RAPPORT

DANMARKS NATIONALBANK

5. MAJ 2020 — NR. 3

Overvågning af den finansielle infrastruktur

- Danmark har en moderne, effektiv og robust betalingsinfrastruktur. Nationalbanken vurderer, at infrastrukturen i høj grad efterlever internationale standarders krav til organisering, risikostyring og beredskab.
- På tværs af infrastrukturens systemer og løsninger er der et stærkt ledelsesmæssigt fokus på at styrke cyberrobustheden. Modenheden i arbejdet er øget de seneste år med styrket risikostyring og deltagelse i de såkaldte TIBER-DK-cybertest.
- En del arbejde med cyberrobusthed sker på sektorniveau. Risikoanlysen fra FSOR (Finansielt Sektorforum for Operationel Robusthed) spiller sammen med risikoarbejdet hos de enkelte aktører, og FSOR's kriseberedskab sikrer koordination på tværs. Under covid-19-pandemien er beredskabet brugt til indhentning af information og videndeling.

Vigtig infrastruktur

618 mia. kr.

afvikles der i gennemsnit betalinger for hver bankdag

Læs mere

TIBER-DK-test af infrastrukturen

Etiske hackere

hjælper med at identificere forbedringsområder og styrke cyberrobustheden

Læs mere

INDHOLD

En moderne og robust betalingsinfrastruktur

Danmark er et af de mest digitaliserede lande i verden. Det gælder også på betalingsområdet, hvor borgere, virksomheder, finansielle institutter og offentlige myndigheder på en gennemsnitsdag sender elektroniske betalinger for over 600 mia. kr. gennem den danske betalingsinfrastruktur.

En velfungerende betalingsinfrastruktur er grundlaget for samfundsøkonomien. Virker tingene ikke, skaber det forstyrrelser, og i værste fald kan nedbrud i betalingsinfrastrukturen true den finansielle stabilitet. Derfor overvåger Nationalbanken, at infrastrukturens centrale systemer og løsninger efterlever internationale standarders krav til sikkerhed og effektivitet.

I denne rapport præsenteres de væsentligste konklusioner fra overvågningen af den danske betalingsinfrastruktur i 2019.

Den danske betalingsinfrastruktur er beskrevet i boks 1.

Internationale standarder efterleves i høj grad
Danmark har en moderne, effektiv og robust betalingsinfrastruktur. Det viser Nationalbankens overvågning.

Infrastrukturens systemer og løsninger kører stabilt, og der opleves kun sjældent forstyrrelser i udvekslingen af betalinger og afviklingen af værdipapir- og valutahandler.

De centrale systemer/løsninger efterlever i høj grad internationale standarder, som stiller krav til bl.a. organisering, risikostyring og beredskab. De ansvarlige for de centrale systemer/løsninger arbejder løbende med at øge robustheden og efterleve Nationalbankens anbefalinger til, hvordan infrastrukturen kan styrkes.

Nationalbankens overvågning

Nationalbanken overvåger, at betalinger og finansielle transaktioner i Danmark kan gennemføres sikkert og effektivt. Overvågningen omfatter de centrale systemer og løsninger i den danske betalingsinfrastruktur:

1. Kronos2 (interbankbetalinger)
2. Sum-, Intradag- og Straksclearingen (detailbetalinger)
3. VP-afviklingen (værdipapirhandler)
4. Dankort, Betalingsservice og konto til konto-overførsler (de vigtigste betalingsløsninger)
5. Internationale systemer, der har relevans i Danmark.

Nationalbankens overvågning sker med udgangspunkt i internationale standarder og retningslinjer og er beskrevet i bankens overvågningspolitik (*link*).

På tværs af systemer og løsninger er der i 2019 bl.a. arbejdet med at styrke risikostyringen og rapporteringen af risici. Herunder er der især fokus på at styrke leverandørstyringen og risikorapporteringen fra leverandør til systemejer. Endvidere er risici ved gensidige afhængigheder mellem de centrale systemer i infrastrukturen nu systematisk indarbejdet i risikostyringen for de enkelte systemer.[1]

Ved at indarbejde risici fra leverandører og forbundne systemer i egen risikostyring skabes et samlet overblik og et godt grundlag for at prioritere og adressere risici. Det er et centralt element i CPMI-IOSCO-principperne at styre både risici, man påføres af andre, og risici man påfører andre aktører. Og det er et centralt element i at skabe et robust samspil mellem infrastrukturens aktører.

Cybertruslen skærper kravene til infrastrukturen
Truslen fra cyberkriminalitet stiller fortsat skærpede krav til infrastrukturens robusthed. Cyberrobusthed

1 Risici ved gensidige afhængigheder identificeres i Risikoforum for Gensidige Afhængigheder (RGA), der er et formaliseret samarbejde mellem Nationalbanken, VP og Finans Danmark. For en beskrivelse af RGA henvises til Danmarks Nationalbank, Overvågning af den finansielle infrastruktur, *Danmarks Nationalbank Rapport* nr. 3, juni 2019. (*Link*).

Betalingsinfrastrukturen i Danmark

Boks 1

Hver bankdag[1] sendes i gennemsnit betalinger for 618 mia. kr. gennem den danske betalingsinfrastruktur, svarende til lidt over en fjerdedel af BNP.

Nationalbankens betalingssystem, Kronos2, har en central rolle i infrastrukturen, både ved afvikling af store, tidskritiske betalinger mellem banker (interbankbetalinger) og i kraft af Nationalbankens rolle som afviklingsbank for de øvrige betalings- og afviklingssystemer. I Kronos2 afvikles dagligt interbankbetalinger for 87 mia. kr.

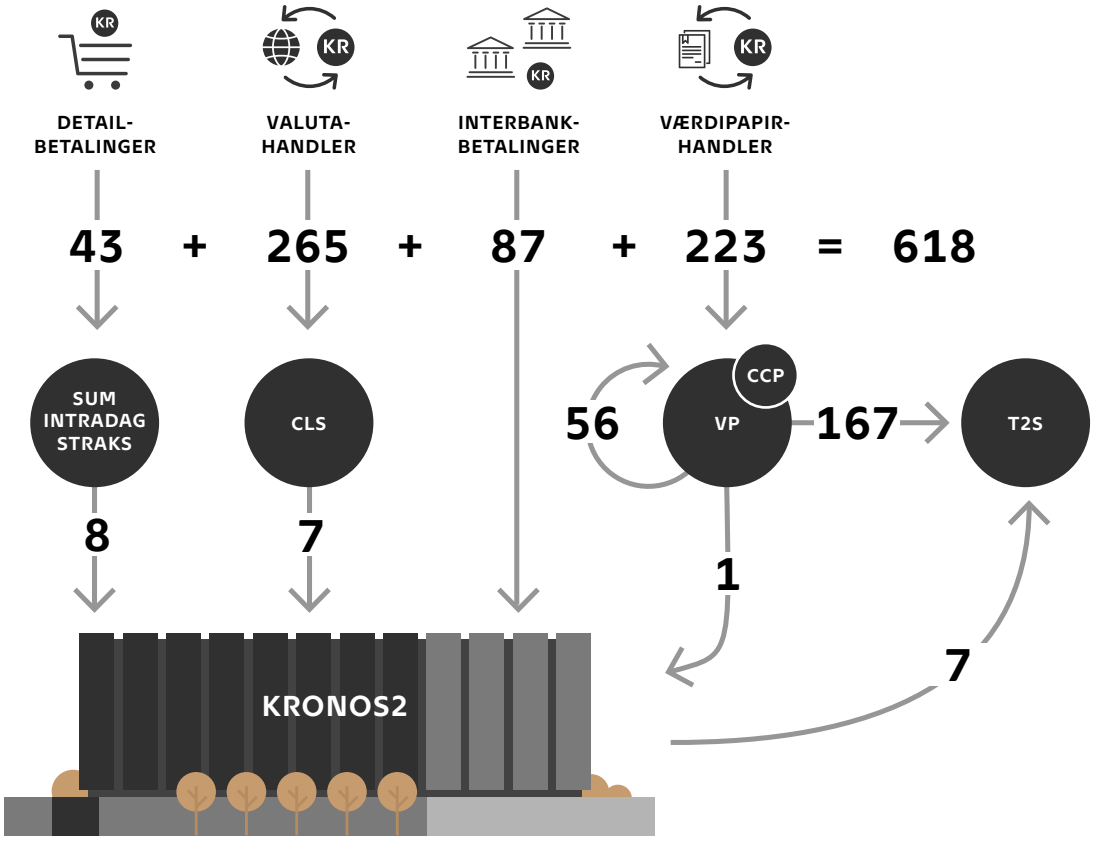
Detailbetalinger er betalinger mellem borgere, virksomheder og offentlige myndigheder, fx ved brug af Dankort eller konto til konto-overførsler. Detailbetalinger cleares og afvikles alt efter type i Sum-, Intradag- eller Straksclearingen (detailbetalingssystemerne).

Valutahandler i CLS omfatter bl.a. FX spot, FX forward og FX swaphandler.

Værdipapirhandler i VP omfatter handler med obligationer, aktier og investeringsbeviser. Hovedparten af værdipapirafviklingen, svarende til 167 mia. kr., sker på den fælleseuropæiske platform Target2-Securities (T2S), resten, dvs. 56 mia. kr., afvikles på VP's egen platform. Nogle værdipapirhandler, fx aktiehandler, cleares gennem en såkaldt central modpart (central counterparty, CCP).

Betalings- og afviklingssystemerne i infrastrukturen, dvs. CLS, VP og de tre detailbetalingssystemer afvikler deres deltageres nettopositioner i Kronos2 eller T2S. Nettopositionerne beregnes i de respektive systemer ved at modregne deltagernes tilgodehavender og forpligtelser. Denne netting reducerer deltagernes likviditetsbehov til afviklingen betydeligt sammenlignet med en situation, hvor alle betalinger afvikles enkeltvist, fx reducerer netting likviditetsbehovet til afvikling af detailbetalinger fra 43 mia. kr. til 8 mia. kr. dagligt, svarende til en reduktion på 81 pct. Ligeledes reducerer netting deltagernes likviditetsbehov til afviklingen på T2S fra 167 mia. kr. til 7 mia. kr., hvilket svarer til en reduktion på 96 pct.

Betalingsflow, mia. kr., gennemsnit pr. bankdag i 2019



1. Nogle typer betalinger kan foretages på alle dage og tidspunkter, andre kun når bankerne har åbent. Fælles for alle betalinger er, at den endelige afvikling og udveksling af beløb mellem bankerne sker på bankdage, dvs. dage, hvor bankerne har åbent.

omfatter både evnen til at beskytte sine systemer mod angreb, opdage eventuel indtrængen i systemerne og ikke mindst at kunne genoprette driften med korrekte data efter et cyberangreb.

Nationalbankens overvågning er løbende i dialog med de ansvarlige for de centrale systemer i infrastrukturen om deres arbejde på cyberområdet. I 2019 har Nationalbanken arbejdet med at vurdere systemerne efter særlige internationale retningslinjer, som fokuserer på cybersikkerhed, se boks 2.

Arbejdet med cyberrobusthed
Der er på tværs af systemer og løsninger et stærkt ledelsesmæssigt fokus på at styrke cyberrobustheden, og modenheden i arbejdet er øget de seneste år. Den styrkede risikostyring og risikorapportering afspejler dette. Og der arbejdes følgelig med løbende at mitigere de identificerede risici, herunder cyberrisici.

En del af arbejdet med at mitigere cyberrisici og øge cyberrobustheden sker på sektorniveau og ved at deltage i forskellige sektorsamarbejder, jf. nedenfor.

FSOR og FSOR-risikoanalyse
De ansvarlige for de centrale systemer og løsninger deltager i FSOR, Finansielt Sektorforum for Operationel Robusthed, der siden 2016 har arbejdet med forskellige aspekter af cyberrobusthed.

I FSOR-regi er der udviklet en metode for løbende risikoanalyse på sektorniveau. Analysen sikrer et fælles overblik over operationelle risici, der kan ramme på tværs af sektoren og potentielt true den finansielle stabilitet. På baggrund af risikoanalysen kan fælles risici adresseres i fællesskab. Ved at tage udgangspunkt i en systematisk risikoanalyse sikres det, at der løbende arbejdes med det, der giver størst værdi.

FSOR's risikoarbejde spiller sammen med og understøtter risikoarbejdet i både Risikoforum for Gensidige Afhængigheder (RGA) og hos de enkelte aktører. Fx er der i FSOR særlig fokus på at inddrage leverandørerne af infrastrukturen. Der er indledt dialog med de mest kritiske leverandører for at opnå en fælles forståelse for de gensidige afhængigheder og de risici, der kan opstå i den forbindelse. Arbejdet i FSOR understøtter på den måde de enkelte aktøres arbejde med leverandørstyring.

Med FSOR's risikoanalyse er der skabt et unikt samspil mellem risikoarbejdet hos de enkelte aktører, risikoarbejdet i RGA og på sektorniveau. Det betyder, at en risiko kan adresseres på flere niveauer på samme tid. FSOR har også mulighed for at eskalere en risiko til nationalt niveau, hvis risikoen vedrører flere samfundskritiske sektorer og derfor bedst imødegås på nationalt plan. FSOR-risikoanalysen er – så vidt vides – den første af sin art i verden.

TIBER-DK
Test er et vigtigt redskab i arbejdet med at styrke cybersikkerheden. Ved løbende at teste systemer, procedurer og planer identificeres konkrete forbedringsområder hos den, som testes. De ansvarlige for infrastrukturens centrale systemer og løsninger deltager i TIBER-DK, der er et dansk Threat Intelligence Based Ethical Red-teaming-testprogram, se boks 3. I en TIBER-test udsættes deltagernes

Vurdering af Cyberrobusthed Boks 2

Nationalbankens vurdering af de centrale systemers cyberrobusthed sker efter CPMI-IOSCO's Guidance on cyber resilience for financial market infrastructure (CPMI-IOSCO's cyber guidance).[1]

CPMI-IOSCO's cyber guidance blev offentliggjort i 2016 og er et sæt retningslinjer, der uddyber CPMI-IOSCO's Principles for financial market infrastructures fra 2012 – i særdeleshed vedrørende princip 2 (governance), princip 3 (framework for the comprehensive management of risks) og princip 17 (operational risk).

Retningslinjerne er organiseret i fem hovedområder:
1. organisering og styring
2. identificering af risici
3. beskyttelse mod angreb
4. opdagelse af angreb
5. genoprettelse af normal drift.

Dertil er der tre tværgående områder vedrørende test, læring og udvikling samt bevågenhed.

ECB offentliggjorde i 2018 sine forventninger til Cyberrobusthed i kritisk infrastruktur i Cyber resilience oversight expectations (CROE).[2] CROE er et supplement til CPMI-IOSCO's cyber guidance og anvendes af ECB ved vurdering af Eurosystemets kritiske infrastrukturer.

CROE kan være en nyttig vejledning til, hvordan de danske systemers cyberrobusthed kan styrkes og samtidig sikre en høj efterlevelse af CPMI-IOSCO's cyber guidance.

1. CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures (*Link*).
2. ECB, Cyber resilience oversight expectations (*Link*).

live-systemer for et simuleret cyberangreb med det formål at finde og udbedre sårbarheder, inden de udnyttes af cyberkriminelle.

NFCERT og CIISI-EU

Videndeling er et andet vigtigt element i bekæmpelsen af cyberkriminalitet. De centrale systemer/løsninger i infrastrukturen deltager alle i Nordic Financial CERT, NFCERT, der er et fælles nordisk sektorsamarbejde om indsamling og deling af information om cybertrusler og cyberangreb.[2] Videndelingen har til formål at styrke mulighederne for at opdage, forhindre og respondere hurtigere på et cyberangreb. NFCERT yder også ekspertbistand i tilfælde af cyberangreb.

Nationalbanken deltager endvidere i CIISI-EU (Cyber Information and Intelligence Sharing Initiative), der er et nyt offentligt/privat videndelingsinitiativ mellem centrale finansielle aktører i Europa, Europol og European Union Agency for Cybersecurity (ENISA). Initiativet har fællestræk med NFCERT, men går på nogle punkter videre.

FSOR-kriseberedskab

FSOR har etableret Den Finansielle Sektors Kriseberedskab, der kan aktiveres ved alvorlige operationelle hændelser, som fx et cyberangreb. Beredskabet skal sikre en koordineret indsats på tværs af sektoren og har også kontakt til NOST, den Nationale Operative Stab, så indsatsen kan koordineres på tværs af samfundskritiske sektorer.

Beredskabet testes flere gange årligt. Det giver deltagerne, herunder de ansvarlige for de kritiske systemer/løsninger mulighed for at teste og forbedre egne beredskaber.

Under covid-19-pandemien har FSOR kriseberedskabet været effektivt til at sikre videndeling og koordination mellem NOST og den finansielle sektor. Information fra NOST er blevet delt med FSOR-medlemmerne to gange ugentligt via beredskabets virtuelle platform, og der er dagligt indhentet information om medarbejdersituationen i de kritiske funktioner i infrastrukturen, som er videregivet til NOST.

TIBER-DK Boks 3

Nationalbanken er myndighed for TIBER-DK-programmet (Threat Intelligence Based Ethical Red-teaming) og har i tæt samarbejde med den danske finansielle sektor udarbejdet TIBER-DK-rammeværket baseret på TIBER-EU.

Rammeværket beskriver, hvordan deltagerne på en etisk, forsvarlig og ensartet måde kan finde sårbarheder i deres kritiske funktioner med henblik på at lære, hvordan cyberrobustheden kan forbedres. Da videndeling blandt deltagerne er en integreret del af TIBER-DK-rammeværket, vil deltagerne både lære af egne og andres test.

TIBER-DK-testen er målrettet de funktioner, som er kritiske både for den enkelte deltager og for samfundet, og testen favner mennesker, processer og systemer. I testen gennemfører et red team (hacker-team) kontrollerede, simulerede angreb på disse kørende, kritiske funktioner. Angrebene er realistiske, da de tager udgangspunkt i efterretningsbaseret trusselsinformation og efterligner aktuelle trusselsaktører og deres anvendte taktikker, teknikker og procedurer.

I forberedelsen og gennemførelsen af en TIBER-DK-test er der fokus på risikostyring for at sikre, at testene gennemføres på en forsvarlig måde. Ligeledes er der i TIBER-DK-rammeværket anvisninger til, hvordan fortroligheden omkring testen og resultaterne bevares.

Under TIBER-DK-programmet testes de største finansielle institutioner, infrastrukturvirksomheder og datacentraler i Danmark.

Udvikling af infrastrukturen

Betalingsinfrastrukturen moderniseres og udvikles løbende. I 2018 implementerede Nationalbanken et nyt, tidssvarende RTGS-system, Kronos2, og afvikling af værdipapirhandler i kroner blev tilsluttet Target2-Securities (T2S). På eurosiden har ECB siden 2016 arbejdet på at konsolidere T2S, Target2 og TIPS på en fælles platform.

I 2019 er også de danske detailbetalingssystemer kommet i spil: På den korte bane ønsker Mastercard at købe bl.a. Betalingsservice og detailclearingerne af Nets. Samtidig arbejder en række nordiske banker på at etablere P27, som er en ny fælles infra-

2 NFCERT har deltagere fra alle fem nordiske lande. De fleste norske og danske banker deltager i NFCERT.

struktur til clearing og afvikling af detailbetalinger i og mellem Danmark, Sverige og Finland.

I april 2020 har Euronext og VP Securities' (VP's) største aktionærer indgået aftale om, at Euronext køber aktiemajoriteten i VP.

De forskellige projekter er beskrevet nærmere i rapportens afsnit om overvågningen af de enkelte betalings- og afviklingssystemer.

Interbankbetalinger

Interbankbetalinger er betalinger mellem finansielle institutter. Betalingerne er typisk karakteriserede ved at være tidskritiske og af høj værdi. De afvikles i realtidsbruttoafviklingssystemer, RTGS-systemer, som afvikler betalinger enkeltvist og øjeblikkeligt.

Kronos2 er Nationalbankens RTGS-system for interbankbetalinger i danske kroner. I Kronos2 afvikles foruden interbankbetalinger også pengepolitiske operationer og nettopositioner fra tilsluttede betalings- og afviklingssystemer.

Brug
I Kronos2 er der 94 direkte deltagere. Deltagerne er primært danske banker, realkreditinstitutter og filialer af udenlandske banker.

I 2019 blev der i gennemsnit pr. bankdag gennemført ca. 5.800 interbankbetalinger i Kronos2 med en samlet værdi på 87,4 mia. kr., jf. tabel 1.

Som følge af overgangen til Kronos2 i august 2018 er der sket et markant fald i overførsler til Sum-, Intradag- og Straksclearingen, jf. tabel 1. I 2017 blev der overført 273,8 mia. kr., mens det i 2019 var 40,5 mia. kr. Tidligere blev hele deltagerens disponible foliolikviditet overført til nattens afviklinger ved funktionen "Mest muligt". Med Kronos2 hentes der automatisk den nødvendige likviditet til de natlige afviklinger i Sum- og Intradagclearingen.

Tilslutningen af danske kroner til Target2-Securities (T2S) i oktober 2018 har også haft betydning for afviklingen i Kronos2. Efter tilslutningen er de professionelle aktørers afvikling flyttet til T2S, mens de private investorers handler fortsat afvikles på VP's egen platform. Afviklingen i nettopositioner fra VP-afviklingen er faldet fra 10,1 mia. kr. i 2017 til 1,0 mia. kr. i 2019.

Transaktioner i Kronos2 Tabel 1

Mia. kr., gennemsnit pr. bankdag	2015	2016	2017	2018	2019
Interbankbetalinger	**99,3**	**83,0**	**74,0**	**83,0**	**87,4**
- Heraf kundebetalinger	12,8	11,5	11,5	13,6	14,0
Pengepolitiske operationer	**37,5**	**28,7**	**39,9**	**36,9**	**48,4**
- Heraf salg af indskudsbeviser	37,3	28,6	39,9	36,9	48,4
- Heraf pengepolitiske udlån	0,2	0,1	0,0	0,0	0,0
Overførsler til afviklingssystemer	**379,9**	**283,4**	**316,3**	**237,3**	**115,1**
- Heraf til Sum-, Intradag- og Straksclearingen	334,9	242,7	273,8	177,2	40,5
- Heraf til VP-afviklingen	35,5	31,7	32,5	40,6	46,4
- Heraf til CLS	9,6	9,0	10,0	19,6	28,2
Afviklede nettopositioner	**27,6**	**25,1**	**24,8**	**24,1**	**16,3**
- Heraf Sum-, Intradag- og Straksclearingen	7,6	7,6	8,0	8,1	8,3
- Heraf VP-afviklingen	12,7	10,6	10,1	9,1	1,0
- Heraf CLS	7,2	6,9	6,7	6,8	7,0

Driftsstabilitet
I 2019 har driftsstabiliteten i Kronos2 overordnet set været tilfredsstillende. Der har kun været få hændelser, som har skyldtes operationelle fejl og det komplekse samspil med de øvrige systemer i infrastrukturen. Årsagerne til hændelserne er blevet identificeret, og der er fulgt op med tiltag, der skal forebygge, at det samme sker igen.

Likviditet
Deltagerne har som helhed haft rigelig likviditet til at gennemføre deres betalinger i Kronos2. Figur 1 viser deltagernes likviditetsmæssige overdækning.

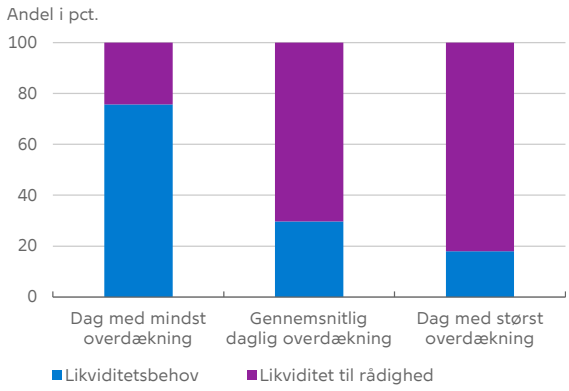
Den rigelige likviditet blandt deltagerne i Kronos2 medvirker til, at afviklingen af betalinger foregår uden problemer. En stresstestanalyse af likviditeten baseret på data fra Kronos i perioden 2. januar 2007 til 3. august 2018 viser, at betalingsafviklingen og deltagernes likviditet var robust over for forskellige former for stress.[3] Likviditeten i Kronos er bl.a. blevet testet i et scenario, hvor en stor deltager udgår af betalingsafviklingen og i et, hvor deltagernes intradagkredit begrænses. Data fra Kronos2 viser, at deltagernes betalingsadfærd har ændret sig en smule, men der er fortsat rigelig likviditet.

Internationale standarder
Nationalbanken arbejder løbende med at efterleve internationale standarder for sikre og effektive betalingssystemer.

Ved at gennemføre jævnlige stresstest, som beskrevet ovenfor, efterlever Nationalbanken CPMI-IOSCO's krav om at udføre stresstest af likviditeten i systemet.

Nationalbanken har i 2019 styrket styring og rapportering af risici i relation til Kronos2. Der er bl.a. indført øget systematik og et skærpet fokus på risici hos kritiske leverandører. Endvidere er risici, identificeret i samarbejde med VP og Finans Danmark, blevet indarbejdet i risikostyringen af Kronos2. Tiltagene følger op på konklusionerne fra en gennemgang af risikostyringen af Kronos2 i 2018 efter CPMI-IOSCO's krav til rammer for risikostyring.

Rigelig likviditet blandt deltagerne i Kronos2 i 2019 Figur 1



Kilde: Danmarks Nationalbank.

Endvidere har Nationalbanken i 2019 igangsat en vurdering af Kronos2 efter samtlige CPMI-IOSCO's principper. Den omfatter alle områder af Kronos2, herunder det juridiske grundlag, den overordnede organisering, og den nærmere styring af alle former for risici, der kan opstå i forbindelse med betalingsafvikling i Kronos2.

Cyberrobusthed
Nationalbanken følger løbende udviklingen i trusselsbilledet og har i 2019 fortsat arbejdet med at styrke cyberrobustheden. Herunder er der arbejdet med at efterleve de skærpede krav i SWIFT Customer Security Programme (CSP) og med at implementere CPMI's endpoint security strategy[4].

Nationalbanken har bl.a. implementeret et værktøj, der skal opdage, hvis en betalingsinstruktion i Kronos2 afviger fra det normale betalingsmønster. Tiltaget skal være med til at reducere risikoen for kriminelle transaktioner i Kronos2. Endvidere er sikkerheden omkring de it-systemer, der er forbundet med Kronos2, blevet styrket. Nationalbanken efterlever dermed alle krav i SWIFT CSP og ECB's Connectivity Guide. Samtidig er der øget fokus på løbende awareness-kampagner, der har til formål at uddanne i cyber- og it-sikkerhed. Uddannelse af medarbejdere er et vigtigt element i cybersikkerhed.

3 Jf. Thomas Christian Nilsson, Likviditetsstresstest viser, at Kronos er robust, *Danmarks Nationalbank Analyse,* nr. 9, maj 2019 (*Link*).

4 CPMI, Reducing the risk of wholesale payments fraud related to endpoint security (*Link*).

Nationalbanken ser derudover på, hvilke krav der kan stilles til deltagernes endpoint-sikkerhed[5]. Et betalingssystems robusthed mod kriminelle transaktioner afhænger både af sikkerheden i selve systemet og af deltagernes sikkerhed. Derfor er det centralt i CPMI's strategi, at ejere af betalingssystemer stiller passende krav til deltagerne om at implementere sikkerhedstiltag ved de endpoints, de kontrollerer.

Systemændringer

Nationalbanken arbejder løbende med at styrke robustheden i sine systemer. Bl.a. arbejdes der med at styrke den eksisterende Extreme Contingency løsning, der sikrer afvikling af betalinger, i tilfælde af at Kronos2 rammes af en større hændelse eller nedbrud. Der planlægges test af løsningen med den finansielle sektor i løbet af 2020.

5 Et betalingssystem er forbundet med andre finansielle infrastrukturer, serviceleverandører og deltagere (dvs. banker og andre finansielle institutioner) via netværk til at sende meddelelser. Tilsammen udgør disse parter og tilhørende netværk et komplekst "økosystem" til at afvikle betalinger. Et endpoint er i CPMI's terminologi defineret som et punkt i økosystemet, hvor betalingsinstrukser udveksles mellem to parter i økosystemet.

Detailbetalinger

De fleste betalinger mellem borgere og virksomheder sker elektronisk med betalingsløsninger som fx Dankort, netbankoverførsler, Betalingsservice og MobilePay. I 2019 blev der i gennemsnit gennemført elektroniske detailbetalinger for 29,1 mia. kr. pr. dag.[6] Nationalbanken overvåger de betalingsløsninger, der har størst betydning i Danmark, jf. boks 4.

Driftsstabilitet
I 2019 har driftsstabiliteten i de systemer, som ligger til grund for Dankort og Betalingsservice, været tilfredsstillende.

En enkelt konkret hændelse i marts 2019, som opstod på grund af en operationel fejl, fik imidlertid konsekvenser for en del Dankortbetalinger. Betalingerne blev gennemført uden problemer i forretningerne, men blev ikke sendt til clearing og afvikling. Cirka en fjerdedel af alle Dankortbetalinger under hændelsen blev derfor indsat på forretningernes konti med nogle dages forsinkelse. Nets har efterfølgende sikret, at de tekniske forhold, som forårsagede hændelsen, ikke gentager sig.

Nets' salg af Betalingsservice til Mastercard
I august 2019 indgik Nets og Mastercard en aftale om, at Mastercard køber bl.a. detailclearingerne og Betalingsservice af Nets.

Handlen er betinget af konkurrencemyndighedernes godkendelse. Handlen er anmeldt til Konkurrence- og Forbrugerstyrelsen (KFST), der efter en række undersøgelser har oversendt sagen til behandling hos EU-Kommissionen.

Godkendes handlen, vil Nets og Mastercard indgå en midlertidig serviceaftale, der skal være med til at sikre en smidig, sikker og stabil overdragelse af driften af Betalingsservice fra Nets til Mastercard. Efter overtagelsen vil Mastercard i en længere periode have mulighed for at få bistand fra Nets i forhold til at understøtte driften af Betalingsservice.

Nationalbanken følger løbende processen omkring Nets' salg af Betalingsservice til Mastercard. Over-

6 Værdien af transaktionerne i detailbetalingssystemerne opgjort pr. kalenderdag, jf. afsnittet *Clearing og afvikling af detailbetalinger*.

Nationalbankens overvågning af betalingsløsninger Boks 4

Nationalbanken overvåger de vigtigste danske betalingsløsninger. På nuværende tidspunkt omfatter overvågningen Dankort, Betalingsservice og konto til konto-overførsler.

Overvågningen af Dankort omfatter både de rene Dankort og Dankort-siden af de co-brandede Dankort (primært Visa/Dankort).

Overvågningen af konto til konto-overførsler indgår som en del af overvågningen af detailbetalingssystemerne (Sum-, Intradag- og Straksclearingen), jf. afsnittet *Clearing og afvikling af detailbetalinger*.

Udviklingen i de forskellige andre betalingsløsninger på det danske marked følges løbende for at vurdere, om der er behov for målrettet overvågning af dem.

MobilePay bruges primært til overførsler mellem privatpersoner, men bruges også til fx handel i butikker, køb på internettet og betaling af faste regninger. Den gennemsnitlige daglige omsætning for MobilePay var på 0,3 mia. kr. i 2019.[1] Til sammenligning lå Dankort i 2019 på 1,1 mia. kr. pr. dag.[2]

De nye betalingsløsninger på det danske marked, Apple Pay og Google Pay, har endnu kun en ganske begrænset markedsandel.

1. MobilePay, (*Link*).
2. Nets' statistik for misbrug af Dankort, (*Link*).

vågningen af Betalingsservice vil blive rettet mod Mastercard, når overtagelsen er gennemført.

Misbruget af Dankort er fortsat faldende

I 2019 lå misbruget af Dankort ifølge Nets på 30,9 mio. kr. Dette svarer til 0,08 promille af det samlede forbrug med Dankort.[7] Dermed fortsætter de seneste års positive udvikling med faldende misbrug, jf. figur 2. Misbruget er faldende både ved køb på nettet, ved handel i butikker og ved kontanthævninger.

Misbruget af stjålne eller tabte Dankort til at handle i butikker eller hæve kontanter er faldet med 25 pct. fra 2. halvår af 2018 til 2. halvår 2019, hvor misbruget udgjorde 0,049 promille.[8]

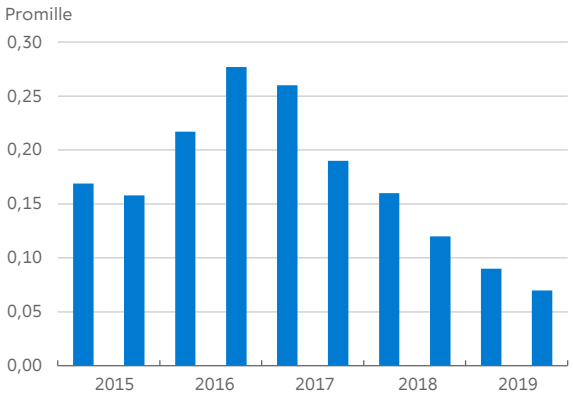
Politiet og Nets samarbejder for at forhindre misbrug med stjålne kort. De har i fællesskab identificeret de steder og tidspunkter, hvor der er størst risiko for at få stjålet kort og pinkode. Denne information anvendes sammen med Nets' overvågningssystem, der udløser en alarm ved et usædvanligt mønster i brugen af et kort.

Derudover peger Nets på, at den fortsatte udbredelse af kontaktløse betalinger også kan have medvirket til at reducere misbruget. I dag sker tre ud af fire betalinger med Dankort kontaktløst.[9] Da pinkoden som udgangspunkt ikke skal indtastes ved kontaktløse betalinger under 350 kr., kan den heller ikke aflures.

Misbruget af Dankort til køb på nettet er faldet med 62 pct. fra 2. halvår 2018 til 2. halvår 2019, hvor misbruget udgjorde 0,14 promille.[10]

Denne type misbrug foregår som regel ved, at forbryderen får fat i kortoplysningerne digitalt (kortnummer og tilhørende CVV/CVC-kode). Det kan fx ske ved, at en internetbutik udsættes for et hacker-angreb, så kortoplysningerne bliver afluret.

Misbrug som andel af det samlede forbrug med Dankort Figur 2



Anm.: Misbruget er opgjort på halvårsbasis.
Kilde: Nets.

Nets vurderer, at det faldende misbrug i nethandlen primært kan tilskrives to faktorer. For det første anvendes sikkerhedsløsningen Dankort Secured by Nets i stadig større grad. Løsningen indebærer, at brugeren ved handel på nettet – foruden oplysningerne på kortet – afkræves en kode, som sendes på SMS, før køb over 450 kr. kan gennemføres. For det andet har Nets foretaget forbedringer af sit overvågningssystem, der kan alarmere om og afvise mistænkelige transaktioner.

Internationale standarder

Nationalbanken har i 2019 foretaget en vurdering af Betalingsservice efter ECB's standarder for direkte debiteringssystemer.[11] Vurderingen viste, at Betalingsservice i vid udstrækning efterlever de krav, som ECB har opstillet, men at der samtidig er områder med forbedringspotentiale. Nets har efterfølgende adresseret alle anbefalinger og bemærkninger i vurderingen.

7 Nets' statistik for misbrug af Dankort, (*Link*).
(NB: Nets' misbrugstal er ikke direkte sammenlignelige med Nationalbankens statistik over misbrug med betalingskort, der viser det samlede misbrug med både Dankort og internationale kort i Danmark.)

8 Nets' statistik for misbrug af Dankort, (*Link*).

9 Svindel med Dankort næsten halveret på et år, den 28. januar 2020 (*Link*).

10 Nets' statistik for misbrug af Dankort, (*Link*).

11 Danmarks Nationalbank, Vurdering af Betalingsservice, *Danmarks Nationalbank Rapport*, nr. 4, oktober 2019 (*Link*).

På den baggrund har Nets styrket styringen og driften af Betalingsservice på flere punkter:

- Der er etableret bedre processer, organisering og rapportering på complianceområdet.
- Der er foretaget regelændringer, der skal sikre, at virksomhedernes betalingsgebyrer bliver mere tydelige for forbrugerne.
- Processen for identifikation og vurdering af finansielle risici for kreditorer og pengeinstitutter er blevet udbygget.
- Et dedikeret og samlet system til it-risikostyringen er under implementering.
- En overvågningsløsning, der skal sikre hurtigere alarmering og respons i tilfælde af mistænkelig aktivitet i systemer eller netværk, er under implementering.
- Beredskabet og risikostyringen er styrket ved at inddrage erfaringer fra større hændelser hos og angreb på andre virksomheder.
- Fokus på og krav til de kritiske leverandørers risikostyring er skærpet.

Regulering

EU's betalingstjenestedirektiv (PSD2) blev med Lov om betalinger gennemført i dansk ret 1. januar 2018. PSD2 sigter bl.a. på at gøre elektroniske betalinger mere sikre og skabe større konkurrence på betalingsmarkedet i EU. Flere af de centrale bestemmelser har først været gældende i deres endelige udformning fra 14. september 2019, hvor EU's forordning om stærk kundeautentifikation, fælles og sikker kommunikation trådte i kraft.

Med denne lovgivning er der bl.a. indført nye betalingstjenester – betalingsinitieringstjeneste og kontooplysningstjeneste. Bankerne skal derfor have tekniske løsninger, der fx gør det muligt for deres kunder at foretage betalinger ved hjælp af en udbyder af en betalingsinitieringstjeneste, uden der er indgået aftale mellem banken og pågældende udbyder.

Hvad angår kravene om stærk kundeautentifikation[12], har European Banking Authority (EBA) valgt at tillade en forlænget implementeringsperiode på 15 måneder, som løber fra 14. september 2019 til 31. december 2020. Forlængelsen, som kun gælder for kortbetalinger på internettet, skal sikre, at overgangen til de nye krav ikke medfører større forstyrrelser af e-handlen i EU.

I Danmark har PSD2 bl.a. omfattet et fortsat arbejde med udrulningen af Dankort Secured by Nets i de danske internetbutikker for at kunne efterleve kravet om stærk kundeautentifikation ved betalinger. I begyndelsen af 2019 blev Dankort Secured by Nets anvendt ved 15 pct. af den samlede omsætning med Dankort på nettet. I begyndelsen af 2020 var det steget til 30 pct.

For Betalingsservice har PSD2 betydet, at der er blevet indført stærk kundeautentifikation, når en forbruger skal oprette en betalingsaftale via sin bank eller Nets.

12 Det vil sige 2-faktor-autentifikation som fx Dankort Secured by Nets.

Clearing og afvikling af detailbetalinger

Detailbetalinger i danske kroner cleares og afvikles i Sum-, Intradag- og Straksclearingen, kaldet detailclearingerne. Systemerne ejes af Finans Danmark, forvaltes af e-nettet og leveres af Nets.

I Sumclearingen cleares betalinger med bl.a. Dankort og Betalingsservice én gang i døgnet på bankdage. I Intradagclearingen cleares konto til konto-overførsler som fx netbankoverførsler, lønudbetalinger og offentlige udbetalinger. På faste tidspunkter opgør systemerne deltagernes nettopositioner svarende til summen af betalinger til og fra bankernes kunder. Nettopositionerne sendes til Kronos2, hvor beløbene udveksles mellem bankerne.

I Straksclearingen gennemføres konto til konto-overførsler på få sekunder døgnet rundt alle ugens dage. Det kan lade sig gøre, fordi bankerne på forhånd reserverer likviditet i Kronos2 til overførslerne. Selve udvekslingen af likviditet sker seks gange om dagen på bankdage. Straksclearingen anvendes primært til netbank-overførsler og til betalinger via MobilePay.

Brug

Der er 53 direkte deltagere i detailclearingerne og 29 indirekte deltagere, som afvikler gennem en direkte deltager. Værdien af transaktionerne i systemerne udgjorde i gennemsnit 42,9 mia. kr. pr. bankdag i 2019, jf. tabel 2.

Antallet af transaktioner i Straksclearingen stiger fortsat, jf. figur 3.[13] Stigningen skyldes bl.a., at betalinger med MobilePay cleares i Straksclearingen. Opgørelser viser, at MobilePay anvendes af mere end 4 mio. danskere.[14]

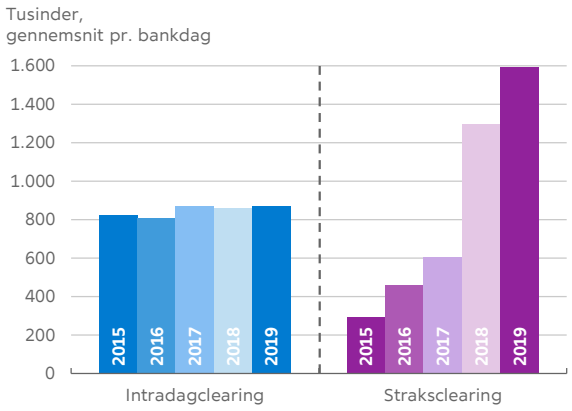
Selv om der har været en stigning i antallet af straksoverførsler, er den samlede værdi af transaktionerne fortsat beskeden, jf. tabel 2. Det skyldes, at Straksclearingen primært anvendes til at overføre mindre beløb. Cirka 45 pct. af transaktionerne

Værdi af transaktioner i Sum-, Intradag- og Straksclearingen Tabel 2

Mia. kr., gennemsnit pr. bankdag	2015	2016	2017	2018	2019
Sumclearingen	16,7	17,2	17,8	19,8	20,7
Intradagclearingen	17,8	18,4	19,7	20,1	20,8
Straksclearingen	0,6	0,8	0,9	1,2	1,4
I alt	35,1	36,4	38,4	41,1	42,9

Kilde: Nets.

Antal transaktioner i Intradag- og Straksclearingen, 2015-19 Figur 3



Kilde: Nets.

13 Antal og værdi af transaktioner i Straksclearingen afspejler ikke det præcise omfang af betalinger. Fx kan en betaling i MobilePay medføre, at der foretages to transaktioner i detailclearingerne.

14 MobilePay, (*Link*).

i Straksclearingen er på under 100 kr., hvorimod transaktioner i Intradagclearingen typisk er noget større, jf. figur 4.

Driftsstabilitet
Driften af detailclearingerne er i 2019 forløbet tilfredsstillende. Sammenlignet med tidligere år har der været markant færre hændelser i systemerne, og der har ikke været større hændelser, som Nationalbanken har fulgt op på.

Likviditet
Deltagerne reserverer likviditet på konti i Nationalbanken til afvikling af deres nettopositioner i detailclearingerne. Hvis en deltager ikke reserverer tilstrækkelig likviditet, bliver deltageren henlagt, og der beregnes nye nettopositioner for de øvrige deltagere, som derved risikerer ikke at modtage den forventede likviditet.

Der har i 2019 kun været tre tilfælde, hvor en deltager er blevet henlagt på grund af manglende likviditet. Det skyldes bl.a., at de fleste af deltagerne anvender systemernes automatiserede værktøjer til likviditetsstyring.

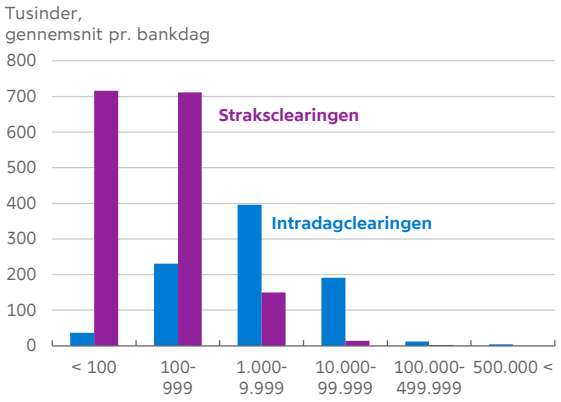
Internationale standarder
Nationalbanken offentliggjorde i 2018 en vurdering af detailclearingerne efter CPMI-IOSCO's principper.[15] Finans Danmark har i løbet af 2019 efterlevet resten af de anbefalinger, som Nationalbanken gav i forbindelse med vurderingen.

Leverandørstyringen er blevet styrket, og der er stillet yderligere og skærpede krav til drift og it-sikkerhed, herunder krav om en totimersmålsætning for sikker genopretning af driften efter et nedbrud.

Der er etableret en mere systematisk risikorapportering fra Nets til Finans Danmark, og det er sikret, at risici rapporteres til relevante ledelseslag.

Derudover gennemfører Finans Danmark løbende test af beredskab og konkursprocedurer, ligesom der senest er gennemført en stresstest for at få indsigt i de likviditetsrisici, der kan opstå, hvis en eller flere deltagere bliver henlagt i afviklingen.

Antal betalinger i Intradag- og Straksclearingen fordelt på størrelse, 2019 Figur 4



Anm.: Straksclearingen har en beløbsgrænse på 500.000 kr. pr. transaktion.
Kilde: Nets.

Nationalbanken har igangsat en vurdering af detailclearingerne efter CPMI-IOSCO's retningslinjer for cybersikkerhed, som uddyber cybersikkerhedsaspekter i CPMI-IOSCO-principperne. Finans Danmarks egenvurdering af systemerne danner udgangspunkt for arbejdet.

Systemændringer
Der arbejdes løbende på at styrke robustheden i detailbetalingsinfrastrukturen.

Den finansielle sektor har bl.a. etableret et nyt datanetværk til brug for clearing og afvikling af detailbetalinger, kaldet e-connect. Netværket leveres af TDC og skal leve op til høje standarder for sikkerhed, redundans og driftsstabilitet. Migreringen af detailclearingernes netværkstrafik til e-connect blev afsluttet medio 2019.

Der har tidligere været eksempler på, at hændelser i den natlige afvikling har forsinket bogføringen på kundernes konti betydeligt. På den baggrund arbejder sektoren på at justere afviklingerne kl. 03.00 og 06.00, så de i tilfælde af en hændelse kan afvikles manuelt og dermed tidli-

15 Danmarks Nationalbank, Vurdering af de danske detailbetalingssystemer, *Danmarks Nationalbank Rapport*, nr. 5, maj 2018 (*Link*).

gere. Det vil give datacentralerne bedre tid til at afslutte bogføringen på kundernes konti inden dagens start. Løsningen forventes implementeret medio 2020.

Nets' salg af detailclearingerne til Mastercard
Mastercard og Nets indgik i august 2019 en aftale om Mastercards køb af bl.a. den del af Nets' infrastruktur, som omfatter detailclearingerne. Købet skal, jf. ovenfor, godkendes af konkurrencemyndighederne, før det kan betragtes som endeligt.

Godkendes købet, vil Mastercard i fremtiden blive leverandør af detailclearingerne i stedet for Nets. I forbindelse med handlen vil der blive indgået en aftale mellem Mastercard og Nets, som træder i kraft på dagen for overtagelsen, og som forpligter Nets til – i en længere periode – at drifte clearingrelaterede systemer, indtil driften er migreret til Mastercard. På kort sigt er det derfor Mastercards plan at fortsætte med drift på IBM's og Nets' datacentre i henholdsvis Danmark og Norge.

Både Nationalbanken og systemejeren, Finans Danmark, samt Nets og Mastercard har fokus på, at detailclearingerne skal køre uforstyrret videre, når de overgår til Mastercard.

P27 – fælles detailbetalingssystem for Danmark, Sverige og Finland
En række nordiske banker har igennem 2019 samarbejdet om at etablere en ny nordisk infrastruktur til clearing og afvikling af detailbetalinger i og mellem Danmark, Sverige og Finland.[16] Samarbejdet er døbt P27 med reference til, at der er ca. 27 millioner indbyggere i Norden.

Ifølge P27 er der stordriftsfordele ved, at de nordiske banker deles om ét fælles detailbetalingssystem, ligesom et fælles system vil muliggøre fælles produkter på tværs af Norden. Samtidig kan systemet medføre mere effektive grænseoverskridende betalinger.

Det er P27-bankernes ambition, at P27 på sigt skal erstatte de nationale detailbetalingssystemer i Sverige, Finland og Danmark, herunder detailclearingerne. Bankerne har etableret et selskab i Sverige med filialer i Danmark og Finland, som skal drive P27. Derudover har bankerne valgt Mastercard som den leverandør, der skal stå for udvikling og drift af systemet.

Som situationen er i dag, har Nationalbanken overvågnings- og tilsynsbeføjelser over for Finans Danmark, der ejer systemerne, mens Finanstilsynet fører it-tilsyn med Nets, som står for driften af systemerne. Begge myndigheder følger projektet tæt og er i dialog med P27, blandt andet for at sikre, at der også i fremtiden er passende overvågning og tilsyn med clearing og afvikling af detailbetalinger i danske kroner.

Derudover drøftes projektet med de nordiske centralbanker og finanstilsyn, bl.a. undersøges muligheden for at oprette et nordisk samarbejde om tilsyn og overvågning med P27.

Finans Danmark er sammen med sektoren ved at undersøge, hvordan afviklingstidspunkterne for P27 og detailclearingerne bedst placeres, hvis begge systemer afvikler i Kronos2. Som en del af arbejdet skal der bl.a. ses på likviditetsstyringen og datacentralernes kapacitet.

16 Bankerne bag initiativet er Danske Bank, Nordea, Handelsbanken, SEB, Swedbank og OP Financial Group. DNB var en del af initiativet, men trak sig sammen med den norske sektor fra projektet marts 2019.

Værdipapirafvikling

VP-afviklingen er det danske system for afvikling af handler med værdipapirer. VP Securities A/S, VP, står også for registrering af ejerskab af værdipapirer og håndtering af periodiske betalinger, emissioner, indfrielser mv.

Salg af aktiemajoriteten i VP til Euronext
I april 2020 indgik Euronext N.V. og de fem største aktionærer i VP, herunder Nationalbanken, en aftale om, at Euronext køber ca. 70 pct. af aktierne i VP med henblik på at opnå fuldt ejerskab. Aftalen er betinget af Finanstilsynets godkendelse i henhold til den fælleseuropæiske regulering af værdipapircentraler, CSDR. Trans-aktionen forventes gennemført i begyndelsen af 3. kvartal 2020.

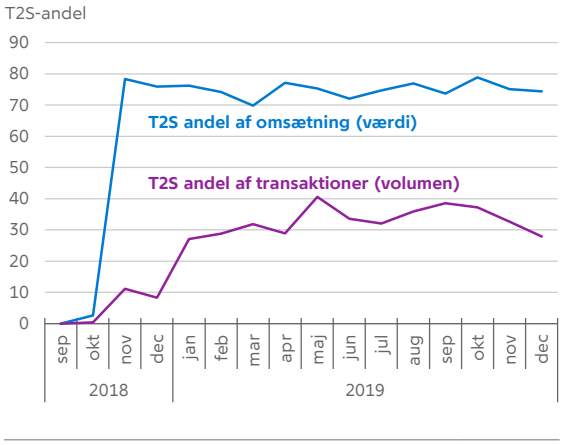
Euronext er en paneuropæisk børs og markedsinfrastruktur-koncern med selskaber i en række europæiske lande. Euronext opkøbte Oslo Børs og den norske værdipapircentral i juni 2019. Ved salget af aktieposten har Nationalbanken lagt vægt på, at Euronext ud fra et finansielt stabilitetssynspunkt er en ejer, der kan udvikle VP og dermed bedst sikre harmoniserede og konkurrencedygtige services for værdipapirhåndtering i Danmark.

VP fortsætter som et dansk selskab reguleret efter CSDR og under tilsyn af Finanstilsynet, mens Nationalbanken overvåger VP i tilknytning hertil som såkaldt relevant myndighed.

Brug
I oktober 2018 blev danske kroner tilsluttet den europæiske værdipapirplatform Target2-Securities (T2S). Siden da er VP's afvikling af deltagernes indbyrdes værdipapirhandler foregået på T2S, mens de private investorers handler fortsat afvikles på VP's egen platform.[17] Afviklingen fordeler sig, så ca. 33 pct. af handlerne og 75 pct. af værdien sker på T2S, jf. figur 5. Det er altså primært større handler, som afvikles hen over T2S.

VP-afviklingen har 119 deltagere, hvoraf 57 er udenlandske markedsdeltagere. Der blev afviklet værdipapirer for 223,4 mia. kr. i gennemsnit pr. bankdag i 2019, jf. tabel 3. Det er en stigning på 32,5 pct. i forhold til 2018, hvilket er drevet af vækst i afviklingen af obligationshandler.

Afviklingsandelen på T2S Figur 5



Kilde: VP.

Driftsstabilitet
Driftsstabiliteten i VP-afviklingen har været tilfredsstillende i 2019. Der har dog været enkelte hændelser, som har påvirket samspillet mellem T2S, VP og Nationalbankens systemer. VP har fulgt op på alle hændelser og gennemført tiltag, der mindsker risikoen for, at det samme sker igen. Det er sket i samarbejde med T2S og Nationalbanken, når det var relevant.

I marts opstod der forsinkelser i værdipapirafviklingen som følge af en kommunikationsfejl ved Nationalbankens Kronos2. Fejlen blev rettet, og VP fik afviklet alle handler inden for det pengepolitiske døgn.

I april måtte T2S udskyde den natlige afvikling på grund af en fejl i sikkerhedsstillelsen. Udskydelsen forsinkede afviklingen i VP og påvirkede hånd-

17 Se Danmarks Nationalbank, Overvågning af den finansielle infrastruktur, *Danmarks Nationalbank Rapport*, nr. 3, juni 2019, side 14, for en nærmere beskrivelse af VP-afviklingen på T2S (*Link*).

Aktier, investeringsbeviser og obligationer afviklet i VP pr. gennemsnitlig bankdag Tabel 3

	I alt		Obligationer		Aktier		Investerings-foreningsbeviser	
År, gennemsnit pr. dag	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.
2015	67,1	206,2	3,4	158,5	33,4	41,4	30,2	6,3
2016	63,6	175,9	2,8	131,8	30,9	37,6	29,9	6,6
2017	66,9	162,7	2,7	118,4	32,4	36,6	31,8	7,7
2018	65,5	168,5	2,6	119,0	29,4	40,8	33,5	8,8
2019	67,1	223,4	4,2	180,9	33,0	34,9	29,8	7,6

Anm.: Værdien er opgjort på baggrund af værdipapirbenet i en handel, dvs. markedsværdien af de papirer sælger overdrager til køber.
Kilde: VP.

ringen af sikkerhedsstillelse i Kronos2. T2S fik hurtigt rettet fejlen og har styrket sine nødprocedurer, så man hurtigere kan håndtere lignende hændelser.

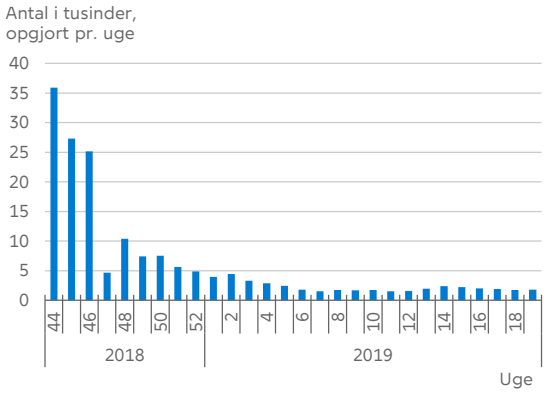
I december resulterede en systemtilpasning i VP's systemer i en fejlkommunikation mellem VP og Nationalbankens porteføljesystem. Fejlen bevirkede, at porteføljesystemet ikke fik registreret sikkerhedsstillelse korrekt. VP rettede fejlen samme dag.

Ikke-matchede handler

Før en handel kan afvikles, skal VP modtage og matche instruktioner fra de to parter, der indgår handlen. Med mange tusinde daglige handler vil der altid være et mindre antal handler, som ikke kan matches, fordi parternes instruktioner ikke er indbyrdes konsistente. Fx kan parterne have forskellige opfattelser af præmisserne for handlen, eller en part kan have fejl i sin instruktion.

Migrationen af danske kroner til T2S betød også tilpasninger i instruktionsformatet. Ikke alle deltagere fik tilpasset formatet korrekt, så mange instruktioner kunne derfor ikke matches i den første tid efter migreringen. VP og deltagerne fik tilpasset instruktionsformatet og håndteret de mange ikke-matchede handler. Antallet af ikke-matchede handler var normaliseret og tilbage på et lavt niveau i løbet af første kvartal 2019, jf. figur 6.

Normalisering af ikke-matchede handler Figur 6



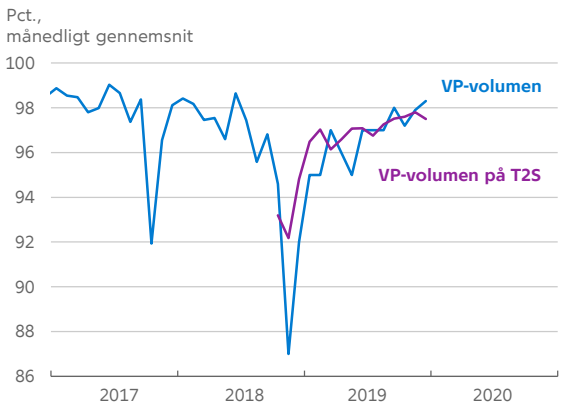
Kilde: VP.

Afviklingsprocent
Ifølge CSDR, artikel 5, skal værdipapirhandler afvikles to dage efter, at handlerne er indgået. Afviklingsprocenten måler andelen af handelsomsætningen, der afvikles rettidigt.

Afviklingsprocenten for handler afviklet i T2S og på VP's platform har siden 2. kvartal 2019 stabiliseret sig på niveauet for VP's afviklingsprocent fra før migrationen af danske kroner til T2S i 2018, jf. figur 7.

Likviditet
Hvis en deltager ikke stiller tilstrækkelig likviditet til værdipapirafviklingen, kan en eller flere handler ikke gennemføres. Det kan give problemer for deltagerens modparter, der på grund af de faldne handler måske ikke kan møde andre forpligtelser. Et sanktionssystem kan medvirke til at disciplinere deltagerne til at stille tilstrækkelig likviditet til afviklingen.

Høj afviklingsprocent i 2019 Figur 7



Anm.: I figuren er afviklingsprocenten opgjort for antal transaktioner.
Kilde: VP.

På T2S-platformen udvikles et fælleseuropæisk sanktionssystem, der skal sanktionere ved handler, som ikke afvikles rettidigt som følge af manglende værdipapirer eller likviditet. Det nye sanktionssystem er blevet forsinket og forventes nu idriftsat februar 2021. VP planlægger, at det nye system skal afløse det nuværende sanktionssystem på VP's platform, således at man følger fælleseuropæisk standard.

Internationale standarder
Nationalbanken gav i 2016 VP fire anbefalinger i forbindelse med Nationalbankens vurdering af VP-afviklingen efter CPMI-IOSCO's principper for finansiel markedsinfrastruktur.

VP har efterlevet tre af anbefalingerne. Den sidste anbefaling vedrører VP's genopretningsplan, hvor VP skal foretage en tydeligere stillingtagen til forskellige kritiske scenarier. VP har revideret sin genopretningsplan, som er til vurdering ved Finanstilsynet og Nationalbanken, der samarbejder om tilsyn og overvågning med VP.

Nationalbanken deltager også i den europæiske overvågning af T2S og har bl.a. givet input til en vurdering af T2S efter CPMI-IOSCO-principperne, jf. afsnittet Betalinger og værdipapirafvikling i euro.

Cyberrobusthed
VP arbejder løbende på at styrke sin cyberrobusthed. Konkret har VP i 2019 styrket sin databeskyttelse, adgangskontroller, sikkerhed i systemer og netværk samt gennemført træning og awareness-kampagner for medarbejdere.

Den 25. oktober 2019 offentliggjorde VP Finanstilsynets redegørelse om tilsynets inspektion ved VP Securities A/S med særligt fokus på cybersikkerhed. Redegørelsen konkluderede, at VP har fokus på risiko herunder cyberrisiko, men Finanstilsynet fandt også grundlag for at give VP påbud om at styrke styringen af kritiske it-leverandører i relation til it-sikkerhed, herunder cybersikkerhed. VP har fremsendt nyt materiale til Finanstilsynet som opfølgning på påbuddene.

I slutningen af 2019 indgik VP ny kontrakt med sin kritiske it-leverandør. Kontrakten giver VP mere fleksibilitet end tidligere. Fx får VP bedre mulighed for at tilpasse kapacitet til spidsbelastningsperioder ved konverteringer. Kontrakten giver også VP bedre mulighed for at stille krav til leverandørens risikostyring.

Nationalbanken har i 2019 gennemført en vurdering af VP's efterlevelse af CPMI-IOSCO's cyber guidance, der præciserer cybersikkerhedsaspekter af CPMI-IOSCO-principperne. De foreløbige konklusioner er drøftet med VP, der har opdateret en del af vurderingsgrundlaget. Der arbejdes videre med vurderingen i 2020.

Systemændringer
VP er ved at forberede etableringen af det kommende fælleseuropæiske sanktionssystem, som vil indebære tilpasninger både i VP's og deltagernes systemer.

CCP-clearing
I Danmark gennemføres handel med aktier fra large- og midcap-segmenterne og repoer gennem en central modpart, også kaldet central counterparty, CCP, jf. boks 5.

På det danske marked clearer de tre CCP'er EuroCCP, LCH Clearnet og Six X-clear aktiehandler, mens Nasdaq Clearing clearer repoforretninger.

Det løbende tilsyn med CCP'erne varetages af de nationale tilsynsmyndigheder i samarbejde med såkaldte tilsynskollegier bestående af tilsynsmyndigheder og centralbanker fra de vigtigste lande, CCP'en opererer i. Der findes ikke danske CCP'er, men Nationalbanken følger udviklingen for de udenlandske CCP'er, som har særlig betydning for danske forhold. Fx deltager Nationalbanken i tilsynskollegiet for EuroCCP.

EuroCCP er en hollandsk CCP, der står for en stor del af clearingen af de danske aktier og derfor vurderes central for dansk værdipapirafvikling. I december 2019 fremsatte den ene af de fem ejere – Chicago Board Options Exchange (CBOE) – tilbud om at overtage det fulde ejerskab af EuroCCP. Det konsoliderede ejerskab forventes ikke at ændre EuroCCP's strategiske fokus, men vil give EuroCCP mulighed for at udvikle deres forretning inden for derivater. Overtagelsen forventes gennemført i første halvdel af 2020, under forudsætning af at den godkendes af de hollandske myndigheder.

Hvad er en CCP? Boks 5

En CCP stiller sig mellem parterne i en handel og påtager sig risikoen for både køber og sælger, i tidsrummet fra handlen er indgået, og til den er endeligt afviklet. Hvis én af parterne i handlen går konkurs inden for det tidsrum, er CCP'en således stadig forpligtet over for den anden part. Det medfører imidlertid også, at risici koncentreres i CCP'en, der derfor er underlagt en række lovkrav[1] for at sikre gennemførelsen af handlen.

1. Jf. Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (*link*).

Betalinger og værdipapirafvikling i euro

Danske bankers betalinger og værdipapirhandler i euro afvikles i Target2 og Target2-Securities (T2S).

Target2 er det fælleseuropæiske RTGS-system til afvikling af interbankbetalinger i euro. I Target2 laves der også overførsler til brug for afvikling i andre eurosystemer, fx T2S. T2S er det fælleseuropæiske system til afvikling af værdipapirhandler i euro og danske kroner.[18]

Brug

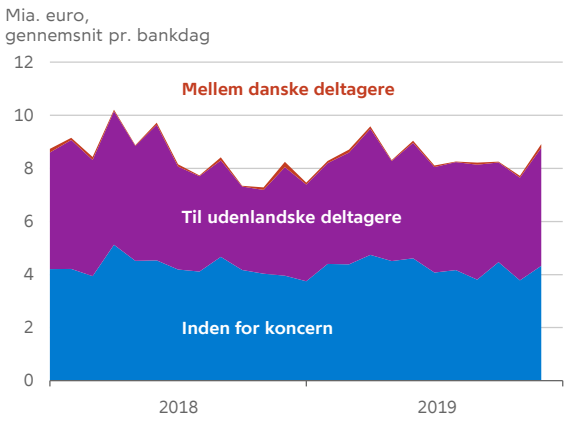
Der er 26 danske deltagere i Target2. I 2019 gennemførte de interbankbetalinger for i gennemsnit 8,4 mia. euro om dagen. De danske deltagere bruger hovedsageligt Target2 til at gennemføre koncerninterne betalinger og betalinger til udenlandske deltagere, jf. figur 8. Der udveksles flest euro med deltagere i Tyskland, Finland, Frankrig og Holland.

I alt 21 værdipapircentraler fra 20 europæiske lande er tilsluttet T2S, herunder VP. En bank kan afvikle på T2S, enten som direkte deltager, hvis banken har en såkaldt T2S-afviklingskonto, eller som indirekte deltager via en anden direkte deltagers adgang.

En T2S-afviklingskonto skal oprettes via en af centralbankerne i EU. 13 danske banker har via Nationalbanken en T2S-afviklingskonto til betaling eller modtagelse af euro i forbindelse med T2S-afviklingen. Andre danske banker kan have oprettet en T2S-afviklingskonto via andre EU-centralbanker.

Der kan ikke placeres euro permanent på T2S-afviklingskontoen. Bankerne skal derfor også have adgang til en Target2-konto, som der kan føres euro tilbage på, når afviklingsdøgnet afsluttes. Hovedparten af de danske banker har indgået aftale med en korrespondentbank herom. Nogle af de største banker har via deres filial etableret en Target2-konto ved en centralbank i euroområdet. En sådan ordning giver også banken mulighed for at kunne låne euro intradag.

Interbankbetalinger i Target2 Figur 8



Anm.: Figuren angiver betalinger afsendt af danske deltagere igennem Target2. Gennemsnit pr. dag er beregnet på månedsbasis.
Kilde: Danmarks Nationalbank.

Driftsstabilitet

Driftsstabiliteten i de lokale komponenter af Target2, som Nationalbanken har ansvaret for, har været tilfredsstillende i 2019. Der har i 2019 kun været mindre hændelser, som ikke har påvirket gennemførelsen af betalinger i euro.

Internationale standarder

Overvågningen af Target2 og T2S sker i samarbejde med centralbankerne i EU. Nationalbanken deltager i den fælles overvågning, som ledes af ECB og foregår i arbejdsgrupper med deltagelse af de nationale centralbanker.

I 2019 færdiggjorde ECB en vurdering af T2S efter et udvalg af CPMI-IOSCO-principperne for finansiel infrastruktur. Vurderingen blev godkendt af Styrelsesrådet i oktober 2019. Nationalbanken har givet input til vurderingen samt deltaget i møder med T2S-operatøren. Vurderingen bliver ikke offentliggjort, men Nationalbanken og VP er bekendt med

18 T2S kan håndtere flere valutaer. Ud over euro er danske kroner den eneste anden valuta tilsluttet til T2S. Læs om kroneafvikling i afsnittet Værdipapirafvikling.

indholdet, og Nationalbanken vil deltage i opfølgningen på vurderingen i 2020.

Sideløbende med overvågning er T2S også underlagt tilsyn. Nationalbanken og Finanstilsynet deltager sammen med andre europæiske centralbanker og tilsyn i et såkaldt Coorporative Arrangement, som definerer fælles rammer og koordinerer tilsynet med T2S.

Systemændringer
ECB har de seneste år arbejdet på at modernisere den europæiske betalingsinfrastruktur.

I 2016 igangsatte ECB et konsolideringsprojekt, som skal samle Target2, T2S og TIPS (Target Instant Payment Settlement) på én platform og derved opnå driftsbesparelser gennem konsolidering af tværgående funktioner. Som en del af konsolideringen vil der ske en udskiftning af Target2 med et mere tidssvarende RTGS-system.

TIPS og T2S giver allerede i dag mulighed for, at der afvikles i andre valutaer end euro. I forbindelse med konsolideringen vil Target2 også kunne håndtere andre valutaer end euro.

Parallelt med konsolideringen etableres en fælles indgang – European System Market Infrastructure Gateway – til eurosystemets betalings- og afviklingssystemer med det formål at give deltagerne lettere og billigere adgang til systemerne.

Endelig udvikler ECB et nyt sikkerhedsstillelses-system kaldet European Collateral Management System (ECMS). ECMS vil som udgangspunkt kun kunne anvendes til at stille sikkerhed i euro.

Valutahandelsafvikling

CLS Bank International (CLS) er et internationalt afviklingssystem for valutahandler. CLS ejes af store internationale banker og afvikler handler i 18 tilsluttede valutaer, herunder danske kroner.

I CLS afvikles de to betalinger, som en valutahandel består af, samtidigt (Payment-versus-Payment, PvP). Dermed reduceres afviklingsrisikoen, dvs. risikoen for at den ene part i en valutahandel ikke betaler sin del af handlen. Ved valutahandler, der afvikles uden for CLS, fx via korrespondentbanker, påføres parterne en afviklingsrisiko, fordi betalingerne afvikles uafhængigt af hinanden.

Nationalbanken deltager i den fælles overvågning af CLS, jf. boks 6.

Brug
Mere end 95 pct. af valutahandlerne i danske kroner gennemføres via CLS.[19] Det er en stigning fra 2016, hvor det var omkring 80 pct.

Både danske banker og erhvervsvirksomheder kan afvikle valutahandler via CLS. Én dansk bank deltager direkte i CLS-afviklingen. Hvis man ikke selv er direkte deltager, kan man afvikle via en af de ni inden- og udenlandske deltagere, der tilbyder indirekte deltagelse til det danske marked.

I alt fem deltagere har en CLS-afviklingskonto i Nationalbanken, hvoraf tre tilbyder håndtering af ind- og udbetalinger til CLS-afviklingen på vegne af de øvrige deltagere.

Den gennemsnitlige daglige værdi af handler i danske kroner var 265 mia. kr. i 2019. Det er en stigning på 12 pct. i forhold til 2018, jf. figur 9. Antal og værdi af afviklede handler er især stor i dagene omkring udenlandske helligdage og ved kvartalsskifter.

Driftsstabilitet og likviditet
Indbetalingerne til CLS sker via de nationale RTGS-systemer, for danske kroner via Kronos2.

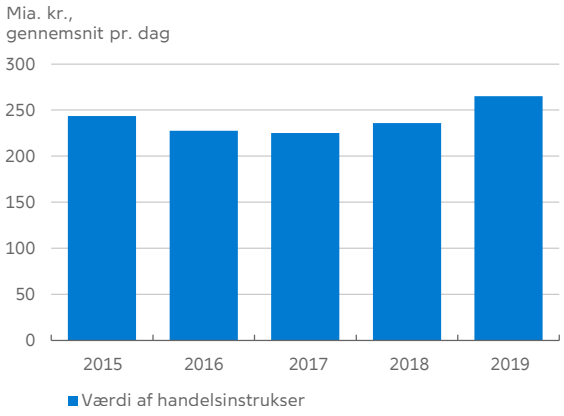
Overvågning af CLS Boks 6

Overvågningen af CLS tager udgangspunkt i CP-MI-IOSCO's principper. CLS offentliggør hvert andet år en opdateret beskrivelse af systemets efterlevelse af principperne.[1]

Overvågningen af CLS foregår i den fælles overvågningskomite, CLS Oversight Committee[2], der er et forum for samarbejde mellem de tilsluttede valutaers centralbanker, som derigennem kan varetage deres nationale overvågningsforpligtelse. Nationalbanken deltager i samarbejdet, der ledes af den amerikanske centralbank, Federal Reserve, FED, som også er tilsynsmyndighed for CLS. Nationalbankens overvågning har fokus på forhold, der har betydning for afviklingen af handler i danske kroner.

1. CLS, Principles for Financial Market Infrastructures Disclosure, 2018, (*Link*).
2. Federal Reserve System, Protocol for the Cooperative Oversight Arrangement of CLS (*Link*).

Værdi af handelsinstruktioner i CLS Figur 9



Anm.: Gennemsnit pr. dag beregnet på årsbasis.
Kilde: CLS Bank.

19 Anslået på baggrund af BIS, Triennial Central Bank Survey, Foreign exchange turnover in April 2019, Bank for International Settlements, September 2019 (*Link*) og data fra CLS Bank.

Driftsstabiliteten i CLS er derfor afhængig af stabiliteten i de tilsluttede RTGS-systemer. I 2019 har der ikke været hændelser i Kronos2, der har påvirket de fastlagte deadlines for afvikling i CLS.

De danske deltagere reserverer tilstrækkelig likviditet til CLS-afviklingen.

Systemændringer

I 2019 blev CLSNow[20] lanceret. CLSNow er en service til at afvikle handler enkeltvist inden for samme dag ved PvP. Det giver deltagerne mulighed for bedre at styre deres likviditet på tværs af valutaer. Afvikling i CLSNow reducerer endvidere afviklingsrisikoen. P.t. kan der afvikles i canadiske dollar, euro, britiske pund og dollar. Servicen vil potentielt blive udvidet til alle CLS-valutaer.

20 CLS, CLSNow (*Link*).

UDGIVELSER

NYT

Nyt giver et hurtigt og tilgængeligt indblik i en Analyse, et Economic Memo, et Working Paper eller en Rapport fra Nationalbanken. Nyt udkommer løbende.

ANALYSE

Nationalbankens Analyseserie har fokus på økonomiske og finansielle forhold. Nogle af analyserne udkommer med fast frekvens, fx *Udsigter for dansk økonomi* og *Finansiel stabilitet*, der begge udkommer halvårligt. Andre analyser udkommer løbende.

RAPPORT

Nationalbankens Rapportserie er tilbagevendende rapporter og beretninger om Nationalbankens virke. Det er fx *Årsrapport* og *Statens låntagning og gæld*.

ECONOMIC MEMO

Economic Memo er en mellemting mellem en Analyse og et Working Paper og viser ofte forfatternes igangværende analysearbejde. Serien henvender sig primært til fagpersoner og offentliggøres alene på engelsk. Economic Memo udkommer løbende.

WORKING PAPER

Working Paper præsenterer forskningsarbejde udført af ansatte i Nationalbanken og samarbejdspartnere. Serien henvender sig primært til fagpersoner og folk med interesse for den akademiske tilgang. Working Paper udkommer løbende.

Rapporten består af en dansk og engelsk version.
I tilfælde af tvivl om oversættelsens korrekthed gælder den danske version.

DANMARKS NATIONALBANK
HAVNEGADE 5
1093 KØBENHAVN K
WWW.NATIONALBANKEN.DK

Redaktionen er afsluttet
15. april 2020

DANMARKS
NATIONALBANK