

DANMARKS NATIONALBANK

4. MAJ 2022 — NR. 3

Overvågning af den finansielle infrastruktur 2021

- Danmark har en sikker og effektiv betalingsinfrastruktur, der er godt rustet til at håndtere operationelle hændelser.
- De dygtigste hackere bliver mere specialiserede og sofistikerede, og eksterne begivenheder som Ruslands angreb på Ukraine medfører nye afledte cyberrisici. Derfor er det helt centralt, at der i infrastrukturen fortsat arbejdes målrettet på at beskytte sig mod cyberangreb.
- Cybertruslen kan ikke elimineres. Det er derfor vigtigt, at der både individuelt og i fællesskab arbejdes på at styrke databeskyttelsen og evnen til at genoprette systemer efter et alvorligt cyberangreb.

INDHOLD

- 2 DANMARK HAR EN SIKKER OG EFFEKTIV BETALINGSINFRASTRUKTUR
- 7 INTERBANKBETALINGER
- 11 DETAILBETALINGER
- 14 CLEARING OG AFVIKLING AF DETAILBETALINGER
- 17 VÆRDIPAPIR-AFVIKLING
- 21 BETALINGER OG VÆRDIPAPIR-AFVIKLING I EURO
- 23 VALUTAHANDELS-AFVIKLING

Samfundskritisk infrastruktur

641 mia. kr.

afvikles der i gennemsnit betalinger for hver bankdag i de centrale systemer.

[Læs mere](#)

Samarbejde på tværs af den finansielle sektor

Øger cyberrobusthed

hos de centrale aktører og bredt i samfundet.

[Læs mere](#)

Danmark har en sikker og effektiv betalingsinfrastruktur

En effektiv og sikker betalingsinfrastruktur er en forudsætning for udvekslingen af varer og tjenester. Hvis systemerne i infrastrukturen ikke virker, vil det skabe forstyrrelser, der i værste fald kan true finansiel stabilitet og skade samfundsøkonomien.

Betalingsinfrastrukturen er et netværk af forskellige systemer, der muliggør, at borgere, virksomheder og finansielle aktører kan udveksle betalinger og værdipapirhandler med hinanden. I 2021 blev der på en gennemsnitsdag sendt elektroniske betalinger for 641 mia. kr. gennem de centrale systemer i den danske betalingsinfrastruktur, jf. betalingsflowet i oversigtsfiguren i boks 1.

Som følge af betalingsinfrastrukturens kritiske rolle overvåger Nationalbanken, at de centrale systemer efterlever internationale standarders krav til sikkerhed og effektivitet. Overvågningen omfatter også de vigtigste betalingsløsninger. De centrale systemer og løsninger i den danske finansielle infrastruktur er beskrevet i boks 1.

I denne rapport præsenteres hovedkonklusioner fra overvågningen og de væsentligste områder, der har haft betydning for den danske finansielle infrastruktur i 2021.

Infrastrukturen er sikker, effektiv og stabil

Nationalbankens overvågning viser, at Danmark har en effektiv og robust betalingsinfrastruktur.

Driftsstabiliteten i 2021 var høj, og der var kun få forstyrrelser i udvekslingen af betalinger og afviklingen af værdipapirhandler. Endvidere efterlever de centrale systemer og løsninger i høj grad de krav, der stilles i internationale standarder, og der arbejdes løbende med at styrke sikkerheden og efterleve Nationalbankens anbefalinger til forbedringer.

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:

- Kronos2 (interbankbetalinger)
- Sum-, Intradag- og Straksclearingen (detailbetalinger)
- Euronext Securities Copenhagens afviklingssystem (værdipapirhandler)
- Dankort, Betalingsservice og konto til konto-overførsler (de vigtigste betalingsløsninger)
- Internationale systemer, der har relevans i Danmark.

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

En række eksterne udfordringer er blevet håndteret gennem de seneste år

Ændringer i risikobilledet betyder, at kravene til en sikker og robust infrastruktur løbende skærpes. Et nyligt eksempel er, at covid-19-pandemien medførte, at systemerne/løsningerne i betalingsinfrastrukturen på kort tid skulle omstille driften til, at medarbejderne i udstrakt grad arbejdede hjemmefra. Fjernopkoblinger via VPN-forbindelser fra private hjem medførte nye muligheder, men også en række nye risici. Det er derfor positivt, at systemerne/løsningerne håndterede risici under covid-19-pandemien sådan, at det ikke påvirkede driftsstabiliteten i betalingsinfrastrukturen.

En anden problemstilling, der kræver løbende opmærksomhed, er håndteringen af risici fra eksterne leverandører. Der har gennem de seneste par år været flere tilfælde af sikkerhedshændelser, som udsprang af sårbarheder i software og services fra tredjepartsleverandører. De mest fremtrædende eksempler er hackerangrebet mod netværksovervågningsprogrammet Solarwinds Orion¹ og sårbarheden i open source-logningsmodulet Log4j².

1 Hackere havde placeret ondsindet kode i SolarWinds Orion-software, som muliggjorde, at udefrakommende aktører kunne få adgang til den organisations systemer, der benyttede sig af produktet.

2 Der blev fundet en sårbarhed i Apache Log4j, der er et open source-logningsbibliotek, som er almindeligt anvendt af apps og tjenester på tværs af internettet. Hvis sårbarheden ikke bliver rettet, kan angribere potentielt bryde ind i systemer, stjæle adgangskoder og logins, udtrække data og inficere netværk med skadelig software.

Betalingsinfrastrukturen i Danmark

Boks 1

Hver bankdag¹ sendes i gennemsnit betalinger for 641 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.

Detailbetalinger er betalinger mellem borgere, virksomheder og offentlige myndigheder med fx betalingskort, mobiltelefon og konto til konto-overførsler. Når betalingerne er initieret og formidlet gennem en række mellemlid, ender de alt efter type med at blive opgjort og afstemt i Sum-, Intradag- eller Straks-clearingen, der er den finansielle sektors detailbetalingssystemer. Afviklingen sker efterfølgende på konti i Nationalbanken via Kronos2. Detailbetalingssystemerne ejes af Finans Danmark.

Værdipapirhandler kan indgås på mange forskellige typer markedspladser, bl.a. fondsbørsen, handelsplatforme eller "over-the-counter" via bank eller mægler. Den efterfølgende afvikling af handlerne sker for professionelle investorer vedkommende på den fælleseuropæiske platform Target2-Securities, T2S, der ejes af Den Europæiske Centralbank, ECB. Deltagelse på T2S kræver pengekonto i Nationalbanken og værdipapirkonto i Euronext Securities Copenhagen,

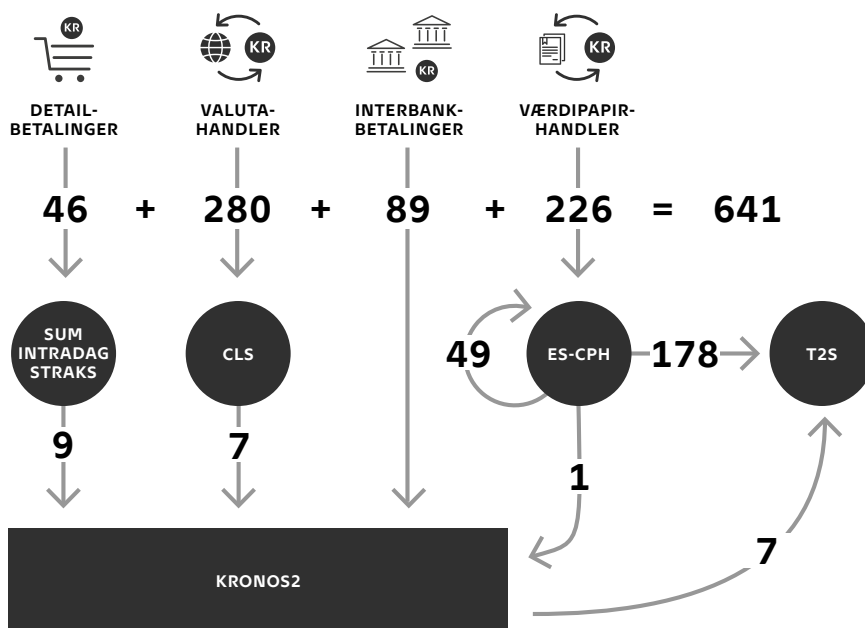
ES-CPH. ES-CPH er således som værdipapircentral ansvarlig for at føre løbende regnskab med beholdningerne af alle danskudstedte værdipapirer på vegne af investorerne. Afviklingen af de private investorers handler sker via ES-CPH-afviklingen, der er ES-CPH's eget afviklingssystem.

Valutahandler afvikles gennem CLS, der er et internationalt system til valutahandler. Nationalbanken stiller konti til rådighed for de pengeinstitutter, der gennemfører handler via CLS. CLS ejes af store internationale banker.

De tre detailbetalingssystemer, CLS og ES-CPH-afviklingen afvikler deres deltageres nettopositioner i Kronos2, hvor deltagerne har konti. Nettopositionerne beregnes i de respektive systemer ved at modregne deltagernes tilgodehavender og forpligtelser, såkaldt netting. Netting reducerer deltagernes likviditetsbehov betydeligt sammenlignet med en situation, hvor alle betalinger afvikles enkeltvist, fx reducerer netting likviditetsbehovet til afvikling af detailbetalinger fra 46 mia. kr. til 9 mia. kr. dagligt, svarende til en reduktion på 80 pct.

På T2S sker afviklingen af de professionelle investorers handler også ved brug af netting. Likviditeten til afviklingen overføres fra deltagernes pengekonti i Nationalbanken. Nettingen reducerer deltagernes likviditetsbehov fra 178 mia. kr. til 7 mia. kr., hvilket svarer til en reduktion på 96 pct.

Betalingsflow, mia. kr., gennemsnit pr. bankdag i 2021



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.

Nationalbankens overvågning viser, at både Solarwinds- og Log4j-sårbarhederne var til stede i centrale systemer i infrastrukturen, men også at de ansvarlige for de konkrete systemer nåede at gribe ind, uden at sårbarhederne fik egentlige driftsmæssige konsekvenser.

Det er vigtigt, at der også fremadrettet arbejdes struktureret med at identificere, mitigere og håndtere ændringer i risikobilledet. Det inkluderer også et effektivt beredskab til at inddæmme nye hændelser, inden de når at gøre alvorlig skade. Det gælder særligt i forhold til truslen fra cyberangreb.

Ruslands krig mod Ukraine ændrer cybertruslen

Aktuelt har Ruslands angreb på Ukraine medført nye afledte risici på cyberområdet. Det skyldes, at krigen ikke alene udkæmpes på landjorden, men også i cyberspace. Selvom den danske betalingsinfrastruktur ikke vurderes at være direkte mål for statssponsorerede russiske hackergrupper, kan der være en øget risiko for, at systemerne bliver indirekte ramt af cyberangreb, som ellers er rettet mod den digitale infrastruktur i Ukraine.

Nationalbanken har i sin overvågning løbende fokus på arbejdet med cyberrobusthed i infrastrukturens systemer og løsninger og er også i dialog med de ansvarlige ejere omkring aktuelle risici som følge af Ruslands invasion af Ukraine. Dialogen viser samlet set, at der for nuværende ikke er tegn på markante skift i trusselsbilledet. Der er dog en klar bevidsthed om, at trusselsbilledet hurtigt kan ændre sig. Situationen overvåges derfor nøje af ejerne, og der er gjort en række tiltag for at øge paratheden og styrke cyberberedskabet. Endvidere koordineres og videndeles der om trusler og hændelser på tværs af sektoren i regi af det sektorkriseberedskab, som drives af Finansielt Sektorforum for Operationel Robust-

hed, FSOR. Nationalbanken udgør sekretariat for sektorkriseberedskabet, der – udover systemerne og løsningerne i infrastrukturen – også har deltagelse af de største danske banker, datacentraler, pensions- og forsikringsselskaber samt relevante myndigheder og Nordic Financial CERT.³

Høj cyberrobusthed skal løbende udvikles

Nationalbanken vurderer løbende, om systemerne i betalingsinfrastrukturen lever op til internationale retningslinjer for cyberrobusthed.⁴ Vurderingerne har indtil videre peget på, at systemernes cyberrobusthed ligger på et højt niveau på de fleste områder.⁵ Billedet ses også i Nationalbankens cyberundersøgelser, hvor kerneaktører (store banker, forsikrings- og pensionselskaber, datacentraler og infrastruktur) i den finansielle sektor selvevaluerer deres aktuelle cyberrobusthedsniveau.⁶ Resultaterne af den seneste undersøgelse fra 2020 pegede på, at systemer og løsninger i infrastrukturen niveaumæssigt lå i toppen blandt undersøgelsens deltagere. Givet systemernes centrale rolle for samfundet er der dog også en klar forventning om, at robustheden ligger på et vedblivende højt niveau.

Som beskrevet ovenfor udvikler trusselsbilledet på cyberområdet sig hurtigt. Udover at eksterne begivenheder, som fx covid-19-pandemien og angrebet på Ukraine, påvirker det generelle trusselsbillede, er der samtidig en tendens til, at de teknikker og taktikker, som de "almindelige" cyberkriminelle benytter sig af, løbende bliver mere specialiserede og sofistikerede.

Udviklingen betyder, at risikoen for, at avancerede hackergrupper bryder igennem det ydre forsvar, ikke kan elimineres. Det er derfor helt centralt, at systemerne og løsningerne i infrastrukturen

3 Nordic Financial CERT er en medlemsdrevet non-profit-organisation, der har til formål at styrke den nordiske finansindustri modstandsdygtighed over for cyberangreb og sætte nordiske finansielle institutioner i stand til at reagere hurtigt og effektivt på cybersikkerhedstrusler og onlinekriminalitet.

4 CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, juni 2016 ([link](#)).

5 En nærmere beskrivelse ses i rapportens afsnit om de enkelte systemer/løsninger.

6 Nationalbanken har gennemført cyberundersøgelser i hhv. 2016, 2018 og 2020. En analyse af de seneste resultater kan findes her ([link](#)).

modgår udviklingen i trusselsbilledet med passende foranstaltninger. Det gælder særligt i forhold til at øge paratheden til at reagere på og håndtere de cyberangreb, der måtte lykkes med at bryde igennem.

Særligt fokus på databeskyttelse og recovery

Beskyttelsen af kritiske data og evnen til at sikre en hurtig og sikker genopretning (recovery) er centrale elementer i arbejdet med at begrænse skadevirkninger fra et angreb, der måtte lykkes med at bryde igennem det ydre forsvar. Databeskyttelse og recovery er tæt beslægtede områder: Hvis kritiske data ikke er tilgængelige, vil det i væsentlig grad påvirke systemernes evne til at genoprette driften.

Nationalbanken har i sin overvågning fokus på arbejdet med databeskyttelse og recovery i infrastrukturen. Det gælder fx systemernes og løsningsernes brug af kryptering og backup, der begge er centrale elementer i en effektiv databeskyttelse. På recovery-området er det vigtigt, at systemerne har udarbejdet en specifik cyberberedskabsplan, der målrettet adresserer genopretning af it-systemer og videreførelse af kritiske forretningsområder efter en cyberhændelse. Planen skal løbende testes ud fra en risikobaseret tilgang med udgangspunkt i de ekstreme, men plausible scenarier, et cyberangreb kan forårsage.

Udover indsatsen i de individuelle virksomheder er arbejdet med databeskyttelse og recovery også særlige indsatsområder, som myndigheder og centrale private aktører arbejder på at styrke i fællesskab, jf. nedenfor.

Konsolidering kan bidrage til endnu højere robusthed i de enkelte systemer

Store internationale koncerner har gennem de seneste to år opkøbt centrale systemer og løsninger eller fusioneret forretningsområder i den danske betalingsinfrastruktur:⁷

- I august 2019 indgik den internationale betalingsvirksomhed Mastercard aftale med Nets om at købe Betalingsservice og clearingsaktiviteter.
- I april 2020 overtog den paneuropæiske infrastrukturkoncern Euronext ejerskabet af den danske værdipapircentral, der nu hedder Euronext

Securities Copenhagen (tidligere VP Securities A/S).

- I juni 2021 blev fusionen mellem Nets og den italienske betalingsvirksomhed Nexi endeligt gennemført.

Baggrunden for den øgede grad af konsolidering er bl.a. skærpede konkurrencevilkår og stordriftsfordele, hvilket skyldes de store faste omkostninger, der er forbundet med drift af betalingssystemer. I de store infrastrukturkoncerner vil der også være en række aktiviteter på sikkerhedsområdet, hvor der som følge af synergier kan skabes et endnu højere robusthedsniveau, fx med henblik på at følge med udviklingen i trusselsbilledet på cyberområdet.

Nationalbanken har i 2021 fortsat arbejdet med at forberede tilslutningen af den danske kroneafvikling til den europæiske betalings- og værdipapirafviklingsplatform, Target Services, jf. boks 2. Projektet omfatter også tilslutning til TIPS, der er en platform for grænseoverskridende straksbetalinger mellem borgere og mellem borgere og virksomheder i Europa. Tilslutningen til den europæiske it-plattform vil give skalafordele, der alt andet lige også vil betyde øgede ressourcer til arbejdet med bl.a. cybersikkerhed. Arbejdet med tilslutningen forløber som planlagt og forventes færdigt i 2025.

Samarbejde på tværs øger robustheden på sektor- og samfundsniveau

En del af arbejdet med at mitigere cyberrisici og øge den operationelle robusthed sker på sektorniveau i forskellige sektorsamarbejder. Finansielt Sektorforum for Operationel Robusthed, FSOR, har gennem de seneste seks år samlet myndigheder og centrale private aktører i den finansielle sektor i et fælles samarbejdsforum, der arbejder på at øge sektorens operationelle robusthed, herunder cyberrobustheden.⁸

Centralt for arbejdet i FSOR er en risikoanalyse på sektorniveau, der bidrager til at identificere samfundsmæssige risici og derved giver et struktureret grundlag for at prioritere tiltag til at reducere risici. Risikoanalysen har bl.a. identificeret flere risici, som omhandler databeskyttelse og recovery. I FSOR er der derfor igangsat initiativer, der har fokus på at

⁷ Dette uddybes i de afsnit af denne rapport, der omhandler de systemer og løsninger i infrastrukturen, udviklingen er relevant for.

⁸ Læs mere i FSOR's årsberetning for 2021 ([link](#)).

styrke den fælles indsats inden for disse områder. Der er bl.a. igangsat et arbejde med at identificere de data, der ud fra et samfundsperspektiv skal passes særligt på, og hvis tilgængelighed er kritisk i en genetableringssituation.

Arbejdet med at identificere samfundskritiske data varetages bl.a. i koordination med Risikoforum for Gensidige Afhængigheder, RGA, der er et samarbejdsforum, hvor de ansvarlige for de centrale betalings- og afviklingssystemer i infrastrukturen deltager.⁹ RGA arbejder også på at udarbejde fælles nedluknings- og genåbningsscenarier samt køreplaner og test for kontrolleret nedlukning af den kritiske infrastruktur i tilfælde af operationelle hændelser, fx et alvorligt cyberangreb.

I TIBER-DK, der er Nationalbankens Threat Intelligence Based Ethical Red team-testprogram, er der også fokus på systemernes evne til at beskytte kritiske data. I en TIBER-test, hvor live-systemer udsættes for et simuleret cyberangreb, er der særlig opmærk-

somhed på at teste scenarier, der afprøver testdeltagerens datasikkerhed. De ansvarlige for de centrale systemer i infrastrukturen deltager i TIBER-DK, og de var derfor – sammen med Nationalbanken og de øvrige deltagere – i foråret 2021 med til at beslutte, at testprogrammet skulle fortsætte.¹⁰

Udover de initiativer, der er søsat i den finansielle sektor i regi af Nationalbanken, fx FSOR og TIBER-DK, arbejdes der også med cyberrobusthed bredt i samfundet. Nationalbanken samarbejder og er repræsenteret i en række samarbejdsfora i Danmark og deltager endvidere i nordisk og europæisk samarbejde. Samarbejderne omfatter bl.a. udveksling af informationer om hændelser og trusler, koordination af krisehåndtering og videndeling af "best-practice".

9 Dvs. Nationalbanken (interbankbetalinger), Euronext Securities Copenhagen (værdipapirhandler), Finans Danmark (detailbetalinger) og e-nettet (kommunikationsnetværk).

10 Læs mere om TIBER-DK her ([link](#)).

Interbankbetalinger

Interbankbetalinger er betalinger mellem finansielle institutter. Typisk er disse betalinger karakteriserede ved at være tidskritiske og af høj værdi. Interbankbetalinger i danske kroner afvikles i Nationalbankens Kronos2.

Kronos2 er et bruttoafviklingsystem i realtid, RTGS-system, der afvikler betalinger enkelvist og øjeblikkeligt. Kronos2 er et centralt omdrejningspunkt i dansk betalingsinfrastruktur, se boks 1. Udover interbankbetalinger afvikles der i Kronos2 også pengepolitiske operationer og nettopositioner fra tilsluttede betalings- og afviklingssystemer.

Brug

Der er 80 deltagere i Kronos2. Deltagerne er primært danske banker, realkreditinstitutter og filialer af udenlandske banker.

I 2021 blev der i gennemsnit pr. bankdag gennemført knap 6900 interbankbetalinger i Kronos2 med en samlet værdi på 88,7 mia. kr., jf. tabel 1.

Værdien af pengepolitiske operationer faldt betydeligt fra 2020 til 2021, jf. tabel 1. Faldet skyldes, at Nationalbanken 19. marts 2021 indførte en teknisk tilpasning af de pengepolitiske instrumenter med det formål at sikre mere stabile pengemarkedsrenter. Med tilpasningen er loftet over bankernes indestående i Nationalbanken fjernet, hvilket betyder, at bankerne kan placere deres samlede indestående på deres foliokonti og ikke længere skal købe eller sælge indskudsbeviser for dagligt at tilpasse likviditeten.¹¹

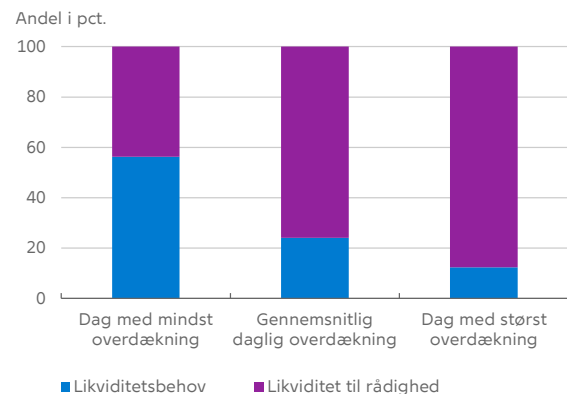
Driftsstabilitet

Driften af Kronos2 var i 2021 påvirket af flere hændelser.

Den 26. april 2021 var Kronos2 ude af drift mellem klokken 15:30 til 20:00. I dette tidsrum kunne der ikke gennemføres betalinger, clearinger eller udveksles beskeder mellem Kronos2 og det fælleseuropæ-

Rigelig likviditet blandt deltagerne i Kronos2 i 2021

Figur 1



Kilde: Danmarks Nationalbank.

iske værdipapirafviklingsystem Target2-Securities, T2S. Årsagen til nedbruddet var en fejl i en funktionalitet, som sjældent er blevet brugt. Det er efterfølgende blevet sikret, at samme fejl ikke kan ske igen.

I midten af juni opgraderede ECB T2S. Opgraderingen medførte imidlertid lange svartider på beskeder mellem T2S og Kronos2 om inddækning af T2S-auto-collateral¹². Konsekvensen var, at deltagerne værdipapirer, som blev brugt ved T2S-auto-collateral, blev fastholdt som pant, og at Nationalbanken måtte frigive papirerne manuelt. Som en midlertidig foranstaltning blev deltagerne i Kronos2 bedt om dagligt at foretage en manuel inddækning af T2S-auto-collateral for at imødegå problemet. I slutningen af juli fik ECB løst problemerne, der også har påvirket andre centralbanker og deltagere i andre lande.

Likviditet

Deltagerne har som helhed haft rigelig likviditet til at gennemføre deres betalinger i Kronos2, jf. figur 1.

¹¹ Danmarks Nationalbank, Teknisk tilpasning af de pengepolitiske instrumenter, *Pressemeddelelse*, 19. marts 2021 ([link](#)).

¹² T2S-Auto-collateral: Kontohaver kan optage intradag-lån i danske kroner til brug for køb af værdipapirer og gennemførelse af periodiske betalinger på T2S mod sikkerhed i indkøbte eller øvrige belånbare værdipapirer.

Transaktioner i Kronos2

Tabel 1

| Mia. kr., gennemsnit pr. bankdag | 2017 | 2018 | 2019 | 2020 | 2021 |
|--|--------------|--------------|--------------|--------------|--------------|
| Interbankbetalinger | 74,0 | 83,0 | 87,4 | 87,6 | 88,7 |
| - Heraf kundebetalinger | 11,5 | 13,6 | 14,0 | 14,0 | 16,6 |
| Pengepolitiske operationer | 39,9 | 36,9 | 48,4 | 34,5 | 6,1 |
| - Heraf salg af indskudsbeviser | 39,9 | 36,9 | 48,4 | 33,3 | 5,6 |
| - Heraf pengepolitiske udlån | 0,0 | 0,0 | 0,0 | 1,3 | 0,5 |
| Overførsler til afviklingssystemer | 316,3 | 237,3 | 115,1 | 113,8 | 106,1 |
| - Heraf til Sum-, Intradag- og Straksclearingen ¹ | 273,8 | 177,2 | 40,5 | 39,9 | 40,6 |
| - Heraf til ES-CPH-afviklingen (tidligere VP-afviklingen) | 32,5 | 40,6 | 46,4 | 41,2 | 38,3 |
| - Heraf til CLS | 10,0 | 19,6 | 28,2 | 32,8 | 27,2 |
| Afviklede nettopositioner | 24,8 | 24,1 | 16,3 | 16,6 | 17,0 |
| - Heraf Sum-, Intradag- og Straksclearingen | 8,0 | 8,1 | 8,3 | 8,3 | 9,3 |
| - Heraf ES-CPH-afviklingen ² | 10,1 | 9,1 | 1,0 | 0,9 | 0,8 |
| - Heraf CLS | 6,7 | 6,8 | 7,0 | 7,3 | 6,8 |

1. Det store fald i overførsler til Sum-, Intradag- og Straksclearingen i 2018 og 2019 skyldtes Nationalbankens udskiftning af Kronos med Kronos2 i august 2018. Tidligere blev hele deltagerens disponible foliolikviditet overført til nattens afviklinger ved funktionen "Mest muligt" i Kronos. Med Kronos2 hentes der automatisk den nødvendige likviditet til de natlige afviklinger i Sum- og Intradagclearingen.
2. Tilslutningen af danske kroner til Target2-Securities, T2S, i oktober 2018 havde også betydning for afviklingen i Kronos2. Efter tilslutningen er de professionelle aktørers afvikling flyttet til T2S, mens de private investorers handler fortsat afvikles på ES-CPH's, tidligere VP's, egen platform. Afviklingen i nettopositioner fra VP-afviklingen faldt fra 9,1 mia. kr. i 2018 til 1,0 mia. kr. i 2019.

Nationalbanken har endvidere udarbejdet en ny stresstestanalyse af likviditeten i Kronos2. Stress-testen undersøger systemets robusthed over for stød til deltagerens likviditet under ekstreme, men plausible scenarier. Det kan fx være en stor deltager, der ikke kan afsende betalinger en hel dag, nedbrud i en datacentral, eller at deltagerens mulighed for at låne intradag i Nationalbanken reduceres ved et stød til deltagerens sikkerhedsstillelse. Stresstestens scenarier er simuleret for hver bankdag i perioden september 2018 til december 2021. Testen viser, at effekterne af scenarierne generelt er begrænsede.

Dog er der enkelte dage, hvor nogle af scenarierne har markante effekter. Nationalbanken kan modgå disse effekter ved at udføre betalinger på deltagerens vegne som nødprocedure. Analysen viser, at værdien af uafviklede betalinger kan halveres ved at gennemføre et begrænset antal betalinger i nødprocedure. Dermed reduceres de uønskede effekter af stød til deltagerens likviditet betydeligt.

Internationale standarder

Nationalbanken har i 2021 færdiggjort en vurdering af Kronos2 efter CPMI-IOSCO's principper for

finansiell markedsinfrastruktur.¹³ Vurderingen viste, at Kronos2 i høj grad efterlever internationale krav til organisering, risikostyring, sikkerhed, effektivitet og beredskab. Samtidig blev der ved vurderingen identificeret forbedringspotentialer, der kan styrke indsatsen inden for bl.a. governance, risikostyring og beredskab. Nationalbanken har gennemført eller igangsat arbejde på disse områder.

Nationalbanken har bl.a. styrket den løbende rapportering til ledelsen om styringen af risici og imødegående tiltag. Der er også sikret en yderligere formalisering og forankring af ansvaret for risikostyringen hos systemejer i 1. forsvarslinje. Konkret er systemejerens involvering og opfølgning i forhold til compliance-relaterede og operationelle risici blevet udvidet. Herudover har Nationalbanken styrket deltagerens inddragelse i risikostyringsarbejdet, både ved deltagelse i test af Nationalbankens nødløsninger samt vidensdeling på faste møder mellem Nationalbanken og deltagerne.

Nationalbanken arbejder desuden med en yderligere formalisering af, hvilke årlige tekniske test der skal gennemføres.

I 2021 har Nationalbanken analyseret risikoen ved indirekte deltagelse i betalingsafviklingen i Kronos2. Indirekte deltagere er deltagere, som har indgået en aftale med en direkte deltager om, at betalinger gennemføres via den direkte deltagers konto i Kronos2. Analysen viser, at den indirekte deltagelse er koncentreret hos de største deltagere, og ud fra transaktionsdata ses det, at indirekte deltagelse ikke giver anledning til bekymring ift. betalingsafviklingen i Kronos2. Der er desuden fastsat rammer for regelmæssige genbesøg af risici ved indirekte deltagelse.

I 2021 har Nationalbanken, som beskrevet ovenfor, udarbejdet en ny stresstestanalyse af likviditeten i Kronos2, og der er udarbejdet rammer for regelmæssige stresstest og håndtering af resultaterne.

Ved at gennemføre regelmæssige analyser af risikoen ved indirekte deltagelse samt likviditetsstresstest efterlever Nationalbanken CPMI-IOSCO's principper.

Cyberrobusthed

Nationalbanken arbejder løbende på at styrke cyberrobustheden i systemerne omkring Kronos2 for at forebygge og forhindre cyberkriminalitet.

Nationalbanken har tidligere indført krav i kontobestemmelserne om, at deltagere i Kronos2, der er forbundet via SWIFT, skal efterleve SWIFT's Customer Security Programme, CSP. SWIFT's CSP er obligatoriske sikkerhedskontroller, der har til formål at forhindre og opdage svig. Nationalbanken har i 2021 indsamlet og fulgt op på deltagerens CSP-selvattesteringer, og der arbejdes på at stille lignende krav til ikke-SWIFT-deltagere. Disse krav vil forventeligt tage udgangspunkt i Finans Danmarks cybersikkerheds-håndbog.

Et vigtigt element i arbejdet med cyberrobusthed er at sikre, at de mest kritiske forretningsaktiviteter i Kronos2 også kan videreføres i ekstreme, men plausible scenarier, hvor begge Kronos2's driftscentre er nede, fx som følge af cyberangreb. I sådanne tilfælde har Nationalbanken en isoleret Extreme Contingency Facility, ECF, der er en nødløsning til afvikling af kritiske betalinger. I 2021 er ECF-løsningen blevet testet med deltagerne og tilsluttede betalings- og afviklingssystemer. Nationalbanken og Finans Danmark har derudover i 2021 indgået aftale om, at Nationalbanken i sådanne ekstreme tilfælde kan opfordre deltagerne til at afvikle så mange betalinger som muligt via Intradagclearingen. Sammen med ECF'en er dette med til at øge visheden for, at betalingsafviklingen i Kronos2 kan håndteres i krisituationer, også over en længere periode.

Systemændringer

I 2021 blev Nationalbankens porteføljestyringsystem til sikkerhedsstillelse, Calypso, opgraderet og overgik i den forbindelse til en cloudbaseret løsning hos Adenza. Opgraderingen har styrket driftsstabiliteten af systemet og givet flere tekniske funktioniteter, der understøtter risikostyringen i forbindelse med Nationalbankens kreditgivning inden for dagen. Opgraderingen af Calypso skete endvidere som et led i klargøringen til den planlagte migrering af danske kroner til den europæiske betalings- og værdipapirafviklings-platform, Target Services, se boks 2.

¹³ Danmarks Nationalbank, Vurdering af Kronos2, *Danmarks Nationalbank Rapport*, nr. 4, december 2021 ([link](#)).

Danske kroner på Target Services i 2025

Boks 2

I 2020 besluttede Danmarks Nationalbank på baggrund af en foranalyse og dialog med den finansielle sektor at migrere afviklingen af danske kroner til den kommende europæiske konsoliderede betalings- og værdipapirafviklingsplatform, Target Services. Migreringen er planlagt til at finde sted i påsken 2025.

Target Services består i dag af RTGS-systemet Target2, værdipapirafviklingssystemet T2S (Target2-Securities) og afviklingssystemet for straksbetalinger TIPS (Target Instant Payment System). Target2 understøtter i dag kun afvikling af euro, men som en del af det europæiske konsolideringsprojekt, der fra november 2022 samler de tre systemer på én platform, moderniseres og omdøbes Target2 til T2 og vil derefter understøtte flere valutaer, ligesom det allerede er tilfældet for T2S.

En del af de danske værdipapirhandler er blevet afviklet på T2S siden 2018. Ved migreringen af kroneafviklingen til T2 i 2025 erstattes Kronos2 med T2, og desuden bliver danske kroner tilsluttet TIPS. Dermed samles al kroneafvikling på Target Services.

I forlængelse af den foranalyse, der førte til beslutningen om at migrere danske kroner til Target Services, igangsatte Nationalbanken i begyndelsen af 2021 et implementeringsprogram, som betegnes Target DKK.

Programmet gennemføres i tæt samarbejde og koordination med ECB og driftsoperatøren 4CB (de fire centralbanker Tyskland, Frankrig, Italien og Spanien). Derudover arbejdes der tæt sammen med den danske finansielle sektor og de øvrige systemejere i betalingsinfrastrukturen. Samarbejdet

er organiseret i en referencegruppe og en sektorgruppe på højt ledelsesniveau, som begge følger Target DKK tæt. Derudover er der etableret arbejdsgrupper med deltagelse af eksperter fra sektoren, som bl.a. bidrager til at afklare likviditetsmæssige og tekniske aspekter af den kommende løsning samt til at planlægge og koordinere test- og go-live-aktiviteter i sektoren.

Programmets afklaringsfase blev afsluttet ved udgangen af 1. kvartal 2022. Løsningen ligger nu fast, og arbejdet med design og udvikling af de dele af løsningen, der skal udvikles, er i gang. Det drejer sig bl.a. om integrationer til og fra Target Services og om understøttelsen af de forretningsområder, som ikke er omfattet af Target Services – nærmere bestemt sikkerhedsstilling og det danske pengepolitiske instrumentarium, som skal understøttes af systemer hos Nationalbanken.

Ift. Target Services er det afklaret, hvilke tilpasninger der er nødvendige for at understøtte særlige danske behov, og ECB er i gang med at detailbehandle Nationalbankens anmodning om de nødvendige tilpasninger. Tilpasningerne er holdt på et minimum, idet Nationalbankens strategi så vidt muligt er at benytte Target Services som standardløsning.

Nationalbanken er herudover i gang med detailplanlægning af aktiviteterne forbundet med løsningsdesign og udvikling, test og go-live samt overgangen til drift og forvaltning.

Den overordnede plan er, at Nationalbankens test op imod Target Services begynder i løbet af 2023, og herefter vil der være test med sektoren frem mod go-live.

Detailbetalinger

Danske borgere og virksomheder gennemfører de fleste betalinger med elektroniske betalingsløsninger som fx Dankort, mobilbetalinger, Betalingsservice eller overførsler via netbank. Der blev gennemført transaktioner med disse betalingsløsninger for 31,7 mia. kr. i gennemsnit pr. dag¹⁴ i 2021.

Nationalbanken overvåger de vigtigste danske betalingsløsninger. På nuværende tidspunkt omfatter overvågningen Dankort og Betalingsservice. Desuden overvåges konto til konto-overførsler som led i Nationalbankens overvågning af detailclearingerne.

Nationalbanken tager løbende stilling til, om der er behov for målrettet overvågning af andre betalingsløsninger, hvis de har fået en mere fremtrædende rolle på det danske marked, se boks 3.

Ny systemejer for Betalingsservice

Nationalbankens overvågning af Dankort og Betalingsservice har hidtil været rettet mod Nets, idet selskabet i lang tid har været systemejer for begge betalingsløsninger. I 2021 gennemførte Mastercard en aftale med Nets om køb af bl.a. Betalingsservice, som Mastercard dermed er ny systemejer for. Efter dette er Dankort og Betalingsservice underlagt adskilt overvågning, som Nationalbanken retter mod henholdsvis Nets og Mastercard.

Nets' ydelser vedrørende Betalingsservice

I forbindelse med Nets' salg af Betalingsservice til Mastercard har selskaberne indgået en serviceaftale om it-infrastruktur og sikkerhed¹⁵, der forpligter Nets til at understøtte driften af Betalingsservice i en overgangsperiode på op til tre år. Mastercard arbejder sammen med Nets henimod at overtage driften af Betalingsservice fra Nets via gennemførelsen af en "Separation Plan" for de relevante tjenester. Hvad angår de kritiske tjenester, som Kyndryl (tidligere IBM) leverer til Betalingsservice, skal kontrakterne erstattes, så der etableres et aftaleforhold mellem Mastercard og Kyndryl.

Betalingsløsninger i vækst i Danmark

Boks 3

Nationalbanken følger løbende udviklingen på det danske betalingsmarked og overvåger de betalingsløsninger, der har størst betydning for danske borgere og virksomheder.

MobilePay og internationale betalingskort som Visa og Mastercard har fået en større rolle på det danske betalingsmarked i de seneste år – de internationale betalingskort bl.a. fordi de anvendes i mobilbetalinger med Apple Pay og Google Pay.

Ifølge Nationalbankens seneste undersøgelse og analyse af de danske borgeres betalingsvaner¹ blev hver femte betaling i butikkerne foretaget med mobiltelefonen i 2021 – mere end en fordobling siden 2019. Undersøgelsen viser også, at 42 pct. af mobilbetalingerne blev foretaget med Apple Pay, mens MobilePay og Google Pay stod for henholdsvis 22 pct. og 6 pct. Betalinger med Apple Pay og Google Pay er hidtil sket via de internationale betalingskort, som dermed er vokset i betydning i Danmark.

I 2021 var det gennemsnitlige transaktionsomfang for de internationale betalingskort 0,7 mia. kr. pr. dag,² og for MobilePay lå det på 0,4 mia. kr. pr. dag.³ Til sammenligning udgjorde værdien af betalinger med Dankort, som er omfattet af Nationalbankens overvågning, i gennemsnit 1,1 mia. kr. pr. dag i 2021.⁴

1. Danmarks Nationalbank, Danmark er blandt de mest digitaliserede lande på betalingsområdet, *Danmarks Nationalbank Analyse*, nr. 2, februar 2022.
2. Nationalbankens statistikbank – DNBSTS-tabellen (sammenholdt med oplysninger fra Nets' statistik for Dankort).
3. MobilePay, ([link](#)).
4. Nets' statistik for Dankort.

¹⁴ Værdien af transaktionerne i detailbetalingssystemerne opgjort pr. kalenderdag, jf. afsnittet *Clearing og afvikling af detailbetalinger*.

¹⁵ The Transitional Service Agreement (TSA) – Schedule 07, IT Infrastructure & Security: Nets is to provide a reliable and secure service to Mastercard in order to run and operate the platforms.

Overvågningen følger løbende med i Mastercards leverandørstyring og arbejdet med overdragelse af tjenesterne.

Nets fusioneret med Nexi og SIA

Nets er over de sidste to år blevet fusioneret med de italienske virksomheder Nexi og SIA.

Efter Europa-Kommissionens godkendelse blev fusionen mellem Nets og Nexi endeligt gennemført i juli 2021. I oktober 2021 fik SIA tilladelse fra Erhvervsstyrelsen til at erhverve en kvalificeret andel i Nets¹⁶, og de italienske konkurrencemyndigheder godkendte fusionen mellem SIA og Nexi. Det nye samlede selskab (Nets, Nexi og SIA) har været en realitet siden januar 2022.¹⁷

Fusionerne forventes ikke umiddelbart at få betydning for Dankort eller Nationalbankens overvågning heraf.

Driftsstabilitet

Driften af Dankort var overordnet tilfredsstillende i 2021. I løbet af året har der dog været to større hændelser.

Den 10. juni 2021 blev omkring 100.000 Dankort-transaktioner ikke bearbejdet korrekt i Nets' systemer. Disse transaktioner blev derfor ikke bogført på forretningernes og kortholdernes konti. Nets genindlæste efterfølgende transaktionerne, og forretningerne modtog pengene tirsdag den 22. juni.

Den 11. juni 2021 gik det centrale system for bearbejdning af Dankorttransaktioner ned på grund af overbelastning. Ifølge Nets skyldtes overbelastningen ekstraordinært mange transaktioner som følge af ophævelsen af Covid-19-restriktioner og godt vejr. Et stort antal transaktioner blev afvist fra klokken halv fire om eftermiddagen og ca. halvanden time frem. I mange forretninger blev problemet dog løst ved at gå over til at gennemføre transaktioner i terminalerne offline. Hændelsen blev til sidst ordnet ved at tilføre systemet mere kapacitet og behand-

lingskraft. Nets har desuden gennemført tiltag for at undgå lignende hændelser i fremtiden ved at sikre driften med en betryggende kapacitetsplan.

Nationalbanken vurderer, at Nets' håndtering af og opfølgning på hændelserne har været tilfredsstillende.

For Betalingservice var driftsstabiliteten høj i 2021, og der har ikke været hændelser af betydning.

Misbruget af Dankort uændret

I 2021 lå misbruget af Dankort på 17,8 mio. kr. og var dermed på omtrent samme niveau som i 2020. Set i forhold til det samlede forbrug med Dankort udgjorde misbruget fortsat 0,05 promille.¹⁸

Hovedparten af misbruget af Dankort sker i butikker og hæveautomater på grund af tyveri eller tab af kort. Denne type misbrug steg med 58 pct. i 2021 til 12,8 mio. kr.¹⁹. Ifølge Nets skyldes stigningen, at samfundet og særligt nattelivet efter en længere periode med Covid-19-restriktioner er blevet genåbnet. Derudover har nyere former for tricktyveri ramt fx ældre kortholdere.

Til gengæld faldt misbruget af Dankort ved handel på nettet i 2021 med 49 pct. sammenlignet med året før.²⁰ Udviklingen kan i vid udstrækning tilskrives, at der fra januar 2021 har været krav efter PSD2, Revised Payment Service Directive 2, om brug af to-faktor-autentifikation ved kortbetalinger på nettet, som er blevet gennemført i Dankort Secured by Nets. PSD2 har derudover også medført, at grænsen for, hvornår Dankort Secured by Nets skal anvendes, blev nedsat fra 450 kr. til 225 kr. i januar 2021.

Misbruget af Dankort på nettet som andel af det samlede forbrug med Dankort på nettet er nu faldet hvert år siden 2016, jf. figur 2.

Misbrug af Betalingservice

Der har ikke været misbrug af Betalingservice i 2021.

16 I henhold til den nye investeringscreeningslov.

17 Nets, Nexi, Nets and SIA becomes Nexi Group, (*link*).

18 Nets' statistik for misbrug af Dankort.

(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).

19 Nets' statistik for misbrug af Dankort.

20 Nets' statistik for misbrug af Dankort.

Internationale standarder

Mastercard har i løbet af 2021 og begyndelsen af 2022 arbejdet videre med opfølgningen på Nationalbankens vurdering af Betalingsservice efter ECB's standarder.²¹ Mastercard har nu imødekommet de sidste udestående anbefalinger og bemærkninger, som vedrører arbejdet med at styrke håndteringen af kritiske leverandører, it-risikostyringen og netværksovervågningen.

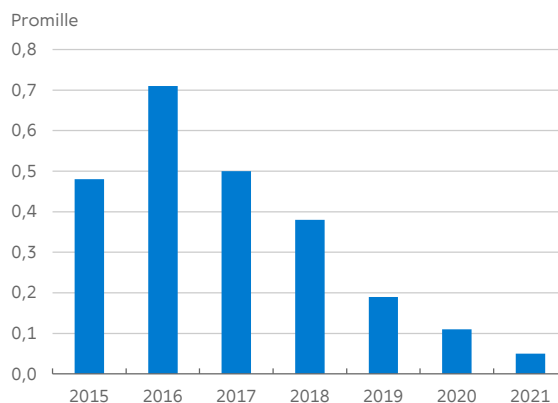
ECB har opdateret standarderne for betalingsløsninger som fx Dankort og Betalingsservice. Det nye rammeværk går under betegnelsen "PISA", som står for Payment Instruments, Schemes & Arrangements (Eurosystem oversight framework). For at harmonisere på betalingsområdet bygger PISA på kravene i de overvågningsstandarder, som anvendes til centrale betalingsystemer – se boks 4.

Med PISA videreføres de nuværende krav i ECB-standarderne i vidt omfang – i særdeleshed med hensyn til de centrale krav. PISA blev offentliggjort i november 2021.²²

Nationalbanken har underrettet Nets og Mastercard om ændringen med henblik på at indlede en dialog om, hvilken betydning de opdaterede standarder har for Dankort og Betalingsservice. I Eurosystemet er datoen for overgangen til PISA den 15. november 2022.

Misbrug af Dankort på nettet (som del af det samlede forbrug med Dankort på nettet)

Figur 2



Kilde: Nets.

PISA – opdaterede standarder for betalingsløsninger

Boks 4

ECB har sammen med centralbankerne i euroområdet opdateret kravene til elektroniske betalingsløsninger og overvågningsrammen for samme. Med PISA er ECB's nuværende standarder (assessment guides) blevet samlet i ét fælles rammeværk, som er baseret på og ensrettet med CPMI-IOSCO's principper for finansielle markedsinfrastrukturer, PFMI. Fokus ligger fortsat på betalingsløsningernes sikkerhed og effektivitet.

Udover et hensyn til harmonisering på betalingsområdet afspejler kravene i PISA den seneste teknologiske og lovgivningsmæssige udvikling, herunder fremkomsten af kryptoaktiver, elektroniske tegnebøger (wallets), PSD2 og EMD2, Electronic Money Directive 2. Overvågningsrammen er dermed udvidet til at omfatte disse løsninger.

Overordnet set viderefører PISA de nuværende krav i ECB's assessment guides i vidt omfang – især med hensyn til de centrale krav på de væsentligste områder, herunder legal basis, governance, access, comprehensive risk management og efficiency. Den væsentligste forskel mellem de eksisterende krav i ECB's assessment guides og PISA er, at PISA stiller tydeligere krav på visse områder – fx i forhold til risici vedrørende betalingstjenesteudbydere misligholdelse af forpligtelser, indløsning af betalinger, operationel robusthed og oplysning af centrale forhold i en betalingsordning (scheme eller arrangement).

21 Danmarks Nationalbank, Vurdering af Betalingsservice, Danmarks Nationalbank Rapport, nr. 4, oktober 2019 ([link](#)).

22 Eurosystem publishes new framework for overseeing electronic payments, november 2021 ([link](#)).

Clearing og afvikling af detailbetalinger

Sum-, Intradag- og Straksclearingen er den finansielle sektors systemer til clearing og afvikling af danske detailbetalinger. Systemerne ejes af Finans Danmark, forvaltes af e-nettet og leveres af Mastercard.

I Sumclearingen cleares betalinger foretaget med bl.a. kort og Betalingsservice én gang i døgnet på bankdage. I Intradagclearingen cleares konto til konto-overførsler som fx netbank-overførsler, løn-udbetalinger og offentlige udbetalinger. Bankernes nettopositioner – svarende til summen af betalinger til og fra bankernes kunder – opgøres i systemerne på faste tidspunkter. Nettopositionerne sendes til Kronos2, der udveksler beløbene 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 mellem bankerne sker seks gange om dagen på bankdage. Straksclearingen anvendes primært til netbank-overførsler og til betalinger via MobilePay.

Brug

Der er 50 direkte deltagere i detailclearingerne og 24 indirekte deltagere, som afvikler gennem en direkte deltager. Værdien af transaktionerne i systemerne udgjorde i gennemsnit 46,1 mia. kr. pr. bankdag i 2021, hvilket er en markant stigning sammenlignet med tidligere år, jf. tabel 2.

Antallet af transaktioner i Straksclearingen er steget i 2021 efter et uændret niveau fra 2019 til 2020, jf. figur 3.

Driftsstabilitet

Driften af detailclearingerne er i 2021 forløbet tilfredsstillende, og der har ikke været hændelser, som det har været nødvendigt for Nationalbanken at følge op på.

En hændelse i en anden del af betalingsinfrastrukturen betød dog, at detailclearingernes beredskab blev aktiveret, da der var bekymring for, om hændelsen ville få indflydelse for afviklingen af detailbetalinger. Hændelsen blev imidlertid håndteret uden at give anledning til forsinkelser i detailclearingerne.

Værdi af transaktioner i Sum-, Intradag- og Straksclearingen

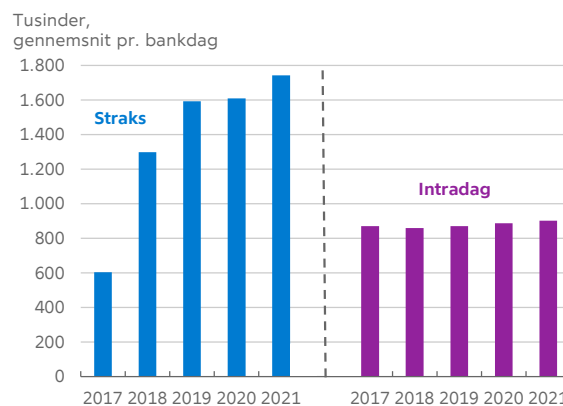
Tabel 2

| Mia. kr., gennemsnit pr. bankdag | 2017 | 2018 | 2019 | 2020 | 2021 |
|----------------------------------|------|------|------|------|------|
| Sumclearingen | 17,8 | 18,3 | 19,2 | 18,7 | 20,5 |
| Intradagclearingen | 19,7 | 20,1 | 20,8 | 21,9 | 23,9 |
| Straksclearingen | 0,9 | 1,2 | 1,4 | 1,6 | 1,7 |
| I alt | 38,4 | 39,6 | 41,4 | 42,2 | 46,1 |

Kilde: Mastercard.

Antal transaktioner i Intradag- og Straksclearingen, 2017-2021

Figur 3



Kilde: Mastercard.

Likviditet

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

De fleste af bankerne anvender systemernes automatiserede værktøjer til likviditetsstyring, og der har i 2021 ikke været hændelser, hvor deltagere er blevet henlagt på grund af manglende likviditet.

Cyberrobusthed

Finans Danmark arbejder løbende på at styrke cyberrobustheden i detailbetalingsinfrastrukturen. Der er senest blevet introduceret en cybersikkerhedshåndbog, som indeholder it-sikkerhedskrav, som bankerne og Mastercard skal implementere og rapportere deres efterlevelse af.

Mastercard foretog ved udgangen af 2021 en selvevaluering, som viste, at de efterlever kravene i cybersikkerhedshåndbogen. Bankerne har ligeledes rapporteret deres efterlevelse af kravene til Finans Danmark.

Nationalbanken er ved at vurdere detailclearingerne efter CPMI-IOSCO's retningslinjer for cybersikkerhed. Vurderingen forventes afsluttet medio 2022.

Systemændringer

Finans Danmark arbejder på at forhøje beløbsgrænsen i Straksclearingen, som i øjeblikket er på 500.000 kr. Ifølge Finans Danmark oplever bankerne et stigende behov for at lave store betalinger i realtid. Det er særligt i forbindelse med virksomhedsbetalinger, bankskifte mv. Derudover ser Finans Danmark en forhøjelse af beløbsgrænsen som et naturligt skridt i retningen mod udbredelsen af straksbetalinger.

Finans Danmark har udarbejdet en række krav for bankernes brug af Straksclearingen, som skal efterleves i forbindelse med en evt. forhøjelse af beløbsgrænsen. Der er bl.a. krav om overvågning af betalinger, så mistænkelige overførsler opdages, differentierede beløbsgrænser for afsendelse af straksbetalinger, bl.a. via kundesegmentering, samt mulighed for hurtig tilbagekaldelse af transaktioner.

Drift af detailclearingerne overtaget af Mastercard

Mastercard købte og overtog i 2021 de områder af Nets' infrastruktur, der omfatter drift af detailclearingerne. I forbindelse med overtagelsen indgik parterne en aftale om, at Nets i en overgangsperiode fortsætter med at drifte detailclearingerne som Mastercards leverandør.

Mastercard har nu anmodet Finans Danmark om samtykke til at flytte driften af Intraday- og Straksclearingen fra Nets' eksisterende datacentre i Norge til Mastercards egne datacentre i henholdsvis Norge og Sverige. Datacentrene er de samme, som skal anvendes til at drive P27. Sumclearingen skal fortsat driftes af Kyndryl (tidligere IBM).

Som en del af migreringen skal der udføres ændringer i den eksisterende opsætning, test og lignende. Flytningen til de nye datacentre, herunder tidspunkt, afventer nærmere analyse og koordinering før endelig godkendelse. Migreringen skal koordineres med TARGET DKK-projektet og sektorens program for fremtidens betalingsinfrastruktur.

Nets Sikkerhedspolitik og de underliggende standarder, der går under betegnelsen Nets Security Framework, er blevet videreført som Mastercard Security Framework. Rammeværket afspejler lovgivningsmæssige, kunderelaterede og branche-dikerede sikkerhedskrav til virksomheder, der driver kritisk infrastruktur. Mastercard har ligeledes beholdt Nets' risikorammeværk for clearingerne og arbejder på at tilpasse det til Mastercards eksisterende standarder og praksisser.

Nationalbanken og systemejeren Finans Danmark samt Nets og Mastercard har alle fokus på, at der er en sikker drift af detailclearingerne efter overgangen til Mastercard.

P27 – fælles detailbetalingssystem for Danmark, Sverige og Finland

Bankerne bag P27 har etableret selskabet P27 Nordic Payments i Sverige og valgt Mastercard som it-leverandør.

P27 vil som udenlandsk selskab ikke automatisk være omfattet af dansk lov og Nationalbankens tilsyns- og overvågningsbeføjelser²³. Nationalbanken og P27 har derfor aftalt en model, hvor P27 frivilligt indarbejder en klausul i deres aftalegrundlag, hvor det fremgår, at clearing og afvikling af danske kroner i P27's svenske system reguleres af dansk ret. Dermed vil P27 blive omfattet af dansk lov og Nationalbankens beføjelser.

²³ Tilsynsforpligtigheden i forhold til detailbetalingssystemer er, jf. kapitalmarkedsloven, placeret hos Nationalbanken. Det fremgår af kapitalmarkedsloven, at Nationalbanken overvåger betalingssystemer, som har væsentlig betydning for betalingsafviklingen.

Folketinget har samtidig vedtaget en ny lov, der skal sikre passende tilsyn og overvågning af de aktører, herunder udenlandske selskaber, der forestår clearing og afvikling af danske detailbetalinger. Loven trådte i kraft januar 2022 og giver danske myndigheder mulighed for at kræve, at systemisk vigtige betalingssystemer og deres it-leverandør etablerer sig i Danmark og dermed omfattes af dansk lov.

P27's nordiske detailbetalingssystem drøftes ligeledes mellem de nordiske centralbanker og finanstilsyn. Det er ambitionen at oprette et nordisk samarbejde om tilsyn og overvågning.

Sektorbeslutning om fremtidens betalingsinfrastruktur

I 2021 besluttede en samlet dansk sektor at arbejde henimod, at de eksisterende detailbetalingssystemer (Sum-, Intradag- og Straksclearingen) erstattes med P27's nordiske detailbetalingssystem.²⁴ Det er planen, at P27 skal gå live med danske kroner i påsken 2025, samtidig med at systemet tilslutter sig Target DKK.

Arbejdet er forankret i et sektorprogram for fremtidens betalingsinfrastruktur under Finans Danmarks bestyrelse, og der er nedsat en styregruppe med bred sektorrepræsentation, herunder af P27.

Programmet drives af e-nettet i tæt samarbejde med Finans Danmark.

²⁴ P27 er etableret af 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 i marts 2019.

Værdipapirafvikling

Værdipapirhandler kan indgås på forskellige måder: på børsen, gennem en multilateral handelsfacilitet eller bilateralt mellem parterne via en bank eller en mægler. Den endelige afvikling af handlerne, dvs. hvor penge og værdipapirer udveksles på deltageres konti, sker i to centrale systemer i den danske og europæiske finansielle infrastruktur:

Euronext Securities Copenhagen, ES-CPH, der indtil november 2021 hed VP Securities²⁵, driver det danske system for afvikling af værdipapirhandler. ES-CPH står også for håndtering af periodiske betalinger, emissioner, indfrielse mv. og er den eneste virksomhed i Danmark med tilladelse til at udstede og opbevare værdipapirer.

ES-CPH indgår i den paneuropæiske børs og markedsinfrastruktur-koncern Euronext Group. Euronext's opkøb af den danske værdipapircentral blev endeligt godkendt af Finanstilsynet i juni 2020, og siden er der pågået en større integrationsproces i ES-CPH. Formålet med processen er at effektivisere ES-CPH's organisation gennem synergier på tværs af koncernen og samtidig ensrette forretning og produkter i de fire værdipapircentraler i hhv. Italien, Norge, Portugal og Danmark, der alle er en del af Euronext.

Target2-Securities, T2S, er en fælleseuropæisk platform, hvor grænseoverskridende værdipapirhandler afvikles lige så effektivt som nationale handler. Siden oktober 2018 er en stor andel af afviklingen af værdipapirhandler i danske kroner blevet afviklet på T2S. T2S ejes af Eurosystemet og drives af de fire centralbanker i de største eurolande med ECB som koordinator.

Den danske model for afvikling af værdipapirhandler fungerer sådan, at de professionelle deltageres²⁶ indbyrdes værdipapirhandler afvikles på T2S, mens

private investorers handler afvikles gennem ES-CPH's eget afviklingssystem. Kroner til pengebenet i afviklingen af handlerne trækkes fra eller tilskrives deltagerens konti i Nationalbankens RTGS-system, Kronos2.²⁷ Registreringer af ændringerne i beholdningerne af værdipapirer sker på værdipapirkonti i ES-CPH.

Brug

ES-CPH's afviklingssystem har 86 deltagere, hvoraf 45 er udenlandske markedsdeltagere, herunder fire CCP'er²⁸. Ud af ES-CPH's deltagere har 48 en dedikeret pengekonto i Nationalbanken, der kan anvendes til afviklingen af kroner i T2S.

I 2021 blev der med over 100.000 afviklede handler i gennemsnit pr. bankdag, jf. tabel 3, sat ny rekord for ES-CPH. Det høje niveau blev især drevet af en stigning på 29 pct. i antallet af handler med investeringsbeviser. Aktiviteten var særlig høj i begyndelsen af 2021, jf. figur 4, der viser udviklingen i antal og værdi af handler med danskudstedte værdipapirer afviklet i hhv. T2S og ES-CPH's eget afviklingssystem. Værdimæssigt blev der samlet set afviklet for 226,4 mia. kr. i gennemsnit pr. bankdag, hvilket var lidt under niveauet året før. 2020 er dermed stadig året med den højeste afviklede værdi i ES-CPH nogensinde.

ES-CPH er som nævnt også ansvarlig for opbevaring af alle danskudstedte værdipapirer. Ved udgangen af 2021 var markedsværdien af værdipapirer opbevaret i ES-CPH 12.200 mia. kr., jf. figur 5, hvilket er en stigning på 46 pct. sammenlignet med januar 2018. Stigningen skyldes primært, at værdien af danskudstedte aktier opbevaret i ES-CPH næsten er fordoblet i perioden 2018-2021.

Driftsstabilitet

Driftsstabiliteten i afviklingen af danske værdipapir-

25 Navneskiftet er alene kommercielt, og den danske virksomhed er stadig registreret som VP Securities A/S i CVR-registeret.

26 Fx banker, institutionelle investorer og børsmæglere.

27 I T2S overføres der likviditet fra Kronos2 til T2S-plattformen, mens afviklingen af pengebenet i ES-CPH sker direkte på konti i Nationalbanken.

28 De fire udenlandske CCP'er i ES-CPH er hhv. EuroCCP, LCH Clearnet og Six X-clear, der clearer aktiehandler, mens Nasdaq Clearing AB clearer repoforretninger. Myndighedskontrollen med CCP'erne sker i såkaldte tilsynskollegier, hvor Finanstilsynet deltager i tilsynet med EuroCCP og Nasdaq Clearing AB.

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

Tabel 3

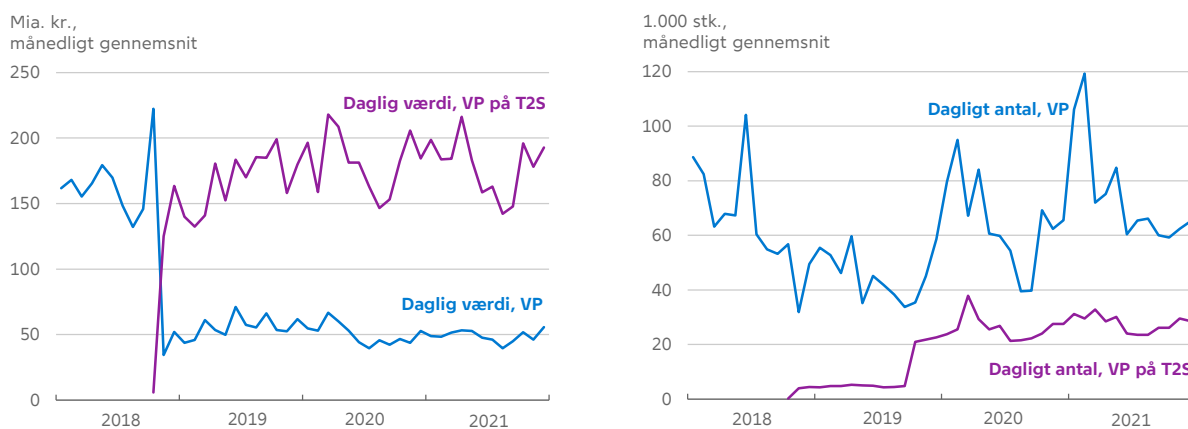
| År, gennemsnit pr. dag | I alt | | Obligationer | | Aktier | | Investerings- foreningsbeviser | |
|------------------------------|------------------------------|--------------------|------------------------------|--------------------|------------------------------|--------------------|-----------------------------------|--------------------|
| | Antal handler, tusinde | Værdi, mia. kr. | Antal handler, tusinde | Værdi, mia. kr. | Antal handler, tusinde | Værdi, mia. kr. | Antal handler, tusinde | Værdi, mia. kr. |
| 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 | 67,0 | 223,1 | 4,2 | 180,7 | 33,0 | 34,8 | 29,8 | 7,6 |
| 2020 | 90,5 | 231,5 | 3,8 | 178,1 | 49,0 | 43,5 | 37,7 | 9,9 |
| 2021 | 101,7 | 226,4 | 3,9 | 163,6 | 49,1 | 51,0 | 48,7 | 11,8 |

Anm.: Antal og værdi af transaktioner er opgjort samlet for ES-CPH og ES-CPH på T2S. Værdien er beregnet på baggrund af værdipapirbenet i en handel, dvs. markedsværdien af de papirer, sælger overdrager til køber.

Kilde: ES-CPH.

Antal og værdi af værdipapirhandler

Figur 4



Anm.: Figuren tv. viser antallet af afviklede handler, mens figuren th. viser værdien af handlerne, der er opgjort på baggrund af markedsværdien af de papirer, sælger overdrager til køber.

Kilde: ES-CPH.

handler har været tilfredsstillende i 2021. Der har i løbet af året været en række mindre hændelser, der kun i begrænset omfang påvirkede driften af ES-CPH's og T2S' systemer. En enkelt hændelse havde dog væsentlig indvirkning på afviklingsstabiliteten:

I november 2021 opstod en teknisk fejl i ES-CPH, der medførte forsinkelser i afviklingen af handler og en række relaterede gener for deltagerne i ES-CPH. Problemerne opstod efter systemopdateringer i hhv. T2S, SWIFT²⁹ og ES-CPH's egne systemer. Hændelsen strakte sig over to dage, hvorefter det lykkedes ES-CPH at identificere og afhjælpe hovedproblemerne og derved stabilisere afviklingen. En række følgevirkninger påvirkede i mindre grad driften i en periode på to uger derefter.

ES-CPH har udarbejdet en grundig rapport, der beskriver de initiativer, der er iværksat for at mindske risikoen for lignende fremtidige hændelser. Nationalbanken følger op på initiativerne som del af den løbende overvågning.

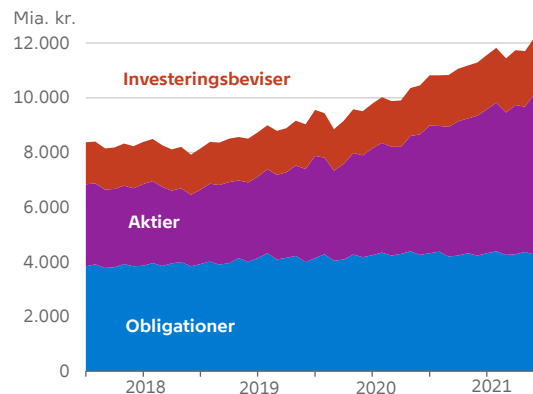
Afviklingsprocent

Afviklingsprocenten måler andelen af handelsomsætningen, der afvikles rettidigt. Ifølge den fælleseuropæiske regulering af værdipapircentraler, CSDR,³⁰ artikel 5, skal værdipapirhandler afvikles to dage efter, at handlerne er indgået, medmindre andet er aftalt mellem handlens parter.

Figur 6 viser afviklingsprocenten for hhv. ES-CPH's eget system og for ES-CPH's afvikling på T2S. Afviklingsprocenten i ES-CPH's eget system tog et dyk i de to sidste måneder af 2021 efter at have ligget på et stabilt niveau det meste af året. Dykket skyldtes problemerne omkring hændelsen i november 2021 i ES-CPH.

Markedsværdi af værdipapirer opbevaret i ES-CPH

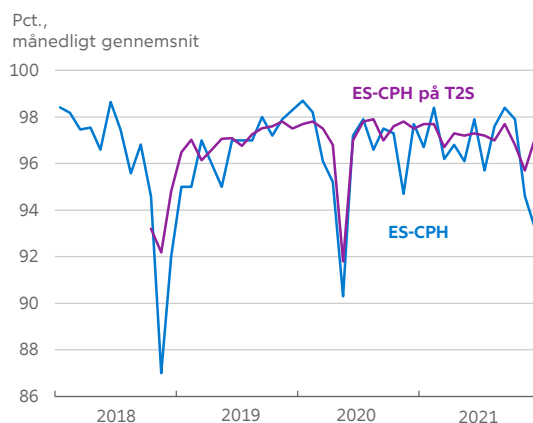
Figur 5



Kilde: ES-CPH.

Afviklingsprocent

Figur 6



Anm.: I figuren er afviklingsprocenten opgjort for antal transaktioner (handelsvolumen). Årsagen til det lave niveau i slutningen af 2018 var en række hændelser, der opstod i ugerne efter ES-CPH's tilslutning til T2S. Dykket i afviklingsprocenten i maj 2020 skyldes en større hændelse i T2S, der også påvirkede ES-CPH.

Kilde: ES-CPH.

29 Society for Worldwide Interbank Financial Telecommunications, SWIFT, er et selskab, der sikrer et standardiseret meddelelsesformat for finansiel telekommunikation.

30 Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union mv., der forkortes CSDR (*link*), har til hensigt at harmonisere tidspunkter og adfærd i forbindelse med værdipapirafviklingen samt reglerne for de værdipapircentraler (CSD'er), som driver afviklingsinfrastrukturen.

Sanktioner

Hvis en deltagers handler ikke afvikles rettidigt, kan det give problemer for deltagerens modparter, der på grund af de faldne handler måske ikke kan møde andre forpligtelser. I februar 2022 blev et nyt fælles-europæisk sanktionssystem taget i brug. Systemet, der er indført som del af CSDR, skal sanktionere deltagere, hvis handler ikke kan afvikles rettidigt som følge af manglende værdipapirer eller likviditet. Sanktionssystemet er beskrevet nærmere i boks 5.

Implementeringen af sanktionssystemet har krævet en række tekniske tilpasninger i både ES-CPH's og T2S' systemer. Særlig i forhold til sidstnævntes system har det medført en række udfordringer og hændelser. Driftsstabiliteten på den fælleseuropæiske platform har derfor været lavere i februar og marts 2022 sammenlignet med det ellers stabile driftsmæssige niveau i hele 2021.

Internationale standarder

Nationalbanken overvåger, at afviklingen af danske værdipapirhandler i ES-CPH og T2S lever op til internationale standarder for værdipapirafviklingssystemer.

For T2S sker overvågningen i samarbejde med alle de centralbanker, der er tilsluttet platformen, med ECB som hovedovervåger og koordinator, jf. afsnit om betalinger og værdipapirafvikling i euro.

Samtidig er værdipapirafviklingen som nævnt også reguleret af fælles lovgivning i EU, herunder CSDR. Finanstilsynet fører tilsyn med, at kravene i lovgivningen efterleves. I det omfang der er overlap mellem standarder og lovkrav, inddrages dokumentation fra Finanstilsynet om efterlevelsen af lovkrav i Nationalbankens overvågning.³¹

Nationalbankens seneste vurdering af ES-CPH's afviklingssystem efter CPMI-IOSCO's principper for finansielle markedsinfrastrukturer, PFMI, blev gennemført i 2016. ES-CPH har efterlevet alle de anbefalinger, som blev givet i vurderingen.

CSDR Settlement Discipline Regime

Boks 5

Sanktionssystemet, der er specificeret i de regulatoriske tekniske standarder (RTS) i CSDR-forordningen, har til formål at harmonisere værdipapirafvikling inden for EU. Det sker ved at sikre, at købere og sælgere modtager deres værdipapirer og penge til tiden og uden risici. For at nå dette mål indeholder RTS'erne en række foranstaltninger til forebyggelse og afhjælpning af fejl i afviklingen af værdipapirtransaktioner.

Som værdipapircentral, der opererer under en CSDR-licens, er ES-CPH forpligtet til at implementere det nye sanktionssystem. Dette har indvirkning på både ES-CPH's kunder og ES-CPH's egne systemer, da de nye funktioner vil blive introduceret til at understøtte bødeme-kanismer, obligatorisk delafregning og suspension af en deltager.

Kilde: Nationalbanken.

Cyberrobusthed

Nationalbanken færdiggjorde i 2020 en vurdering af ES-CPH's efterlevelse af CPMI-IOSCO's cyberguidance. Vurderingen viser, at ES-CPH har en høj modenhed og efterlever cyberguidance på de fleste områder. Der er dog også få men centrale områder, hvor ES-CPH ikke fuldt ud efterlever de internationale standarder. Nationalbanken har derfor givet ES-CPH en række anbefalinger, hvoraf 6 ud af 16 stadig er åbne, mens de resterende er efterlevet. Nationalbanken følger op på de åbne anbefalinger som del af den løbende overvågning.

Systemændringer

ES-CPH er som nævnt i gang med at tilpasse sin organisation, processer og produkter til Euronexts. Der arbejdes også på en fremtidig konsolidering af udvalgte services på en fælles cloud-baseret platform, der skal deles af de fire værdipapircentraler i koncernen. Indtil videre driftes alle ES-CPH's kritiske forretningsområder dog i egne separate og lokale systemer.

³¹ Nationalbanken er relevant myndighed for ES-CPH, jf. Artikel 12 i CSDR, og skal derfor underrettes om forhold, der vedrører værdipapircentralens efterlevelse af kravene i forordningen.

Betalinger og værdipapirafvikling i euro

Target2 og Target2-Securities (T2S) bruges af de danske banker til at afvikle betalinger og værdipapirhandlinger i euro. Systemerne ejes og drives af eurosystemet.

Det fælleseuropæiske RTGS-system, Target2, bruges til afvikling af store tidskritiske betalinger i euro. I Target2 overføres derudover likviditet til brug for afvikling i andre eurosystemer, herunder T2S. T2S er det fælleseuropæiske system til afvikling af værdipapirhandlinger i euro og danske kroner.³²

Brug

Der er 21 danske deltagere, som i 2021 gennemførte interbankbetalinger for i gennemsnit 9,5 mia. euro om dagen. De danske deltagere bruger hovedsageligt Target2 til at gennemføre koncerninterne betalinger og betalinger til udenlandske deltagere, jf. figur 7. Der udveksles flest euro med deltagere i Tyskland, Finland, Frankrig og Belgien.

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

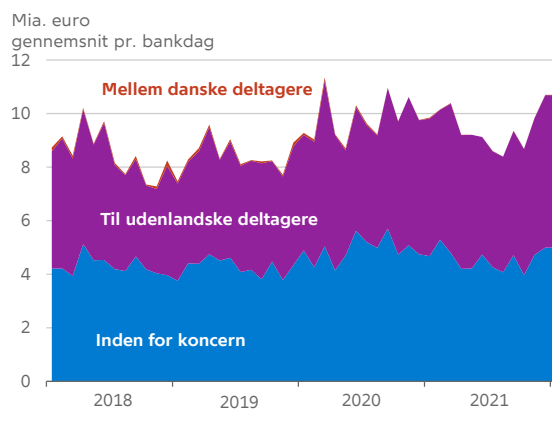
En T2S-afviklingskonto oprettes via en af centralbankerne i EU. 15 danske deltagere har via Nationalbanken en T2S-afviklingskonto til betaling eller modtagelse af euro i forbindelse med T2S-afviklingen. Andre danske deltagere kan have oprettet en T2S-afviklingskonto via andre EU-centralbanker.³³

Driftsstabilitet

Driftsstabiliteten i de lokale komponenter af Target2, som Nationalbanken har ansvaret for, har været tilfredsstillende i 2021.

Interbankbetalinger i Target2

Figur 7



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

Kilde: Danmarks Nationalbank.

En opgradering af T2S i juni 2021 påvirkede Nationalbankens Kronos2 og Kronos2-deltagerne. Hændelsen og hændelsesopfølgningen er beskrevet nærmere i afsnittet om interbankbetalinger.

Tilbage i 2020 var der fem større it-relaterede hændelser (ikke cyber-hændelser), der påvirkede afviklingen af betalinger og værdipapirer i Target2 og T2S. Som opfølgning på hændelserne bestilte ECB en ekstern undersøgelse af årsagerne og af de mere generelle procedurer og processer på udvalgte områder. Den eksterne undersøgelse blev foretaget af Deloitte. Undersøgelsen blev afsluttet med en rapport, der indeholder anbefalinger til, hvordan ECB kan styrke risikostyringsarbejdet på flere områder,

³² T2S kan håndtere flere valutaer. Ud over euro er danske kroner den eneste anden valuta tilsluttet til T2S. Læs om kroneafvikling i afsnittet *Værdipapirafvikling*.

³³ Da der ikke kan placeres euro permanent på T2S-afviklingskontoen, skal bankerne 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, mens nogle af de største banker via deres filial har etableret en Target2-konto i en centralbank i euroområdet.

herunder ændringsstyring, forretningsvidereførelse, governance mfl.³⁴. ECB har accepteret alle anbefalinger og har udarbejdet en samlet handlingsplan, der adresserer anbefalingerne fra både Deloitte, overvågningen og ECB's interne revision. I 2021 har ECB implementeret og initieret tiltag, der skal imødekomme de fleste af anbefalingerne. ECB forventer, at hovedparten af tiltagene i handlingsplanen er gennemført inden slutningen af 2022. Nationalbanken deltager i ECB's opfølgning på handlingsplanen i regi af den fælles overvågning af Target2 og T2S, jf. nedenfor.

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 2021 har Nationalbanken i regi af ECB deltaget i opfølgningen på en vurdering af T2S efter CPMI-IOSCO-principperne fra 2019.

Nationalbanken har i 2021 også bidraget til arbejdet med at vurdere T2S efter Cyber Resilience Oversight Expectations, CROE, der er ECB's udmøntning af CPMI-IOSCO's cyberguidance.

Systemændringer

ECB igangsatte i 2016 en større modernisering af den europæiske betalingsinfrastruktur og har lige siden arbejdet på en konsolidering af Target2, T2S og straksbetalingssystemet Target Instant Payment System, TIPS, på én it-plattform. Formålet er at imødekomme nye markedskrav og optimere deltagerens likviditetsstyring på tværs af alle Target Services.

Konsolideringen lanceres 21. november 2022. På denne dato migrerer alle tilsluttede centralbanker og deltagere fra Target2's Single Shared Platform over på den konsoliderede platform, T2 Service, på samme tid i et såkaldt big bang.

Som forberedelse til migreringen indledte centralbankerne deres testfase i juni 2021, og markedsdeltagerne påbegyndte deres testfase i december 2021. Testfaserne skal gøre centralbankerne og markedsdeltagerne fortrolige med systemet og dets opbygning, men har også til formål at finde eventuelle fejl.

Der afholdes flere test af selve migreringen, så centralbankerne og deltagere har afprøvet og testet migreringsplanen af flere omgange inden den endelige go-live i november 2022.

³⁴ European Central Bank, ECB publishes an independent review of TARGET incidents in 2020, Press release, 28 juli 2021 ([link](#)).

Valutahandelsafvikling

I en valutahandel indgår to modsatrettede betalinger i to forskellige valutaer. Valutahandler kan enten afvikles via korrespondentbanker eller via det internationale valutahandelsafviklingssystem, CLS, der afvikler handler i 18 tilsluttede valutaer. Langt hovedparten af valutahandler i danske kroner afvikles i CLS.

CLS Bank International (CLS) driver CLS-afviklingen og ejes af store internationale banker. I CLS-afviklingen indberetter deltagerne deres betalinger til CLS, hvorefter betalingerne matches af CLS, og de to betalinger i valutahandlen afvikles samtidigt (Payment-versus-Payment, PvP), hvilket fjerner risikoen mellem handlens parter.

Nationalbanken indgår i et samarbejde med andre centralbanker om overvågningen af CLS, jf. boks 6.

Brug

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.

Over 95 pct. af valutahandlerne i danske kroner gennemføres via CLS.³⁵ Den gennemsnitlige daglige værdi af handler i danske kroner var 280 mia. kr. i 2021 og var på niveau med 2020, jf. figur 8.

CLS indgik i 2020 et samarbejde med flere deltagere om at adressere risikoen ved valutahandler, der afvikles uden PvP³⁶. Når de to betalinger i en valuta-handel ikke gennemføres samtidig, påføres parterne en afviklingsrisiko, dvs. en risiko for, at modparten ikke betaler sin del af handlen. I juni 2021 startede CLS og deltagerne et pilotprojekt, der skal undersøge forskellige løsninger og finde det optimale design til en PvP-løsning for valutaer, som pt. ikke indgår i CLS-afviklingen.

35 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.

36 CLS, CLS announces collaboration with 12 global banks to pilot PvP solution for a wider range of currencies and market participants, september 2021 ([link](#)).

Overvågning af CLS

Boks 6

Overvågningen af CLS tager udgangspunkt i CP-MI-IOSCO's principper for sikre og effektive betalings-systemer. CLS offentliggør hvert andet år en opdateret beskrivelse af systemets efterlevelse af principperne.¹

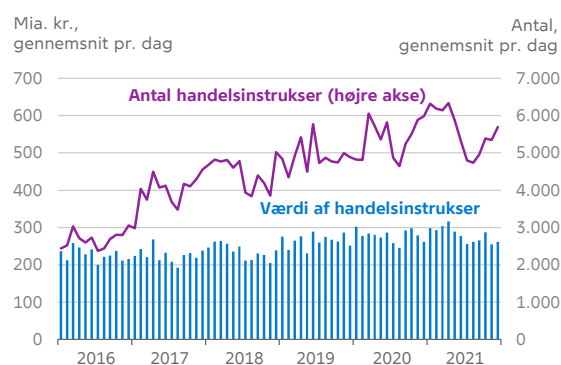
Overvågningen af CLS foregår i den fælles overvågningskomite, CLS Oversight Committee², der er et samarbejde mellem de tilsluttede valutaers centralbanker, som derigennem kan varetage deres nationale overvågningsforpligtelse. Nationalbanken deltager i samarbejdet, der ledes og koordineres af den amerikanske centralbank, Federal Reserve, som også er tilsynsmyndighed for CLS.

Nationalbankens overvågning af CLS har særligt fokus på forhold, der har betydning for afviklingen af handler i danske kroner.

1. CLS, Principles for Financial Market Infrastructures Disclosure, 2019 ([link](#)).
2. Federal Reserve System, Protocol for the Cooperative Oversight Arrangement of CLS ([link](#)).

Handelsinstruktioner i CLS

Figur 8



Kilde: CLS Bank.

Driftsstabilitet og likviditet

CLS-afviklingen foregår i et relativt kort tidsrum på døgnet, hvor de tilsluttede centralbankers RTGS-systemer – på tværs af tidszoner – er åbne samtidigt. Ind- og udbetalinger til CLS sker via RTGS-systemerne, for danske kroner via Kronos2. Driftsstabiliteten i CLS er derfor afhængig af stabiliteten i de tilsluttede RTGS-systemer for at gennemføre afviklingen inden for kritiske tidsfrister.

Der har i 2021 ikke været nogle hændelser i Kronos2, som har påvirket CLS-afviklingen.

De danske deltagere reserverer tilstrækkelig likviditet til CLS-afviklingen.

Systemændringer

I 2021 har CLS fuldført en migrering af alle sine afviklingsservices, herunder CLS-afviklingen, og samlet dem på en ny teknologisk platform kaldet Unified Services Platform, USP. Udover en optimeret, fleksibel og mere robust teknologisk platform har migreringen også ført til forbedret overvågning og alarmering samt mere automatisering til gavn for CLS' økosystem.³⁷

³⁷ CLS, CLS completes migration of its settlement service to new state-of-the-art technology platform, juli 2021 ([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 forfatterens igangværende analysearbejde. Serien henvender sig primært til fagpersoner. 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
LANGELINIE ALLÉ 47
2100 KØBENHAVN Ø
WWW.NATIONALBANKEN.DK

Redaktionen er afsluttet
8. april 2022



DANMARKS
NATIONALBANK

KONTAKT

Teis Hald Jensen
Kommunikations-
og presserådgiver

tehj@nationalbanken.dk
+45 3363 6066

SEKRETARIAT
OG KOMMUNIKATION