PM-konto modtage direkte debitordrer.

- 2) Deltagere skal følge feltspecifikationer, som er defineret i kapitel 9.1.2.2 i UDFS.
- 3) Indholdet af felter skal godkendes af TARGET2 [indsæt centralbanken/landerreference] i henhold til kravene i UDFS. Deltagere kan indbyrdes aftale særlige regler for indholdet af felter. TARGET2 [indsæt centralbanken/landerreference] foretager imidlertid ingen særlig kontrol af, om deltagere følger sådanne regler.
- 4) Deltagere der anvender internetbaseret adgang kan foretage dækningsbetalinger via TARGET2, dvs. betalinger der er foretaget af korrespondentbanker til at afvikle (dække) kreditoverførselsmeddelelser, der er fremsendt til en kundes bank på andre og mere direkte måder. Kundeoplysningerne i disse dækningsbetalinger vises ikke i ICM-modulet.

3. Dobbelt ordre kontrol

- 1) Alle betalingsordrer skal igennem en dobbeltordre kontrol, som har til formål at returnere betalingsordrer, som ved en fejl er afgivet mere end én gang.

2) Følgende felter i meddelelsetyperne kontrolleres:

Detaljer	Part of the message	Felt
Afsender	Basic Header	BIC Address
Meddelelsestype	Application Header	Meddelelsestype
Modtager	Application Header	Destination Address
Transaktion Reference Nummer (TRN)	Tekst Blok	:20
Relateret Reference	Tekst Blok	:21
Valør Dato	Tekst Blok	:32
Beløb	Tekst Blok	:32

3) Hvis felterne beskrevet i stk. 2 i forbindelse med en senere afgivet betalingsordre er identisk med felterne i en allerede accepteret betalingsordre, returneres den senere afgivne betalingsordre som uafviklet.

4. Fejlkoder

Hvis en betalingsordre returneres som uafviklet, afgives en fejlmeddelelse, som angiver årsagen til returneringen ved anvendelse af fejlkoder. Fejlkoderne er defineret i kapitel 9.4.2 i UDFS.

5. På forhånd fastsatte afviklingstidspunkter

- 1) For betalingsordrer, som anvender Earliest Debit Time Indicator, anvendes kodeordet »/FROTIME/«.
- 2) For betalingsordrer, som anvender Latest Debit Time Indicator, er der to mulige kodeord.
 - a) Kodeordet »/REJTIME/«: hvis betalingsordren ikke kan afvikles på det angivne debiteringstidspunkt, returneres betalingsordren som uafviklet.
 - b) Kodeordet »/TILTIME/«: hvis betalingsordren ikke kan afvikles på det angivne debiteringstidspunkt, returneres betalingsordren ikke, men opretholdes i den relevante kø.

I begge tilfælde bliver en meddelelse automatisk sendt via ICM, hvis en betalingsordre med Latest Debit Time Indicator ikke er afviklet 15 minutter forud for det deri angivne tidspunkt.

- 3) Hvis kodeordet »/CLSTIME/« er anvendt, behandles betalingen på samme måde som en betalingsordre, nævnt i stk. 2, litra b).

6. Afvikling af betalingsordrer i entry disposition

- 1) Der gennemføres modregningskontrol, og — hvis relevant — udvidet modregningskontrol (begge udtryk som defineret i stk. 2 og 3) af betalingsordrer, som er indført i entry disposition, for at sikre en hurtig og likviditetsbesparende bruttoafvikling af betalingsordrer.
- 2) En modregningskontrol skal fastslå, hvorvidt betalingsmodtagerens betalingsordrer, som er forrest i den meget hastende kø (highly urgent queue) eller, hvis ikke relevant, i den hastende kø (urgent queue), er til rådighed til modregning i betalerens betalingsordre (herefter: »modregnende betalingsordrer«). Hvis en modregnende betalingsordre ikke giver tilstrækkelige midler til den pågældende betalers betalingsordre i entry disposition, afgøres det, om der er tilstrækkelig likviditet til rådighed på betalerens PM-konto.

- 3) Hvis modregningskontrollen ikke lykkes, kan [indsæt centralbankens navn] anvende den udvidede modregningskontrol. Ved en udvidet modregningskontrol fastslås det, hvorvidt der er modregnede betalingsordrer til rådighed i nogen af betalingsmodtagerens køer, uden hensyn til, hvornår de kom i køen. Hvis der i betalingsmodtagerens kø er betalingsordrer med højere prioritet, som er adresseret til andre TARGET2 deltagere, kan FIFU-princippet dog kun fraviges, såfremt afvikling af en sådan modregnende betalingsordre vil medføre en likviditetsforøgelse for betalingsmodtageren.

7. Afvikling af betalingsordrer i køen

- 1) Behandlingen af betalingsordrer i kø, afhænger af den prioritetskategori, som den ordregivende deltager har angivet.
- 2) Betalingsordrer i den meget hastende og i den hastende kø afvikles ved anvendelse af modregningskontrollen beskrevet i stk. 6, idet der begyndes med betalingsordren forrest i køen i de tilfælde, hvor der sker en forøgelse af likviditeten, eller hvor der foretages indgriben i køen (ændring af placering i køen, afviklingstidspunkt eller -prioritet, eller tilbagekaldelse af betalingsordren).
- 3) Betalingsordrer i den normale kø afvikles løbende, herunder alle meget hastende og hastende betalingsordrer, som endnu ikke er afviklet. Der anvendes forskellige optimeringsmekanismer (algoritmer). Hvis en algoritme lykkes, bliver de omfattede betalingsordrer afviklet. Hvis en algoritme ikke lykkes, forbliver de omfattede betalingsordrer i køen. Der anvendes tre algoritmer (1 til 3) til modregning af betalingsstrømme. Afviklingsprocedure 5 (som denne er defineret i kapitel 2.8.1 i UDFS) kan — ved brug af algoritme 4 — anvendes til afvikling af afviklingssystemers betalingsordrer. For at optimere afviklingen af meget hastende transaktioner i afviklingssystemer på deltagerens afviklingskonti, anvendes en særlig algoritme (Algoritme 5).
 - a) I Algoritme 1 («all-or-nothing») skal [indsæt centralbankens navn] for såvel alle modpartsforhold, for hvilke der er fastsat et bilateralt limit, som for de summen af modpartsforhold, for hvilke der er fastsat et multilateralt limit:
 - i) beregne den samlede likviditetsposition for hver TARGET2 deltagers PM-konto ved at fastslå, hvorvidt den samlede sum af alle udgående og indgående betalingsordrer, som venter i køen, er negativ eller positiv, samt — såfremt den er negativ — kontrollere, om den overstiger den pågældende deltagers disponible likviditet (den samlede likviditet skal udgøre den »totale likviditetsposition«), og
 - ii) kontrollere, om limits og reserveringer, som er fastsat af hver TARGET2 deltager i relation til hver relevant PM-konto, overholdes.

Hvis resultatet af disse beregninger og kontroller er positivt for hver relevant PM-konto, skal [indsæt centralbankens navn] og andre centralbanker, som er involveret, afvikle alle betalinger samtidig på de pågældende TARGET2 deltagers PM-konti.

- b) Under Algoritme 2 («partial») skal [indsæt centralbankens navn]:

- i) beregne og kontrollere likviditetspositioner, limits og reservationer for hver relevant PM-konto, som under Algoritme 1, og
- ii) hvis den samlede likviditetsposition på én eller flere relevante PM-konti er negativ, udtage enkelte betalingsordrer, indtil den samlede likviditetsposition på hver relevant PM-konto er positiv.

Derefter skal [indsæt centralbankens navn] og de andre involverede centralbanker, i det omfang der er tilstrækkelige midler, afvikle alle tilbageværende betalinger (bortset fra de udtagne betalingsordrer) samtidig på de pågældende TARGET2 deltagers PM-konti.

Ved udtagelse af betalingsordrer, begynder [indsæt centralbankens navn] med den TARGET2 deltagers PM-konto, som har den største negative likviditetsposition, og med den betalingsordre bagest i køen, som har lavest prioritet. Algoritmen løber kun i kort tid, som nærmere fastsat efter [indsæt centralbankens navn]'s skøn.

- c) Under Algoritme 3 («multiple») skal [indsæt centralbankens navn]:

- i) sammenligne TARGET2 deltagers PM-konti parvis for at fastslå, hvorvidt betalingsordrer i kø kan afvikles inden for den likviditet, som er til rådighed for de pågældende to TARGET2 deltagers PM-konti, og inden for de fastsatte limits, (idet der begyndes med det PM-konti par med den mindste forskel mellem betalingsordrer, som er adresseret til hinanden), og de(n) centralbank(er), som er involveret, bogfører disse betalinger samtidig hos de to TARGET2 deltagers PM-konti, og

- ii) såfremt der for et par PM-konti, som beskrevet under punkt i), ikke er tilstrækkelig likviditet til at finansiere den bilaterale position, udtage enkelte betalingsordrer, indtil der er tilstrækkelig likviditet. I dette tilfælde afvikler de(n) centralbank(er), som er involveret, de tilbageværende betalinger, (bortset fra de udtagne) samtidig på de to TARGET2 deltageres PM-konti.

Efter gennemførelse af de kontroller, som er nævnt i underpunkt i) og ii), kontrollerer [indsæt centralbankens navn] de multilaterale afviklingspositioner (mellem en deltagers PM-konti og andre TARGET2 deltageres PM-konti, for hvilke der er sat multilaterale limits). Til brug herfor finder proceduren beskrevet i underpunkt i) til iii) tilsvarende anvendelse.

- d) Under Algoritme 4 («partial plus ancillary system settlement») følger [indsæt centralbankens navn] samme procedure som for Algoritme 2, men uden at udtage betalingsordrer, der relaterer sig til afvikling i et afviklingssystem (idet disse afvikles samtidig og multilateralt).
 - e) Under Algoritme 5 («ancillary system settlement via sub-accounts») følger [indsæt centralbankens navn] samme procedure som for Algoritme 1 med den ændring, at [indsæt centralbankens navn] starter Algoritme 5 via Ancillary System Interface og kun kontrollerer, hvorvidt der er tilstrækkelig midler til rådighed på deltagerens afviklingskonti. Der tages endvidere ikke hensyn til limits og reserveringer. Algoritme 5 løber også under natafvikling.
- 4) Betalingsordrer, som er indført i entry disposition efter påbegyndelse af en af algoritmerne 1-4, kan dog afvikles straks i entry disposition, hvis positionerne og limits for de pågældende TARGET2 deltageres PM-konti er forenelige både med afvikling af disse betalingsordrer og med afvikling af betalingsordrer i den løbende optimeringsprocedure. To algoritmer må dog ikke løbe samtidig.
 - 5) I dagfasen løber algoritmerne sekventielt. Så længe der ikke er en udestående samtidig multilateral afvikling i et afviklingssystem, er rækkefølgen følgende:
 - a) algoritme 1
 - b) hvis algoritme 1 ikke lykkes, så algoritme 2
 - c) hvis algoritme 2 ikke lykkes, så algoritme 3, eller hvis algoritme 2 lykkes, gentagelse af algoritme 1.

Når der udestår en samtidig multilateral afvikling («procedure 5») i et afviklingssystem, skal Algoritme 4 løbe.

- 6) Algoritmerne skal løbe fleksibelt ved forhåndsfastsættelse af en tidsforsinkelse mellem anvendelsen af forskellige algoritmer, for derved at sikre et minimumsinterval mellem gennemførelse af to algoritmer. Tidssekvensen kontrolleres automatisk. Der skal være mulighed for manuel indgriben.
- 7) Når en betalingsordre er indeholdt i en løbende algoritme, må den ikke ændres (ændring af placering i en kø) eller tilbagekaldes. Anmodninger om ændring eller tilbagekaldelse af en betalingsordre placeres i kø, indtil algoritmen er færdig. Hvis den pågældende betalingsordre afvikles som led i den løbende algoritme, afvises en anmodning om ændring eller tilbagekaldelse. Hvis betalingsordren ikke bliver afviklet, bliver deltagerens anmodning straks taget i betragtning.

8. Anvendelse af Informations- og kontrolmodulet ICM

- 1) ICM kan anvendes til afgivelse af betalingsordrer.
- 2) ICM kan anvendes til at erhverve information og styre likviditet.
- 3) Bortset fra betalingsordrer, som er warehoused, og statisk data information, er det kun data i forbindelse med den aktuelle bankdag, der er tilgængelige via ICM. Der tilbydes kun skærme på engelsk.
- 4) Information leveres i »pull« modus, dvs at hver deltager skal anmode om at få leveret information. Deltagere skal regelmæssigt i løbet af dagen kontrollere ICM for vigtige meddelelser.
- 5) Kun user-to-application modus (U2A) er til rådighed for deltagere, der anvender internetbaseret adgang. U2A muliggør direkte kommunikation mellem en deltager og ICM. Informationen vises i en browser, som kører på et PC-system. ICM User Handbook indeholder yderligere detaljer.

- 6) En deltager skal mindst have én arbejdsstation med internetadgang for at få adgang til ICM via U2A.
- 7) Adgangsrettigheder til ICM gives ved brug af certifikater, og brugen af disse er nærmere beskrevet i stk. 10-13.
- 8) Deltagere kan også anvende ICM til at overføre likviditet:
 - a) [indsæt hvis relevant] fra deres PM-konto til deres konto uden for PM-modulet
 - b) mellem PM-kontoen og deltagerens afviklingskonti, og
 - c) fra PM-kontoen til skyggekontoen, som administreres af afviklingssystemet.

9. UDSF og ICM User Handbook og »User Manual: Internet Access for the Public Key Certification Service«

Yderligere oplysninger og eksempler, som forklarer ovennævnte regler, findes i den til enhver tid gældende UDFS- og ICM User Handbook, der er offentliggjort på engelsk på [indsæt centralbankens navn]'s og ECB's websted og i »User Manual: Internet Access for the Public Key Certification Service«

10. Udstedelse, suspension, reaktivering, tilbagekaldelse og fornyelse af certifikater

- 1) Deltagere skal anmode [indsæt centralbankens navn] om udstedelse af certifikater, der giver dem mulighed for adgang til TARGET2 [indsæt centralbank/landereference] ved brug af internetbaseret adgang.
- 2) Deltagere skal anmode [indsæt centralbankens navn] om suspendering og reaktivering af certifikater samt tilbagekaldelse og fornyelse af certifikater, når en indehaver af certifikat ikke længere ønsker at have adgang til TARGET2, eller hvis deltageren ophører med sine aktiviteter i TARGET2-[indsæt centralbank/landereference] i overensstemmelse med de harmoniserede vilkår. (f.eks. som følge af fusion eller overtagelse).
- 3) Deltageren skal træffe alle sikkerhedsregler og organisatoriske foranstaltninger til sikring af, at certifikater kun anvendes i overensstemmelse med de harmoniserede vilkår.
- 4) Deltageren skal straks meddele [indsæt centralbankens navn] enhver væsentlig ændring af enhver oplysning i de formularer, som indsendtes til [indsæt centralbankens navn] i forbindelse med udstedelse af certifikater.
- 5) Deltageren kan højst have fem aktive certifikater til hver PM-konto. Efter anmodning kan [indsæt centralbankens navn] efter eget skøn ansøge om udstedelse af yderligere certifikater for certifikationsmyndighederne.

11. Deltagerens behandling af certifikater

- 1) Deltageren skal sikre, at alle certifikater opbevares sikkert, og foretage væsentlige organisatoriske og tekniske foranstaltninger således, at tredjeparter ikke lider skade, samt sikre at ethvert certifikat kun anvendes af den særlige indehaver, som det blev udstedt til.
- 2) Deltageren skal straks afgive alle de oplysninger, som [indsæt centralbankens navn] anmoder om samt garantere rigtigheden af disse. Deltagere bærer til enhver tid det fulde ansvar for, at de oplysninger, som de har afgivet til [indsæt centralbankens navn] i forbindelse med udstedelsen af certifikater, fortsat er korrekte.
- 3) Deltageren bærer det fulde ansvar for at sikre, at alle dennes indehavere af certifikater, opbevarer de certifikater, som de har fået tildelt, adskilt fra deres fra deres hemmelige PIN- og PUK-koder.
- 4) Deltageren bærer det fulde ansvar for at tilse, at ingen af dennes indehavere af certifikater benytter certifikaterne i funktioner eller til formål andre end dem, hvortil certifikaterne blev udstedt.
- 5) Deltageren skal straks give [indsæt centralbankens navn] oplysning om enhver anmodning om og begrundelse for suspendering, reaktivering, tilbagekaldelse eller fornyelse af certifikater.
- 6) Deltageren skal straks anmode [indsæt centralbankens navn] om at suspendere alle certifikater eller nøglerne, som er indeholdt i disse, som er mangelfulde, eller som indehaveren af certifikaterne ikke længere har i sin besiddelse.
- 7) Deltageren skal straks give [indsæt centralbankens navn] meddelelse om tab eller tyveri af certifikater.

12. Sikkerhedskrav

- 1) Det computersystem, som en deltager benytter for at få adgang til TARGET2 ved anvendelse af internetbaseret adgang, skal være tilstede på et forretningssted, som deltageren ejer eller lejer. Adgang til TARGET2-[indsæt centralbank/landereference] vil kun være tilladt fra dette forretningssted, og for at undgå tvivl vil fjernadgang ikke blive tilladt.
- 2) Deltageren skal køre al software på computersystemer, som er opstillet og tilpasset i overensstemmelse med gældende internationale it-sikkerhedsstandarder, der mindst skal omfatte de krav, der nærmere er beskrevet i artikel 12, stk. 3, og 13, stk. 4. Deltageren skal træffe passende foranstaltninger, herunder navnlig anti-virus og malware beskyttelse, anti-phishing foranstaltninger, procedurer til hærkning (hardening), og programrettelser (patch management). Deltageren skal regelmæssigt opdatere alle disse foranstaltninger og procedurer.
- 3) Deltageren skal oprette et krypteret meddelelseslink med TARGET2-[indsæt centralbank/landereference].
- 4) Brugerdrev på deltagerens arbejdsstationer må ikke have administratorrettigheder. Rettigheder skal tildeles i overensstemmelse med princippet om mindst mulig forret (least privilege).
- 5) Deltageren skal til enhver tid beskytte computersystemerne, der anvendes til TARGET2-[indsæt centralbank/landereference] internetadgang på følgende måde:
 - a) De skal beskytte computersystemerne og arbejdsstationerne mod uautoriseret adgang både fysisk og via netværk ved konstant brug af firewalls til at beskytte computersystemerne og arbejdsstationerne mod indkommende internettraffik, og arbejdsstationerne mod uautoriseret adgang over det interne netværk. De skal bruge en firewall, som beskytter mod indkommende trafik, samt en firewall på arbejdsstationer, som sikrer at kun autoriserede programmer kommunikerer udadtil.
 - b) Deltagere vil kun få tilladelse til at installere den software på arbejdsstationer, som er nødvendig for TARGET2, og som er autoriseret i henhold til deltagerens interne sikkerhedspolitik.
 - c) Deltagere skal til enhver tid sikre, at alle software applikationer, som kører på arbejdsstationerne, opdateres regelmæssigt og bliver programrettet (patched) med den seneste version. Dette gælder navnlig med hensyn til styresystemer, internetbrowseren og plug-ins.
 - d) Deltagere skal til stadighed begrænse udgående trafik fra arbejdsstationer til websteder, som er forretningsmæssig nødvendige, samt websteder, som kræves til lovlig og rimelig opdatering af software.
 - e) Deltagere skal sikre, at al nødvendig intern post ind og ud til arbejdsstationer er beskyttet mod videregivelse og skadelige ændringer, navnlig hvis filer overføres gennem et netværk.
- 6) Deltageren skal sikre, at indehavere af certifikater hos denne, til stadighed følger en sikker praksis med hensyn til browsing, herunder:
 - a) reservere visse arbejdsstationer til adgang til websteder af samme vigtighedsgrad og kun at åbne disse websteder fra disse arbejdsstationer,
 - b) altid at genstarte brugen af browseren før og efter at have åbnet TARGET2-[indsæt centralbank/landereference] gennem internetbaseret adgang,
 - c) kontrollere alle serveres SSL certifikat-godkendelse hver gang, der logges på TARGET2-[indsæt centralbank/landereference] internetbaseret adgang,
 - d) udvise mistænksomhed over for e-mails, som ser ud til at komme fra TARGET2-[indsæt centralbank/landereference], og aldrig udlevere certifikatets adgangskode, såfremt der spørges herom, idet TARGET2-[indsæt centralbank/landereference] aldrig spørger om certifikatets adgangskode i en e-mail eller på anden vis.
- 7) Deltageren skal til enhver tid gennemføre følgende ledelsesprincipper for at mindske risici for sit system:
 - a) indføre ledelsespraksis på brugerniveau, der sikrer, at der kun autoriserede brugere bliver oprettet og forbliver i systemet, samt vedligeholde en nøjagtig og opdateret liste over autoriserede brugere, og

- b) tilpasse den daglige betalingstrafik, således at forskelle afsløres mellem autoriseret og faktisk daglig betalings-traffik, såvel afsendt som modtaget
- c) sikre at en indehaver af et certifikat ikke browser på andre internetsteder samtidig med at denne åbner TARGET2-[indsæt centralbank/landereference].

13. Yderligere sikkerhedskrav

- 1) Deltageren skal til enhver tid ved brug af passende organisatoriske og/eller tekniske foranstaltninger sikre, at brugeres adgangskoder, der videregives til kontrol af adgangsrettigheder (Access Right Review), ikke misbruges og navnlig, at ingen ikke-autoriserede personer får kendskab til dem.
 - 2) Deltageren skal have indrettet en procedure til brugeradministration til sikring af, at såfremt en ansat eller anden bruger af et system på deltagerens forretningssted forlader deltagerens organisation, den tilhørende bruger adgangskode straks og varigt bliver slettet.
 - 3) Deltageren skal have indrettet en procedure til brugeradministration og skal straks og varigt blokere adgangskoder, som på en eller anden måde er videregivet, herunder tilfælde hvor certifikater er mistet eller stjålet, eller hvor adgangskoder er phished.
 - 4) Såfremt en deltager er ude af stand til at afhjælpe sikkerhedsmangler eller fejl ved konfigurationen (f.eks. som følge af systemer, der er smittet af malware), kan de centralbanker, som er SSP-leverandører, efter tre forekomster varigt blokere alle deltagerens brugeradgangskoder.
-

*Tillæg II A***GEBYROVERSIGT OG FAKTURERING FOR INTERNETBASERET ADGANG****Gebyrer for direkte deltagere**

1. Det månedlige gebyr for behandling af betalingsordrer i TARGET2-[indsæt centralbankens navn]/landereference] for direkte deltagere udgør 70 EUR pr. PM-konto for internetadgang samt 100 EUR pr. PM-konto samt et fast gebyr pr. transaktion (debit entry) på 0,80 EUR.
2. For direkte deltagere, som ikke ønsker BIC-koden for deres konto offentliggjort i TARGET2 registret, gælder et supplerende månedsgebyr på 30 EUR pr. konto.

Fakturering

3. For direkte deltagere gælder følgende regler for fakturering: Den direkte deltager modtager faktura for den foregående måned med opgørelse over de gebyrer, der skal betales, senest den femte bankdag i den følgende måned. Indbetaling skal ske senest den tiende bankdag i den pågældende måned på den konto, som er angivet af [indsæt centralbankens navn] og vil blive debiteret denne deltagers PM-konto.«
-