RAPPORT

DANMARKS NATIONALBANK

4. MAJ 2021 — NR. 3

Overvågning af den finansielle infrastruktur

- Danmark har en sikker, effektiv og robust betalingsinfrastruktur. Nationalbanken vurderer, at infrastrukturen i høj grad efterlever internationale standarders krav til organisering, risikostyring og beredskab.
- Cybertruslen er kompleks og udvikler sig hurtigt. SolarWind-hackerangrebet gav i 2020 eksempler på de sofistikerede teknikker, som de mest avancerede trusselsaktører på cyberområdet benytter sig af.
- Som følge af udviklingen i trusselsbilledet er arbejdet med cyberrobusthed et område, som kræver vedvarende udvikling og tilpasninger i infrastrukturen. Der sker løbende fremskridt, men Nationalbankens vurdering er, at der også er plads til forbedringer.

Samfundskritisk infrastruktur

639 mia. kr.

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

Læs mere

Samarbejde på tværs af den finansielle sektor

Cyberisiko

Nationalbanken organiserer samarbejde på sektorniveau om at reducere cyberrisici og øge den operationelle robusthed.

Læs mere

INDHOLD

Danmark har en sikker og effektiv finansiel infrastruktur

Det er afgørende for samfundsøkonomien, at varer, tjenester og finansielle aktiver kan udveksles. Det kræver, at betalinger og værdipapirhandler kan gennemføres sikkert og effektivt.

Den danske finansielle infrastruktur er det netværk af systemer, der muliggør, at borgere, virksomheder og finansielle aktører kan udveksle betalinger og værdipapirhandler med hinanden. På en gennemsnitlig bankdag cleares og afvikles der betalinger til en værdi af mere end 630 mia. kroner igennem de centrale it-systemer i den danske finansielle infrastruktur. Se boks 1 for en forklaring af begreberne clearing og afvikling.

Som følge af de centrale systemers kritiske rolle stilles der høje krav til deres driftsstabilitet og risikostyring. Virker systemerne ikke, skaber det forstyrrelser, der i værste fald kan true den finansielle stabilitet. Nationalbanken overvåger, at infrastrukturens centrale systemer efterlever internationale standarders krav til sikkerhed og effektivitet.[1] Overvågningen omfatter også de vigtigste betalingsløsninger. Systemer og løsninger i den danske finansielle infrastruktur er beskrevet i boks 2.

I denne rapport præsenteres hovedkonklusioner fra overvågningen og de væsentligste områder, der har haft betydning for den danske finansielle infrastruktur i 2020.

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

Driftsstabiliteten er høj, og der opleves sjældent forstyrrelser i udvekslingen af betalinger og afviklingen af værdipapirhandler.

De centrale systemer/løsninger i infrastrukturen efterlever 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)
- VP-afviklingen (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*).

Begreberne clearing og afvikling

Boks 1

For at borgere, virksomheder og finansielle aktører kan udveksle betalinger og gennemføre værdipapirhandler med hinanden, skal transaktionerne cleares og afvikles i infrastrukturens centrale systemer.

Clearing er betegnelsen for den aktivitet i systemerne, hvor betalinger eller værdipapirhandler gøres klar til at blive endeligt gennemført mellem deltagerne. Clearingen omfatter opgørelse, afstemning og bekræftelse af transaktionerne og i de fleste tilfælde såkaldt netting, hvilket vil sige modregning af tilgodehavender og forpligtelser, så hver deltager kun har én samlet nettoposition over for hver af de øvrige deltagere i systemet.

Afvikling er selve udvekslingen af beløb eller værdipapirer mellem deltagerne. I Kronos2 vil det sige forløbet fra en betaling debiteres afsenders konto, til betalingen krediteres modtagers konto. Ved afvikling af en værdipapirhandel udveksles penge og værdipapirer. Hvis afviklingen finder sted umiddelbart efter transaktionens indgåelse, kaldes det straksafvikling. Efter afvikling er transaktionen endelig. Afvikling kan både omfatte enkelttransaktioner og nettopositioner.

1 Overvågningen sker med udgangspunkt i CPMI-IOSCO's Principles for financial infrastructures (*link*).

Betalingsinfrastrukturen i Danmark

Boks 2

Hver bankdag[1] sendes i gennemsnit betalinger for 639 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 mellemled, ender de alt efter type med at blive opgjort og afstemt i Sum-, Intradag- eller Straksclearingen, der er den finansielle sektors detailbetalingssystemer. Afviklingen sker efterfølgende på konti i Nationalbanken via Kronos2. Detailbetalingssystemerne ejes af Finans Danmark.

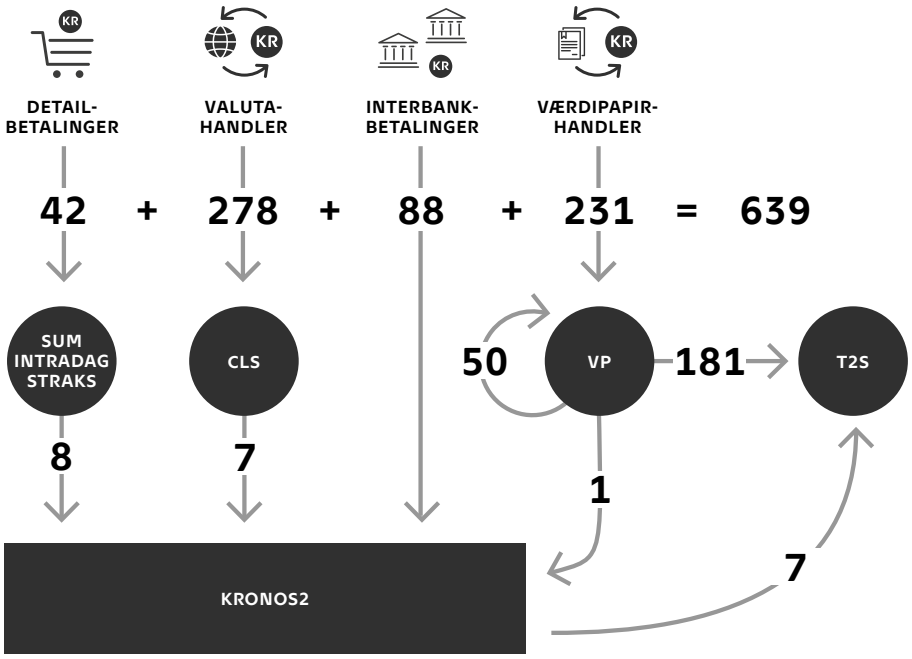
Værdipapirhandler kan indgås på mange forskellige typer markedspladser, bl.a. fondsbørsen, handelsplatforme eller "over-the-counter" via bank eller mægler. Den efterfølgende afvikling af handlerne sker for professionelle investorers vedkommende på den fælleseuropæiske platform Target2-Securities, T2S, der ejes af den Europæiske Centralbank, ECB. Deltagelse på T2S kræver pengekonto i Nationalbanken og værdipapirkonto i VP Securities (VP). VP 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 VP-afviklingen, der er VP'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 VP-afviklingen afvikler deres deltageres nettopositioner i Kronos2, hvor deltagerne har konti. Nettopositionerne beregnes i de respektive systemer ved at modregne deltagernes tilgodehavender og forpligtelser. Netting reducerer deltagernes likviditetsbehov betydeligt sammenlignet med en situation, hvor alle betalinger afvikles enkeltvist, fx reducerer netting likviditetsbehovet til afvikling af detailbetalinger fra 42 mia. kr. til 8 mia. kr. dagligt, svarende til en reduktion på 81 pct.

På T2S sker afviklingen af de professionelle investorers handler ved brug af såkaldt teknisk netting. Likviditeten til afviklingen overføres fra deltagernes pengekonti i Nationalbanken, og selve afviklingen sker i T2S.

Betalingsflow, mia. kr., gennemsnit pr. bankdag i 2020



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.

Udviklingen på it-området, herunder særligt ændringerne i trusselsbilledet på cyberområdet, betyder imidlertid, at kravene til systemerne og løsningerne i infrastrukturen løbende skærpes. Nationalbanken har i 2020 sat fokus på flere områder, hvor der er behov for en øget indsats. Det gælder særligt arbejdet med cyberrobusthed, beredskab, leverandørstyring samt organisation og ledelse i de virksomheder, der er ansvarlige for driften af de centrale systemer og løsninger i infrastrukturen.

Covid-19 har ikke påvirket driftsstabiliteten

Driftsstabiliteten i betalingsinfrastrukturen har i 2020 været høj og har ikke været påvirket af de ændrede vilkår under covid-19-pandemien. Der er i udstrakt grad gjort brug af hjemmearbejde, og den fysiske bemanding har kun omfattet særligt forretningskritisk personale, der endvidere er inddelt i flere teams for at undgå potentiel smittespredning. Håndteringen af de driftsforstyrrelser, der har været, er koordineret ved brug af virtuelle møder og fjernkommunikation.

SolarWind-angreb ramte infrastrukturen

I 2020 blev et af de hidtil mest omfattende cyberangreb opdaget. En fjendtlig aktør havde foretaget ondsindede ændringer i opdateringer af programmet SolarWinds Orion, der er anvendt af mange private og offentlige organisationer over hele verden. Angrebet ramte også den danske finansielle infrastruktur, men uden tegn på, at det har haft reelle konsekvenser. De relevante systemer blev inddæmmet og analyseret, så snart kompromitteringen af SolarWinds Orion blev kendt.

Angrebet var ikke målrettet mod systemer i infrastrukturen, hvilket kan have været medvirkende til, at det blev håndteret uden egentlige skadesvirkninger. SolarWind-hændelsen understreger behovet for effektive foranstaltninger, der modvirker risikoen for cyberangreb via software fra eksterne leverandører. Hackerangrebet via SolarWind Orion er beskrevet nærmere i boks 3.

Operationelle forstyrrelser kan ikke undgås, men skal kunne håndteres effektivt

Generelt vil risikoen for operationelle forstyrrelser i og imellem komplekse it-systemer ikke kunne undgås. Covid-19 og SolarWind-hackerangrebet er to forskellige eksempler på operationelle forstyrrelser, der er blevet håndteret af systemerne og løsningerne i den finansielle infrastruktur. Der sker også med varierende mellemrum tekniske forstyrrelser, fx i forbindelse med systemopdateringer eller som

Hackerangrebet via SolarWinds Orion Boks 3

I december 2020 kom det frem, at en meget veletableret leverandør af bl.a. netværksovervågning, SolarWinds, havde haft et sikkerhedsbrud. En avanceret og sandsynligvis statssponsoreret fjendtlig aktør havde foretaget ondsindede ændringer i visse opdateringer af programmet SolarWinds Orion, der anvendes af mange organisationer over hele verden. Med installeringen af en sådan forvansket opdatering fik de intetanende kunder dermed en trojansk hest indenfor murerne.

Via den skadelige kode ("Sunburst") i opdateringerne af SolarWinds Orion fik den fjendtlige aktør skabt en bagdør hos cirka 18.000 private og offentlige organisationer. I flere kendte tilfælde er bagdøren blevet udnyttet til videre hackerangreb mod nøje udvalgte mål – især i USA, hvor fx flere ministerier har oplevet, at fortrolige oplysninger er blevet tilgået. Men fx også den anerkendte it-sikkerhedsvirksomhed FireEye og Microsoft har været udsat for indtrængen i deres systemer.

Den centrale betalingsinfrastruktur i Danmark er i et tilfælde også blevet ramt, idet en opdatering af SolarWinds Orion med Sunburst har været installeret. Der er dog ingen tegn på, at pågældende bagdør er blevet udnyttet. I den konkrete sag blev der grebet hurtigt ind med nedlukning af de servere, som programmet var installeret på, så snart problemet blev opdaget.

Den kritiske forsyningsinfrastruktur i Danmark er på tilsvarende måde blevet ramt af SolarWinds Orion-angrebet. Bagdøren har været installeret i flere store energiselskabers it-systemer, men der er ikke konstateret indikationer på udnyttelse heraf. I selskabernes arbejde med opfølgning på angrebet er der identificeret behov for bedre datalogning, så man sikrer, at man kan undersøge, hvad der er sket. Dansk Energi har derfor foreslået, at de vigtigste virksomheder i den danske infrastruktur skal gemme datalogning og netværksovervågning i 12 måneder. Desuden vil der i den kommende tid blive installeret sensorer hos 200 energi- og forsyningsselskaber, som skal overvåge it-systemerne i forhold til hackerangreb.

følge af menneskelige fejl; forstyrrelser som dog typisk kun påvirker systemernes tilgængelighed i mindre grad. Der har også været få eksempler på større hændelser med mærkbare konsekvenser for borgere og virksomheder i Danmark.[2]

De ansvarlige for de centrale systemer/løsninger i infrastrukturen er overordnet set velforberedte i forhold til at håndtere traditionelle operationelle hændelser. Det er fx et krav, at systemerne skal driftes fra to separate og geografisk uafhængige it-driftscentre, så der hurtigt kan skiftes platform ved nedbrud i et af centrene. Det bliver løbende testet, om det er muligt at skifte platform og genoptage driften i løbet af 2 timer. 2-timerskravet bidrager til at sikre, at kritiske transaktioner kan gennemføres på den aftalte afviklingsdag.

Kompleksiteten på cyberområdet betyder imidlertid, at det er en særlig udfordring at sikre et effektivt beredskab til håndtering af cyberangreb. Det er væsentligt, at de centrale systemer/løsninger i infrastrukturen løbende identificerer og vurderer de forskellige typer trusler og sårbarheder, der er potentielle kilder til cyberrisici. Beredskabsplaner og planer for genopretning af it-systemer og videreførelse af kritiske forretningsområder skal struktureres med udgangspunkt i de hovedrisici, vurderingerne peger på. Endvidere skal planerne testes med udgangspunkt i de ekstreme men plausible scenarier, som et cyberangreb kan forårsage.

Nationalbanken overvåger løbende de centrale systemers arbejde med at lægge specifikke planer for at sikre en hurtig og sikker genopretning efter et cyberangreb. Der sker løbende fremskridt, men Nationalbankens vurdering er, at der også er plads til forbedringer.

Cybertruslen er en udfordring

Cybertruslen er kompleks og udvikler sig hurtigt. SolarWind-angrebet gav eksempler på de sofistikerede teknikker, som de mest avancerede trusselsaktører på cyberområdet benytter sig af. Som følge af udviklingen i trusselsbilledet er arbejdet med cyberrobusthed et område, som kræver vedvarende udvikling og tilpasninger; det er ikke et arbejde, man bliver "færdig" med.

Da truslen fra cyberangreb potentielt udgør en risiko for de finansielle virksomheders forretning, er det vigtigt, at den overordnede ramme for risikostyringen fastlægges af virksomhedernes topledelser, dvs. direktion og bestyrelse. Det skal sikre, at der er strategisk fokus og den rette prioritering i arbejdet med cyberrobusthed. Endvidere er ledelsen ansvarlig for at sikre, at der organisatorisk er en klar, synlig og praktiseret ansvars- og arbejdsfordeling mellem driftsansvarlige, de ansvarlige for kontrol og compliance og den uafhængige revision (de tre forsvarslinjer) i virksomhederne.

Nationalbanken har igangsat en proces, hvor de centrale systemer i infrastrukturen vurderes mod særskilte internationale retningslinjer for cyberrobusthed.[3] Det foreløbige arbejde viser, at det aktuelle cyberrobusthedsniveau generelt er højt. En positiv tendens er fx, at ledelsernes involvering i arbejdet med cyberrobusthed er steget betydeligt sammenlignet med observationer fra tidligere år. Vurderingerne peger også på fremskridt i de ansvarlige virksomheders øvrige organisering og risikostyring.

Nationalbankens vurderinger viser imidlertid også områder med plads til forbedringer. Systemernes evne til hurtig og sikker genopretning efter et cyberangreb er som nævnt et område, hvor Nationalbanken mener, der er plads til forbedringer. Et beslægtet område, der også har behov for øget fokus, er arbejdet med databeskyttelse. En effektiv brug af kryptering og backup skal sikre, at data ikke ødelægges eller på anden vis kompromitteres under et cyberangreb. Hvis kritiske data ikke er tilgængelige, vil det også i væsentlig grad påvirke systemernes evne til at genoprette driften.

2 Et eksempel var problemer hos IBM i januar 2014, der medførte et længerevarende nedbrud på dankortsystemet. Et andet eksempel var en systemfejl i Nationalbankens betalingssystem, Kronos2, der i august 2018 medførte forsinkelser i udbetalingen af løn og sociale ydelser.

3 Cybervurderingerne sker med udgangspunkt i CPMI-IOCSCO Guidance on cyber resilience for Financial Market Infrastructures (*link*), der supplerer de standarder, som Nationalbanken generelt set overvåger mod.

Nationalbankens anbefalinger fra cybervurderingerne deles på bilaterale møder med de systemansvarlige. Anbefalingerne offentliggøres ikke af sikkerhedshensyn.[4]

Fokus på leverandørstyring

Cyberangreb kan også ske via leverandører til infrastrukturen. Det er derfor vigtigt, at de centrale systemer/løsninger i infrastrukturen i tilstrækkelig grad indarbejder risici fra leverandører i deres egen risikostyring. Det skal sikre, at de ansvarlige virksomheder har et samlet overblik og dermed et godt grundlag at prioritere og adressere risici ud fra. Nationalbanken har løbende fokus på, at systemer/løsninger arbejder struktureret med de risici, som de påføres fra samarbejdet med deres leverandører.

En særlig problemstilling er, at der ikke er et særskilt myndighedsansvar for kontrollen med de kritiske it-driftsleverandører, hvilket kan være problematisk, givet den centrale rolle disse leverandører har. Der arbejdes med denne fælles europæiske problemstilling i EU, hvor Europa-Kommissionen har stillet forslag om nye beføjelser i Digital Operational Resilience ACT, DORA, jf. boks 4.

Bredere samarbejde om operationelle risici

En del af arbejdet med at mitigere cyberrisici og øge den operationelle robusthed sker på sektorniveau i forskellige sektorsamarbejder.

De ansvarlige for de centrale systemer i infrastrukturen, dvs. Nationalbankens eget system Kronos2, VP-afviklingen og Finans Danmarks detailbetalingssystemer, har siden 2016 på anbefaling af Nationalbanken indgået i et formaliseret samarbejde, hvor de gensidige afhængigheder og operationelle risici, der går på tværs af systemerne, identificeres og adresseres. Samarbejdet skal bidrage til, at der er effektive nødprocedurer og sikret redundante forbindelser mellem systemerne og til deltagerne i infrastrukturen.[5]

De centrale systemer/løsninger deltager også i FSOR, Finansielt Sektorforum for Operationel Robusthed,

Digital Operational Resilience Act (DORA) Boks 4

Europa-Kommissionen offentliggjorde den 24. september 2020 et forslag til en forordning om digital operationel robusthed i den finansielle sektor ("DORA"). Forslaget afspejler en af de strategiske prioriteringer i Europa-Kommissionens Digital Finance Package, nemlig behovet for at adressere udfordringer og risici forbundet med den digitale transformation af samfundet. I DORA fremsættes på den baggrund vidtgående krav til it-risikostyringen i de finansielle virksomheder.

Forslaget omfatter de fleste typer reguleret virksomhed på det finansielle område. Der er også bestemmelser i forslaget, som finder anvendelse på disse virksomheders it-leverandører, herunder cloud-computing-tjenester. Systemoperatører (som defineret i finalitydirektivet) er dog ikke omfattet – bl.a. med henvisning til, at de vigtigste betalingssystemer i forvejen er underlagt centralbankovervågning og tilhørende særskilt regulering.

Der sigtes i DORA på at ajourføre, samle og harmonisere regler om it-risikostyring og hændelsesrapportering, som i dag er spredt ud over nationale og fælleseuropæiske love og standarder. Forslaget indeholder således regler om styring og organisation, identifikation, beskyttelse, detektion og beredskab, tillige med monitorering, registrering og klassifikation af hændelser samt tilhørende rapportering til nationale og fælleseuropæiske tilsynsmyndigheder og ECB.

Endvidere indføres der nye eller mere detaljerede regler for informationsudveksling mellem de finansielle virksomheder og ansvarlig offentliggørelse af hændelser eller væsentlige sårbarheder. Det samme gælder for test og risikostyring af leverandører (bl.a. reguleres it-kontrakter med leverandører). Herunder er der almene krav om test af it-systemer og krav om trusselsbaseret penetrationstest af de vigtigste finansielle virksomheder.

Med DORA foreslås ydermere, at der etableres fælleseuropæisk tilsyn af de kritiske leverandører i EU. De relevante tilsynsmyndigheder vil få beføjelser til at inspicere og give henstillinger og bøder til leverandørerne (fx hvis en anmodning om oplysninger ikke efterfølges).

Med hensyn til den videre proces har Europa-Kommissionen overdraget forslaget til gennemgang og forhandling i Europa-Parlamentet og Ministerrådet. Vedtagelsesprocessen for denne type af vidtgående lovgivning kan tage op til to år.

4 Hvilket ellers er praksis for andre typer af vurderinger, jf. Nationalbankens overvågningspolitik (*link*).

5 E-nettet, der er et forvaltningsselskab ejet af Finans Danmark, deltager også i samarbejdet i rollen som ansvarlig for netværket e-connect, der forbinder datacentralerne med detailbetalingssystemerne og Kronos2.

hvor en række vigtige aktører og myndigheder i den finansielle sektor siden 2016 har samarbejdet om forskellige aspekter af cyberrobusthed. Nationalbanken varetager formandskab og sekretariat for FSOR.

FSOR arbejder ud fra en risikobaseret tilgang med at understøtte de individuelle aktørers arbejde med cyberrobusthed og dermed øge den samlede robusthed i infrastrukturen. I 2020 blev der bl.a. igangsat et arbejde med fokus på at styrke niveauet for databeskyttelse og skærpe evnen til en hurtig og sikker genopretning efter et cyberangreb. Det er områder, hvor der generelt er behov før øget fokus i hele sektoren, hvilket bl.a. fremgår af den undersøgelse af cyberrobustheden i den finansielle sektor, som Nationalbanken har gennemført i 2020.[6] I undersøgelsen har 25 af de vigtigste aktører og leverandører i sektoren selvevalueret deres aktuelle cyberrobusthedsniveau, inkl. alle de operationelle medlemmer af FSOR.

En anden af FSOR's opgaver er ansvaret for et kriseberedskab på sektorniveau, som supplerer medlemmernes egne kriseplaner og det nationale kriseberedskab, NOST. Kriseberedskabet bliver løbende opdateret på baggrund af bl.a. erfaringer fra de test, der gennemføres to gange om året. Testene skal sikre, at kriseplanen fungerer i praksis i tilfælde af en alvorlig hændelse i sektoren. Den seneste test fandt sted i november 2020, hvor koordineringen på tværs af seks samfundskritiske sektorer for første gang blev testet i forbindelse med et fiktivt cyberangreb. Center for Cybersikkerhed orkestrerede øvelsen.

En uddybende gennemgang af arbejdet i FSOR kan læses i forummets årsrapport, der findes på Nationalbankens hjemmeside (*link*).

De centrale systemer/løsninger i infrastrukturen deltager også i TIBER-DK, der er Nationalbankens Threat Intelligence Based Ethical Red team-testprogram.[7] I en TIBER-test udsættes deltagernes live-systemer for et simuleret cyberangreb med det formål at finde og udbedre sårbarheder, inden de udnyttes af cyberkriminelle. Flere af de centrale virksomheder i infrastrukturen var blandt de første til at gennemgå et TIBER-testforløb.

Finansiel infrastruktur er dynamisk
Finansiel infrastruktur udvikles over tid for at forbedre borgere og virksomheders muligheder for at betale og for at øge systemernes og løsningernes sikkerhed og effektivitet.

Der pågår i øjeblikket et arbejde på europæisk plan, der bl.a. skal fremme et betalingsmarked med sikre, effektive og konkurrencedygtige betalinger på tværs af Europa. Brugen af elektroniske betalingsløsninger er gennemsnitligt væsentligt lavere i EU som helhed end fx i Danmark. Europa-Kommissionens arbejde med en "Digital Finance Package" er beskrevet nærmere i boks 5.

Der er også en klar tendens til konsolidering af forretningsaktiviteter på tværs af landegrænser. I Danmark har det bl.a. gjort sig gældende ved Nets' salg af bl.a. clearingaktiviteter til Mastercard og efterfølgende fusion med det italienske selskab Nexi, ligesom den danske værdipapircentral VP Securities A/S nu indgår i Euronext-koncernen, der er blandt de største infrastrukturvirksomheder på værdipapirområdet i Europa. Den øgede grad af konsolidering skyldes bl.a. skærpede konkurrencevilkår og stordriftsfordele, men betyder også, at der er flere ressourcer i virksomhederne til arbejdet med sikkerhed, fx på cyberområdet.

I 2020 offentliggjorde Nationalbanken planerne om at samle dansk kroneafvikling på den europæiske betalings- og værdipapirafviklingsplatform Target Services. Det vil bane vejen for et tættere samarbejde med andre centralbanker i Europa og give skalafordele ved fælles brug af it-platform, hvilket alt andet lige vil betyde, at der er øgede ressourcer til arbejdet med sikkerhed, herunder cybersikkerhed. Projektet omfatter også tilslutning til TIPS, der er en platform for grænseoverskridende straksbetalinger mellem borgere og mellem borgere og virksomheder i Europa. I regi af TIPS analyseres muligheden for straksbetalinger på tværs af valutaer i Europa. Migreringen til Target Services og opkoblingen til TIPS forventes gennemført i 2024/25. Se også boks 6 i afsnittet om interbankbetalinger.

6 Tilsvarende undersøgelse blev gennemført i 2016 og 2018.

7 Se mere om TIBER-DK på Nationalbankens hjemmeside (*link*).

Et andet igangværende projekt er P27, hvor seks nordiske banker arbejder på ny fælles infrastruktur til clearing og afvikling af detailbetalinger i og mellem Danmark, Sverige og Finland. Arbejdet med P27 er beskrevet nærmere i afsnittet om clearing og afvikling af detailbetalinger.

Nationalbanken følger udviklingen i den finansielle infrastruktur tæt og vil, uanset hvilke lande systemer ligger i, arbejde målrettet for at løfte myndighedsansvaret for at bidrage til en sikker og effektiv betalingsinfrastruktur i Danmark.

Nye strategiske tiltag på det europæiske betalingsmarked Boks 5

Europa-Kommissionen offentliggjorde i september 2020 "Digital Finance Package", herunder en strategi for det europæiske detailbetalingsmarked.[1] Kommissionens vision er at fremme et betalingsmarked med sikre, effektive og konkurrencedygtige betalinger på tværs af Europa, bl.a. via en effektiv og sammenhængende betalingsinfrastruktur samt betalingsløsninger med paneuropæisk rækkevidde.

I de kommende år vil der bl.a. være fokus på et review af betalingstjenestedirektivet, PSD2, og mulighederne for at fremme brugen af et digitalt ID på tværs af medlemslandene undersøges i samarbejde mellem Kommissionen og den europæiske tilsynsmyndighed, EBA. Kommissionen vil endvidere se på borgernes adgang til centralbankpenge, dels i form af kontanter, og dels ved støtte til det undersøgende arbejde, ECB har igangsat om digitale centralbankpenge.

Endelig har Kommissionen og ECB aktivt støttet European Payments Initiative (EPI), der har til hensigt at skabe en paneuropæisk betalingsløsning, der fungerer både med kort og straksbetalinger (fx via en mobil app), og som også understøtter person til person-betalinger på tværs af Europa. EPI er et privat samarbejde mellem 16 større europæiske pengeinstitutter og en række kortindløsere, herunder Nets.

1. Europa-Kommissionen, 24. september 2020, "Retail Payments Strategy for the EU" (*link*).

Interbankbetalinger

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

Kronos2 er Nationalbankens realtidsbruttoafviklingssystem, RTGS-system, der afviklinger betalinger enkeltvist og øjeblikkeligt. I Kronos2 afvikles, udover interbankbetalinger, også pengepolitiske operationer og nettopositioner fra tilsluttede betalings- og afviklingssystemer.

Kronos2 er et centralt omdrejningspunkt i dansk betalingsinfrastruktur, jf. boks 2.

Brug
Der er 83 deltagere i Kronos2. Deltagerne er primært danske banker, realkreditinstitutter og filialer af udenlandske banker.

I 2020 blev der i gennemsnit pr. bankdag gennemført knap 6100 interbankbetalinger i Kronos2 med en samlet værdi på 87,6 mia. kr., jf. tabel 1.

Driftsstabilitet
I 2020 har driftsstabiliteten i Kronos2 overordnet set været tilfredsstillende.

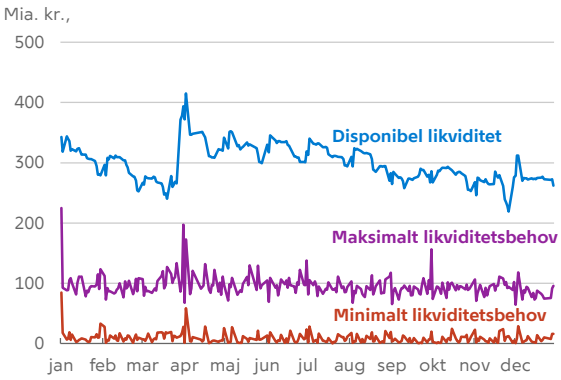
Der har været enkelte hændelser, hvor Kronos2 har været utilgængelig for nogle af deltagerne i løbet af dagen. Nødprocedurer har sikret, at kritiske betalinger blev gennemført. Der er lavet årsagsanalyser og implementeret tiltag, der skal modvirke, at det sker igen.

Som en del af covid-19-beredskabet har driften af Kronos2 været kørt i splitteams, der sidder forskellige steder og ikke mødes fysisk. Betalingsafviklingen i Kronos2 har ikke været påvirket af covid-19-pandemien.

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

I forbindelse med udbruddet af coronavirus etablerede Nationalbanken i marts 2020 en ekstraordinær udlånsfacilitet for midlertidigt at øge de pengepolitiske modparters adgang til likviditet, hvis der skulle opstå behov.

Rigelig likviditet blandt deltagerne i Kronos2 i 2020 Figur 1



Kilde: Danmarks Nationalbank.

Internationale standarder
En vurdering af Kronos2 efter CPMI-IOSCO's principper for finansiel markedsinfrastruktur er ved at blive færdiggjort. Vurderingen omfatter alle områder af Kronos2 – både det juridiske grundlag, den overordnede organisering, it-sikkerhed og den nærmere styring af alle risici, som kan opstå i forbindelse med betalingsafvikling i Kronos2.

I 2021 vil Nationalbanken endvidere igangsætte en vurdering af Kronos2 efter CPMI-IOSCO's retningslinjer for cybersikkerhed, der uddyber cybersikkerhedsaspekter af de mere generelle principper fra CPMI-IOSCO.

Cyberrobusthed
I lyset af et stadig mere alvorligt trusselsbillede arbejder Nationalbanken løbende på at styrke robustheden i systemerne omkring Kronos2.

Et vigtigt element i et stærkt cyberforsvar er at kunne opdage usædvanlige aktiviteter, som kan være tegn på cyberangreb. Tidlig detektion giver mulighed for hurtigere at respondere og afbøde virkningen af et angreb. I 2020 har Nationalbanken udbygget sin overvågningskapacitet.

Transaktioner i Kronos2 Tabel 1

Mia. kr., gennemsnit pr. bankdag	2016	2017	2018	2019	2020
Interbankbetalinger	**83,0**	**74,0**	**83,0**	**87,4**	**87,6**
- Heraf kundebetalinger	11,5	11,5	13,6	14,0	14,0
Pengepolitiske operationer	**28,7**	**39,9**	**36,9**	**48,4**	**34,5**
- Heraf salg af indskudsbeviser	28,6	39,9	36,9	48,4	33,3
- Heraf pengepolitiske udlån	0,1	0,0	0,0	0,0	1,3
Overførsler til afviklingssystemer	**283,4**	**316,3**	**237,3**	**115,1**	**113,8**
- Heraf til Sum-, Intradag- og Straksclearingen	242,7	273,8	177,2	40,5	39,9
- Heraf til VP-afviklingen	31,7	32,5	40,6	46,4	41,2
- Heraf til CLS	9,0	10,0	19,6	28,2	32,8
Afviklede nettopositioner	**25,1**	**24,8**	**24,1**	**16,3**	**16,6**
- Heraf Sum-, Intradag- og Straksclearingen	7,6	8,0	8,1	8,3	8,3
- Heraf VP-afviklingen	10,6	10,1	9,1	1,0	0,9
- Heraf CLS	6,9	6,7	6,8	7,0	7,3

Vidensdeling om cybertrusler fra NFCERT og CIISI-EU bidrager også til Nationalbankens overvågning af sårbarheder og unormale aktiviteter i systemer og netværk.

Nationalbanken har indført begrænsninger i brugen af en bestemt beskedtype til at sende betalinger fra Nationalbankens konti. Tiltaget er med til at reducere risikoen for, at det lykkes en hacker at stjæle penge fra Nationalbankens konti.

Nationalbanken arbejder fortsat med CPMI's strategi for endpoint-sikkerhed og har bl.a. indført krav om, at alle deltagere i Kronos2, der er forbundet via SWIFT, skal efterleve SWIFT's Customer Security Programme's krav til it-sikkerhed. Dette omfatter de største deltagere i Kronos2.

Systemændringer

Nationalbankens Extreme Contingency Facility (ECF) er i 2020 blevet testet med de største deltagere i Kronos2. ECF er den løsning, der skal sikre afvikling af betalinger, i tilfælde af at Kronos2 rammes af en alvorlig hændelse eller nedbrud. Testen har øget visheden om, at betalingsafviklingen kan håndteres i krisesituationer. Nationalbanken vil videreudvikle ECF-løsningen og planlægger at teste den med hele sektoren i 2021.

I 2020 besluttede Nationalbanken at migrere danske kroner til den kommende europæiske, konsoliderede betalings- og værdipapirafviklingsplatform Target Services i 2024/25. Se boks 6.

Danske kroner på europæisk og fremtidssikret infrastruktur

Boks 6

I 2020 har Danmarks Nationalbank på baggrund af en foranalyse, risikovurdering og dialog med den finansielle sektor besluttet at migrere afviklingen af danske kroner til den kommende europæiske, konsoliderede betalings- og værdipapirafviklingsplatform Target Services i 2024/25. En migration af danske kroner til Target Services vil sikre:

- én platform for afvikling af danske kroner
- styrket it-sikkerhed og fælles front imod cybertrusler
- harmoniseret infrastruktur med øgede driftsfordele i forhold til vedligeholdelse og videreudvikling.

Target Services består af betalingssystemet 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 samler de tre systemer på én platform, moderniseres og omdøbes Target2 til T2 og vil derefter også kunne understøtte flere valutaer.

Siden 2018 er en del af de danske værdipapirhandler blevet afviklet på T2S. Danske kroner var dermed den første valuta, som udnyttede T2S-systemets mulighed for at håndtere flere forskellige valutaer. Ved migreringen af kroneafviklingen til Target Services erstattes Kronos2 med T2. Desuden bliver danske kroner tilsluttet TIPS. Dermed samles al kroneafvikling på Target Services.

Ved at samle dansk krone- og værdipapirafvikling på det konsoliderede Target Services opnås væsentlige stordriftsfordele og løbende driftsbesparelser sammenlignet med den nuværende løsning. Dertil vil Nationalbanken, eurosystemet og øvrige deltagende centralbanker kunne gøre fælles front mod fremtidens cybertrusler og samarbejde om at videreudvikle den samlede europæiske betalingsstruktur.

Adgangen til Target Services er omfattet af en høj beskyttelse og sikkerhed, hvilket også stiller højere krav til de tilkoblede banker og brugere af platformen. Alle deltagere, der ønsker direkte adgang til Target Services, skal indgå aftale med én af de to prækvalificerede netværksleverandører, som kan give adgang. Deltagere i euroafviklingen vil under alle omstændigheder skulle indgå en sådan aftale og kan også bruge denne adgang til danske kroner.

Det konsoliderede Target Services vil også understøtte et nyt beskedformat – ISO20022 - for finansielle beskeder, som skal være fuldt implementeret i alle betalingssystemer ved udgangen af 2025.

Danmark får med migreringen af kroner til Target Services en stærkere placering og indflydelse på europæisk betalingsinfrastruktur, og øget harmonisering vil give nye muligheder for betalingsområdet på længere sigt. Flytningen af danske kroner til Target Services vil således effektivisere og fremtidssikre dansk betalingsformidling – både i dansk, nordisk og europæisk kontekst.

Danmark er foregangsland på straksbetalingsområdet og vil med danske kroner på TIPS få helt nye muligheder. Eurosystemet besluttede i 2020, at TIPS skal være afviklingsplatform for alle straksbetalinger i euro. Ved at samle straksbetalinger i flere valutaer på TIPS – herunder også danske kroner – opnås en øget harmonisering af straksbetalinger. Det danner grundlag for betalinger på tværs af de deltagende valutaer på længere sigt. Denne mulighed undersøges i en særskilt arbejdsgruppe ledet af ECB.

Nationalbanken har etableret en projektgruppe, som i samarbejde og koordination med Den Europæiske Centralbank, ECB, driftsoperatøren 4CB (de fire centralbanker Tyskland, Frankrig, Italien og Spanien), sektoren og øvrige systemejere i betalingsinfrastrukturen vil fastlægge rammerne for den fremtidige betalingsafvikling for danske kroner på Target Services. Nationalbanken og Eurosystemet skal indgå såkaldte Currency Participation Agreements (CPA) om kroneafvikling på T2 og TIPS. Den eksisterende CPA for T2S forventes videreført.

Der er etableret en referencegruppe og sektorgruppe, bestående af repræsentanter fra sektoren og Nationalbanken, som vil følge udviklingsprojektet tæt i alle dets faser i de kommende år. I forbindelse med igangsættelsen af projektet blev der etableret arbejdsgrupper med deltagelse af eksperter fra sektoren. Arbejdsgrupperne skal afklare de likviditetsmæssige og tekniske aspekter af den kommende løsning. Yderligere grupper kan blive etableret i projektets senere faser – fx i forbindelse med større sektortest mv. Der er også afholdt informationsmøder i starten af 2021, hvor alle kontohavere var inviteret.

Detailbetalinger

I Danmark gennemføres de fleste betalinger ved hjælp af elektroniske betalingsløsninger, som fx Dankort, MobilePay, netbank-overførsler, Betalingsservice m.fl. Med disse betalingsløsninger gennemførte danske virksomheder og borgere transaktioner for 28,8 mia. kr. i gennemsnit pr. dag[8] i 2020.

De betalingsløsninger, der har størst betydning i Danmark, overvåges af Nationalbanken, jf. boks 7.

Anvendelsen af kontanter som betalingsmiddel har gennem en længere periode været støt faldende. Kontanternes andel af det samlede antal betalinger ved handel med fysisk tilstedeværelse (i fx supermarkeder) er faldet fra 48 pct. i 2009 til 16 pct. i 2019.[9] Corona-pandemien ser ud til at have forstærket denne udvikling i 2020.[10]

Skiftet væk fra kontanter indebærer, at de elektroniske betalingsløsninger får større betydning – herunder dem overvåget af Nationalbanken.

Driftsstabilitet
I 2020 var driftsstabiliteten høj i de systemer, som ligger til grund for Dankort og Betalingsservice.

Der har alene været nogle mindre hændelser i løbet af året, som ikke har påvirket brugernes mulighed for at anvende Dankort og Betalingsservice. For Dankorts vedkommende har der været tale om små forstyrrelser i anvendelsen af *Dankort Secured by Nets* ved handel på nettet. Betalingsservice har oplevet en kort periode med problemer med kreditorernes adgang til BS Creditor portal.

Driftsstabiliteten har ikke været påvirket af corona-pandemien. For at undgå smitte med covid-19 og sikre den daglige drift er alle medarbejdere i Dankort og Betalingsservice blevet delt op i 2 hold, hvor kun et hold ad gangen må være på kontoret. Alle arbejder dog så vidt muligt hjemmefra.

Nationalbankens overvågning af betalingsløsninger Boks 7

Nationalbanken overvåger de vigtigste danske betalingsløsninger. På nuværende tidspunkt omfatter overvågningen Dankort, Betalingsservice og konto til konto-overførsler (via overvågningen af detailclearingerne). Nationalbanken tager løbende stilling til, om der er behov for målrettet overvågning af de andre betalingsløsninger på det danske marked. MobilePay er en af de betalingsløsninger, som oplever vækst. MobilePay's omsætning ligger dog fortsat på et væsentligt lavere niveau end Dankort, Betalingsservice og konto til konto-overførsler. Den gennemsnitlige omsætning for MobilePay var på 0,3 mia. kr. pr. dag i 2020.[1] Til sammenligning lå Dankort på 1,1 mia. kr. pr. dag.[2]

1. MobilePay (*link*).
2. Nets' statistik for Dankort.

Nets' salg af Betalingsservice til Mastercard
Mastercard indgik i august 2019 en aftale med Nets om køb af bl.a. Betalingsservice. Efter at have imødekommet Europa-Kommissionens betingelser for godkendelse af aftalen, blev købet gennemført i marts 2021 (se også afsnittet nedenfor om clearing og afvikling af detailbetalinger).

Nets og Mastercard har indgået en serviceaftale, der skal være med til at sikre en fortsat smidig, sikker og stabil drift af Betalingsservice. Dermed vil Mastercard i en overgangsperiode på op til tre år efter overtagelsen have mulighed for at få bistand fra Nets i forhold til at understøtte driften af Betalingsservice.

Overvågningen af Betalingsservice vil fremover blive rettet mod Mastercard.

Fusion mellem Nets og Nexi (og SIA)
I november 2020 indgik Nets og Nexi en bindende aftale om at fusionere. I marts 2021 godkendte Euro-

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

9 Danmarks Nationalbank, Der bliver længere mellem kontantbetalinger, *Danmarks Nationalbank Analyse*, nr. 3, februar 2020 (*link*).

10 Danmarks Nationalbank, Betalinger før, under og efter corona-nedlukningen, *Danmarks Nationalbank Analyse*, nr. 16, september *2020* (*link*).

pa-Kommissionen fusionen, hvorefter Nets og Nexi forventer at kunne afslutte handlen i andet kvartal af 2021.

Herefter er det planen, at det nye konsoliderede selskab gennemfører den fusion med SIA, som Nexi og SIA tidligere har aftalt (uafhængigt af fusionen mellem Nets og Nexi). Den fusion skal dog først godkendes af de relevante myndigheder. Nets forventer, at det samlede selskab (Nets, Nexi og SIA) vil være på plads i 2. halvår af 2021.

Formålet med ovennævnte fusioner er ifølge de tre selskaber at skabe en stor og finansielt stærk aktør på det europæiske betalingsmarked med en bred vifte af løsninger til banker og forretninger i hele Europa – med fokus på overgangen til digitale betalinger.

Dankort vil fortsat være en del af Nets Danmark, som følger med i fusionen med Nexi. Fusionen vil ikke umiddelbart have betydning for Dankort og Nationalbankens overvågning heraf.

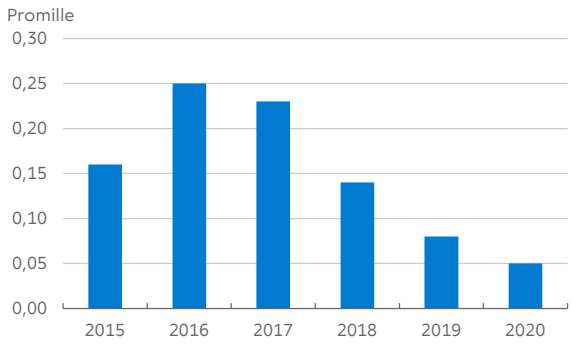
Stort fald i misbruget af Dankort

I 2020 lå misbruget af Dankort ifølge Nets på 17,9 mio. kr., hvilket svarer til 0,05 promille af det samlede forbrug med Dankort.[11]

Misbruget er faldet med samlet set 42 pct. fra 2019 til 2020. Mere specifikt er misbruget af Dankort ved handel på nettet faldet med 35 pct. fra 2019 til 2020, mens misbruget af Dankort ved anvendelse i fysisk handel er blevet næsten halveret i samme periode (fald på 49 pct.).[12] Dermed er de seneste års positive udvikling med en betydelig reduktion af misbruget af Dankort fortsat, jf. figur 2.

Flere faktorer ligger til grund for det faldende misbrug af Dankort i 2020.

Misbrug som del af det samlede forbrug med Dankort Figur 2



Kilde: Nets.

De restriktioner i samfundet, som corona-pandemien har medført, vurderes at have medvirket til det faldende misbrug. Det skyldes, at nedlukningen af bl.a. nattelivet har givet de kriminelle sværere betingelser for at stjæle Dankort.[13]

Nets, politiet og bankerne samarbejder på fast basis om at identificere og overvåge de hæveautomater, som de kriminelle oftest anvender efter at have afluret ofrenes pinkode og stjålet deres kort. Nets har samtidigt udbygget sine systemer til overvågning af mistænkelig adfærd. Nets har peget på, at disse tiltag har haft en dæmpende effekt på misbruget.

Det kontaktløse Dankort kan også have spillet en rolle. Det benyttes ved mere end tre ud af fire betalinger med Dankort. Her skal køberen som udgangspunkt ikke indtaste pinkode, så længe beløbet er under 350 kr. Pinkoden kan i det tilfælde ikke aflures af de kriminelle. Samtidig ser covid-19-

11 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.)

12 Nets' statistik for misbrug af Dankort.

13 Via Ritzau, *Nets: Misbrug på Dankort halveret*, den 10. august 2020 (*link*).

pandemien ud til at have øget brugen af kontaktløse betalinger.[14]

Regulering og afledte tiltag for sikre betalinger
Den 1. januar 2021 er tidligere blevet fastsat af de europæiske tilsynsmyndigheder som frist for gennemførelse af kravet i PSD2 om stærk kundeautentifikation (dvs. to-faktor-autentifikation)[15] ved kortbetalinger på nettet.[16]

Finanstilsynet har offentliggjort, at de forventer, at pengeinstitutter og andre kortudstedere senest fra 11. januar 2021 begynder at afvise kortbetalinger, der ikke er godkendt med stærk kundeautentifikation.[17]

For at forberede dette har de danske internetbutikker i løbet af 2020 arbejdet på at udrulle sikkerhedsløsningen *Dankort Secured by Nets* med krav om brug af en engangskode på SMS ved køb med Dankort på nettet over en vis beløbsgrænse. Fra og med 2021 er sikkerheden i *Dankort Secured by Nets* styrket som følge af ovennævnte krav i PSD2. Fra årsskiftet er der således krav om anvendelse af en af følgende fremgangsmåder for to-faktor autentifikation ved handel på nettet med Dankort:

1. En engangskode på SMS og et kodeord.
2. NemID-brugernavn og adgangskode med bekræftelse ved hjælp af NemID-nøgleapp eller NemID-nøgleviser.

Samtidig med denne styrkelse af sikkerheden har PSD2 også medført, at beløbsgrænsen for, hvornår Dankort Secured by Nets skal anvendes, er nedsat fra 450 kr. til 225 kr. fra begyndelsen af 2021. Disse tiltag må forventes at have en dæmpende effekt på misbruget af Dankort fremadrettet.

Internationale standarder
Nets har i løbet af 2020 arbejdet videre med opfølgningen på Nationalbankens vurdering af Betalingsservice efter ECB's standarder.[18] Nets har imødekommet de fleste anbefalinger og bemærkninger, men på tre områder har det været svært at komme helt i mål på grund af hindringer for arbejdet som følge af covid-19-pandemien. Det gælder for arbejdet med at styrke it-risikostyringen, netværksovervågningen og håndteringen af kritiske leverandører. Nationalbanken har fulgt op på dette ved de kvartalsvise møder med Nets.

14 Via Ritzau, *Nets: Corona-frygt skaber vækst i kontaktløse betalinger*, den 18. november 2020 (*link*).

15 Stærk kundeautentifikation er en kontrolforanstaltning, der indebærer, at der skal anvendes mindst to faktorer til at godkende en betaling. De to faktorer skal være noget, betaleren ved (fx et password), har (fx en mobiltelefon, der kan modtage en engangskode), eller er (fx et fingeraftryk) – jf. EU's forordning om stærk kundeautentifikation, fælles og sikker kommunikation (*link*).

16 Finans Danmark, Fakta om nye EU-regler for betalinger, den 28. december 2020 (*link*).

17 Finanstilsynet, *Danske netbutikker skal være klar til nye sikkerhedsregler fra 1. januar 2021*, den 21. oktober 2020 (*link*).

18 Danmarks Nationalbank, Vurdering af Betalingsservice, *Danmarks Nationalbank Rapport*, nr. 4, oktober 2019 (*link*).

Clearing og afvikling af detailbetalinger

Danske detailbetalinger cleares og afvikles i Sum-, Intradag- og Straksclearingen, kaldet detailclearingerne. Systemerne ejes af Finans Danmark 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 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, der udveksler beløbene mellem bankerne.

I Straksclearingen bogføres konto til konto-overførsler på kundernes konti, i takt med at de foretages. 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 til netbank-overførsler og betalinger via MobilePay.

Brug

Ved udgangen af 2020 var der 50 direkte deltagere i detailclearingerne og 25 indirekte deltagere, som afvikler gennem en direkte deltager.

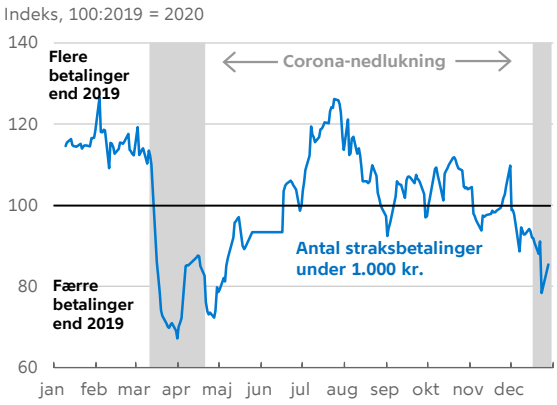
Værdien af transaktionerne i systemerne udgjorde i gennemsnit 42,2 mia. kr. pr. bankdag i 2020, jf. tabel 2.

Antallet af straksbetalinger under 1.000 kr. faldt ved covid-19-nedlukningerne i marts og december, jf. figur 3. Straksclearingen anvendes særligt til betalinger mellem privatpersoner, bl.a. via MobilePay. Nedlukningen af samfundet har altså i en vis grad påvirket den form for betalinger.

Driftsstabilitet

Driften af detailclearingerne er i 2020 forløbet tilfredsstillende. Der har været enkelte hændelser i årets løb. Bl.a. blev en række betalinger forsinket, da en mindre bank – som var under frivillig afvikling – ikke havde tilstrækkelig likviditet, fordi den som led i afviklingen havde overført sine midler til en konto i en anden bank. Der er fulgt op på hændelsen for at forhindre, at lignende situationer opstår ved fremtidige bankafviklinger.

Fald i antal straksbetalinger under 1.000 kr. ved corona-nedlukningerne Figur 3



Anm.: Indeks=100: 2019 lig med 2020. Dvs. udviklingen gennem 2020 vises relativt til udviklingen gennem 2019. Serien angiver et 7-dages glidende gennemsnit med seneste observation. Der er korrigeret for helligdagenes placering i henholdsvis 2019 og 2020 på nær perioden 25. maj til 16. juni, hvor der er anvendt et gennemsnit for at undgå outliers.
Kilde: Nets.

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

Mia. kr., gennemsnit pr. bankdag	2016	2017	2018	2019	2020
Sumclearingen	17,2	17,8	18,3	19,2	18,7
Intradagclearingen	18,4	19,7	20,1	20,8	21,9
Straksclearingen	0,8	0,9	1,2	1,4	1,6
I alt	36,4	38,4	39,6	41,4	42,2

Kilde: Nets.

I forbindelse med covid-19 er de medarbejdere, der skal være fysisk til stede i forbindelse med driften, blevet inddelt i flere teams for at undgå potentiel smittespredning. Endvidere er der blevet etableret et særligt informationsberedskab mellem Finans Danmark, e-nettet, Mastercard og datacentralerne.

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

De fleste af deltagerne anvender systemernes automatiserede værktøjer til likviditetsstyring, og der har udover ovennævnte hændelse kun været et tilfælde i 2020, hvor en deltager er blevet henlagt på grund af manglende likviditet.

Internationale standarder
Nationalbanken er ved at vurdere detailclearingerne efter CPMI-IOSCO's retningslinjer for cybersikkerhed. Vurderingen forventes afsluttet i 2021.

Finans Danmark har tidligere gennemgået kravene til cybersikkerhed og har på den baggrund igangsat et arbejde for at styrke cyberrobustheden i detailbetalingsinfrastrukturen. Der er bl.a. udarbejdet en cybersikkerhedshåndbog, der indeholder it-sikkerhedskrav, som deltagerne skal implementere og rapportere deres efterlevelse af.

Systemændringer
Der har tidligere været eksempler på, at hændelser i den natlige afvikling har forsinket bogføringen på kundernes konti betydeligt. De natlige afviklinger er derfor blevet justeret, så afviklingerne kl. 03.00 og 06.00 – i tilfælde af en hændelse – kan afvikles manuelt og dermed tidligere. Det giver datacentralerne bedre tid til at afslutte bogføringen på kundernes konti inden dagens start.

I Straksclearingen tilføres der døgnet rundt automatisk likviditet til bankernes betalinger. For at mitigere risikoen for hurtig udstrømning af likviditet fra en deltager, fx ved et hackerangreb, er frekvensen for, hvor ofte der tilføres ny likviditet, blevet ændret fra hver 15. minut til hver anden time. Derudover har deltagerne fået mulighed for at fastsætte deres egne individuelle frekvenser for tilførsel af ny likviditet samt en stopklods for, hvor mange gange der må tilføres ny likviditet mellem to afviklingsblokke.

Drift af detailclearingerne overtaget af Mastercard
Mastercard indgik august 2019 en aftale med Nets om køb af bl.a. de områder af Nets' infrastruktur, der omfatter drift af detailclearingerne.

Europa-Kommissionens konkurrencemyndighed godkendte handlen på betingelse af, at Nets' straksclearingsteknologi blev licenseret til en tredjepart med eksklusivret til at tilbyde løsningen inden for EØS.

Nets og Mastercard har siden opnået de nødvendige godkendelser fra relevante konkurrence- og tilsynsmyndigheder, og Europa-Kommissionens betingelse for aftalens gennemførelse er blevet opfyldt. Mastercard overtog derfor driften af detailclearingerne i marts 2021.

Nationalbanken og systemejeren Finans Danmark samt Nets og Mastercard har alle fokus på, at detailclearingerne skal køre uforstyrret videre efter overgangen til Mastercard.

P27 – fælles detailbetalingssystem for Danmark, Sverige og Finland
Seks nordiske banker samarbejder om at etablere en nordisk infrastruktur, kaldet P27, til clearing og afvikling af detailbetalinger i og mellem Danmark, Sverige og Finland.[19] Bankerne har etableret selskabet P27 Nordic Payments i Sverige, som skal drive P27. Derudover har bankerne valgt Mastercard som den leverandør, der skal stå for udvikling og drift af systemet.

19 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 i marts 2019.

P27 vil som udenlandsk selskab ikke automatisk være omfattet af dansk lov og Nationalbankens tilsyns- og overvågningsbeføjelser[20]. Der arbejdes derfor på at sikre, at der også i fremtiden er passende tilsyn og overvågning med clearing og afvikling af detailbetalinger i danske kroner.

Parterne er i dialog om en model, hvor P27 indarbejder en klausul i deres aftalegrundlag med bankerne, hvor det fremgår, at clearing og afvikling af danske kroner i P27's system reguleres af dansk ret. Dermed vil afviklingen blive omfattet af Nationalbankens beføjelser, og overvågningen kan rettes mod P27's selskab i Sverige.

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

Danske straksbetalinger i TIPS

ECB har i 2020 arbejdet videre med udviklingen af TIPS, som er ECB's system til afvikling af straksbetalinger. TIPS indgår i ECB's konsolideringsprojekt og samles med Target2 og T2S på én platform i Target Services. Som følge af Nationalbankens beslutning om at migrere afviklingen af danske kroner til Target Services, vil danske kroner også blive tilsluttet TIPS, hvilket vil give mulighed for at afvikle danske straksbetalinger i TIPS.

Sveriges Riksbank har ligeledes besluttet at anvende TIPS, og fra medio 2022 vil Riksbankens system til straksbetalinger afvikle i TIPS. Derudover er Riksbanken og ECB ved at undersøge muligheden for at udvikle en cross-currency funktionalitet, således at kontohavere i forskellige lande kan sende straksbetalinger til hinanden, jf. boks 8.

TIPS udvikler cross-currency Boks 8

ECB og Riksbanken er ved at undersøge muligheden for at udvikle en cross-currency funktionalitet i TIPS, hvilket vil give kontohavere på tværs af valutaer mulighed for at sende straksbetalinger til hinanden.

Det undersøges derfor, om der kan tilknyttes en såkaldt central exchange hub til TIPS, der på markedsvilkår skal sikre den bedste vekselkurs til afsenderen af en cross-currency-betaling. Ambitionen er en fuldautomatisk procedure, så en straksbetaling kan afvikles på mindre end 10 sekunder, uanset om den er national eller cross-currency.

ECB og Riksbanken forventer i 2021 at beslutte, hvorvidt de vil gå videre med projektet og fortsætte med målsætningen om implementering i 2023. Såfremt det realiseres, vil cross-currency-betalinger blive en mulighed for danske kontohavere, når danske kroner migrerer til Target Services i 2024/25.

Arbejdet er forankret i en arbejdsgruppe, som Nationalbanken deltager i.

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

Værdipapirafvikling

Værdipapirhandler kan indgås på forskellige typer markedspladser, bl.a. fondsbørsen, handelsplatforme eller "over-the-counter" via bank eller mægler. Den endelige afvikling af handlerne, dvs. hvor penge og værdipapirer udveksles på deltagernes konti, sker i VP-afviklingen og Target2 Securities, T2S.

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.

I juli 2020 gav Finanstilsynet godkendelse til Euronext Group til at købe VP, som siden da har været en del af den paneuropæiske børs og markeds-infrastruktur-koncern. Euronext har selskaber i en række europæiske lande, herunder værdipapircentraler i Norge, Portugal og nu også i Danmark.

T2S er en europæisk værdipapirafviklings-platform. Siden oktober 2018 er en stor andel af værdien af værdipapirafviklingen i danske kroner sket i T2S. T2S ejes af Eurosystemet og drives af de fire centralbanker i de største eurolande med ECB som koordinator. Afviklingen af kronehandler i T2S sker gennem VP, der som værdipapircentral er tilsluttet T2S. Danske kroner til pengebenet i handlerne overføres fra deltagernes konti i Nationalbanken.

Brug

VP-afviklingen har 110 deltagere, hvoraf 56 er udenlandske markedsdeltagere, herunder fire CCP'er, jf. boks 9. De professionelle deltageres indbyrdes værdipapirhandler afvikles på T2S, mens de private investorers handler afvikles på VP's egen platform.[21] Det betyder, at det typisk er store handler af høj værdi, som afvikles på T2S, mens der antalsmæssigt gennemføres flest handler i VP-afviklingen.

Den gennemsnitlige afvikling pr. bankdag i 2020 var 231,5 mia. kr., jf. tabel 3, hvilket er et rekordhøjt niveau. Det var bl.a. drevet af den øgede aktivitet på markederne i begyndelse af året, hvor usikkerheden omkring covid-19-pandemien påvirkede investorernes adfærd. Hen over sommeren og efteråret aftog aktiviteten for at så stige igen ved udgangen af året.

Særligt handlen med aktier steg sammenlignet med året forinden. Værdimæssigt blev der omsat aktier for 8,7 mia. kr. mere i gennemsnit pr. bankdag, hvilket er en stigning på 25 pct., mens antallet af handler steg med næsten 50 pct. Fremgangen blev altså især året af mange mindre aktiehandler mellem private investorer, hvilket også afspejles i den store stigning i antallet af afviklede transaktioner på VP's egen platform, jf. figur 4.

Driftsstabilitet

Driftsstabiliteten i afviklingen af danske værdipapirhandler har overordnet set været tilfredsstillende, men der har været flere hændelser i 2020.

Både VP og T2S har i udstrakt grad gjort brug af hjemmearbejde under covid-19-pandemien, hvor on-site-bemandingen for begge systemers vedkom

Centrale modparter, CCP Boks 9

En CCP stiller sig mellem parterne i en værdipapirhandel og påtager sig risikoen for både køber og sælger, i tidsrummet fra handlen er indgået, og til den er endeligt afviklet. De fire udenlandske CCP'er i VP, er hhv. EuroCCP, LCH Clearnet og Six X-clear, der clearer aktiehandler, mens Nasdaq Clearing clearer repoforretninger. Myndighedskontrollen med CCP'er sker i samarbejde i såkaldte tilsynskollegier, hvor myndigheder fra de lande, hvor de respektive CCP'er ud fra objektive kriterier er vurderet systemisk vigtige, jf. EMIR-forordningen.[1]

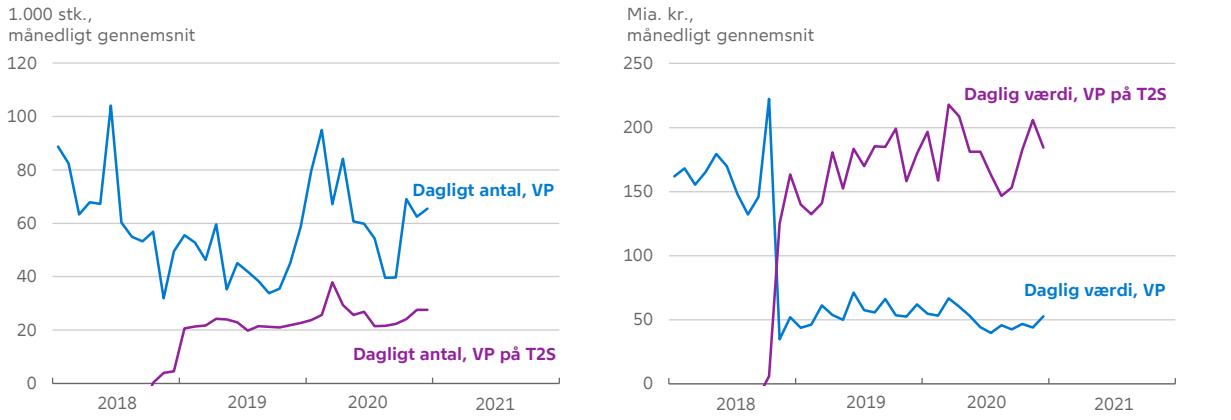
Nationalbanken deltager i øjeblikket ikke i nogen tilsynskollegier, da værdien af clearede transaktioner i danske kroner sammenlignet med andre valutaer er forholdsmæssig lav i de fire CCP'er, der afvikler i VP. Finanstilsynet deltager i tilsynskollegierne for Nasdaq Clearing og EuroCCP.

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

21 Se Danmarks Nationalbank, Overvågning af den finansielle infrastruktur 2018, Danmarks Nationalbank Rapport, nr. 3, juni 2019. Se side 14, for en nærmere beskrivelse af VP-afviklingen på T2S (*link*).

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: VP.

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.
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	67,0	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

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

mende kun har omfattet særligt forretningskritisk personale. De ændrede vilkår har ikke haft betydning for driften af systemerne, og de hændelser, der har været, er blevet håndteret bl.a. ved brug af virtuelle møder og fjernkommunikation.

I marts resulterede usikkerheden omkring covid-19-pandemien ikke alene i en forøgelse af handelsaktiviteten i Danmark, men også i en stor stigning på tværs af alle europæiske værdipapirmarkeder. Stigningen i antallet af transaktioner medførte et kapacitetspres på afviklingerne i VP og T2S. Begge systemer måtte derfor tilføre yderligere kapacitet for at være sikre på at kunne håndtere det stigende transaktionsomfang.

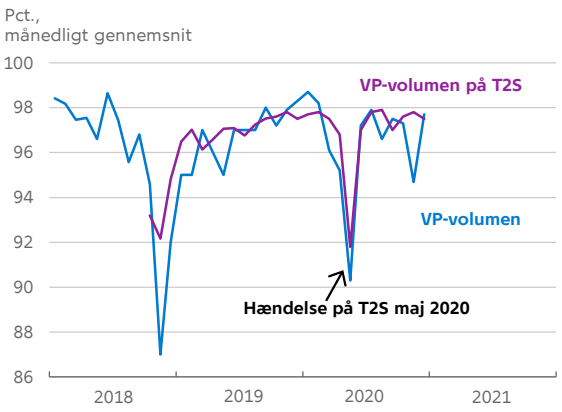
I maj medførte en teknisk fejl på T2S, at der opstod problemer i platformens forretningskontroller. Da fejlen blev opdaget og løst, var der allerede gennemført fejlbehæftede posteringer. Det medførte et større oprydningsarbejde i flere af de værdipapircentraler, der er tilsluttet T2S-platformen, herunder VP. VP måtte over flere omgange afvente tilstrækkelige og nødvendige informationer fra T2S for at komme på plads, hvilket resulterede i, at VP måtte blokere for afviklingen af 99 specifikke fondskoder (ISINs) i 55 timer, indtil korrekte data var modtaget fra T2S.

Der var tale om en alvorlig hændelse, og T2S har efterfølgende gennemført et større analysearbejde, der kortlægger årsagerne til hændelsen, og har implementeret tiltag, der skal modvirke, at en lignende hændelse sker igen. VP har også udarbejdet en rapport, der bl.a. evaluerer VP's egen håndtering af hændelsesforløbet.

I september måtte VP anmode ECB om at udsætte den natlige afvikling pga. problemer med forbindelsen til T2S. ECB imødekom VP's anmodning, og det lykkedes VP at få sendt alle beskeder til T2S, så afviklingen kunne starte og gennemføres med begrænset forsinkelse. Hændelsen skete natten før et kvartalsskifte, hvilket er særlig kritisk pga. den store volumen fra afviklingen af realkreditinstitutternes refinansieringer. En langvarig forsinkelse ville have medført, at refinansieringerne ikke var blevet gennemført rettidigt. VP har efterfølgende identificeret årsagen til hændelsen, der skyldtes en softwarefejl, som efterfølgende er løst og testet.

Afviklingsprocent

Figur 5



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

Afviklingsprocent

Afviklingsprocenten måler andelen af handelsomsætningen, der afvikles rettidigt. Ifølge den fælleseuropæiske regulering af værdipapircentraler, CSDR[22], artikel 5, skal alle værdipapirhandler, der indgås på en markedsplads, afvikles to dage efter, at handlerne er indgået.

Figur 5 viser afviklingsprocenten for hhv. VP's eget system og for VP's afvikling på T2S. Årsagen til det lave niveau i slutningen af 2018 var en række hændelser, der opstod i ugerne efter VP's tilslutning til T2S. I takt med at problemerne blev håndteret, stabiliserede afviklingsprocenten sig på et niveau svarende til før VP's migrering til T2S for så at tage et stort dyk i maj 2020. Her var den bagvedliggende årsag den alvorlige hændelse på T2S, der forsinkede afviklingen af et større antal handler, jf. ovenfor. Den lavere afviklingsprocent i VP sidst i 2020 skyldtes bl.a. forholdsvis mange nytegnede aktier, der skulle afvikles i november.

22 Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union mv.

Sanktioner
På T2S-platformen udvikles et fælleseuropæisk sanktionssystem, der skal sanktionere deltagere, hvis handler ikke kan afvikles rettidigt som følge af manglende værdipapirer eller likviditet. 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. Et sanktionssystem kan medvirke til at disciplinere deltagerne til at stille tilstrækkeligt med penge og værdipapirer til afviklingen.

Arbejdet med det fælleseuropæiske sanktionssystem, der i forvejen var forsinket, blev i 2020 yderligere udsat som følge af de udfordringer, covid-19-pandemien har medført. Systemet forventes nu først idriftsat i 1. kvartal 2022. VP har suspenderet sit eget sanktionssystem og afventer, at det nye system træder i kraft, så VP kan følge den fælleseuropæiske standard.

Internationale standarder
Nationalbanken overvåger VP og deltager i europæisk samarbejde om overvågningen af T2S, der ledes af ECB.

I 2016 fik 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, mens den sidste anbefaling, der vedrører VP's genopretningsplan, skal revurderes som følge af ændringerne i VP's ejerskab. Hovedansvaret for vurderingen ligger hos Finanstilsynet, der som kompetent myndighed fører tilsyn med, at VP lever op til kravene i den fælleseuropæiske værdipapircentral-forordning, CSDR, vedrørende planer for finansiel genopretning. Finanstilsynet er som foreskrevet i CSDR-reglerne præsenteret for genopretningsplanen, som efterfølgende er godkendt af VP's bestyrelse.

I 2020 har Nationalbanken i regi af ECB deltaget i opfølgningen på en vurdering af T2S efter et udvalg af CPMI-IOSCO-principperne. Vurderingen, der blev færdiggjort i 2019, er ikke offentliggjort, men Nationalbanken har deltaget i arbejdet.

Cyberrobusthed
Nationalbanken færdigjorde i 2020 en vurdering af VP's efterlevelse af CPMI-IOSCO's cyberguidance. Vurderingen viser, at VP har en høj modenhed og efterlever cyberguidance på de fleste områder. VP og Nationalbanken har aftalt et forløb i første halvår 2021 for opfølgningen på de anbefalinger, som Nationalbanken har givet i vurderingen.

I 2020 har Nationalbanken også bidraget til arbejdet med at vurdere T2S efter Cyber Resilience Oversight Expectations, CROE, der er ECB's udmøntning af CPMI-IOSCO's cyberguidance. Arbejdet med vurderingen, der ledes af ECB, forventes færdigt i løbet af 2021.

Systemændringer
VP er som følge af Euronexts overtagelse af ejerskabet i gang med at tilpasse sin organisation og processer til Euronexts. Arbejdet indebærer også konsolidering af services og forretningsmodeller, der tilbydes på tværs af koncernen. Der er ikke aktuelle planer om udrulning af en fælles it-platform for de tre værdipapircentraler i hhv. Danmark, Norge og Portugal, der alle er en del af Euronext-koncernen.

Betalinger og værdipapirafvikling i euro

Danske bankers betalinger og værdipapirhandler i euro afvikles i hhv. Target2 og Target2-Securities (T2S), der ejes og drives af Eurosystemet.

Target2 er det fælleseuropæiske RTGS-system til afvikling af store tidskritiske betalinger i euro. I Target2 overføres også likviditet til brug for afvikling i andre eurosystemer, herunder T2S. T2S er det fælleseuropæiske system til afvikling af værdipapirhandler i euro og danske kroner.[23]

Brug

Flere end 1000 banker anvender Target2 til eurobetalinger. Heraf er der 22 danske deltagere, som i 2020 gennemførte interbankbetalinger for i gennemsnit 9,8 mia. euro om dagen. De danske deltagere bruger hovedsageligt Target2 til at gennemføre koncerninterne betalinger og betalinger til udenlandske deltagere, jf. figur 6. Der udveksles flest euro med deltagere i Tyskland, Finland, Frankrig og Belgien.

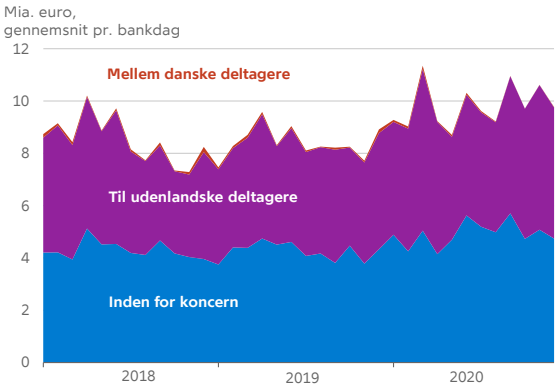
I alt 21 værdipapircentraler fra 20 europæiske lande er tilsluttet T2S, herunder VP. En bank kan afvikle på T2S, enten som direkte deltager, hvis banken har en såkaldt T2S-afviklingskonto, eller som indirekte deltager via en anden direkte deltagers adgang.

En T2S-afviklingskonto skal oprettes via en af centralbankerne i EU. 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.[24]

Driftsstabilitet

Driftsstabiliteten i de lokale komponenter af Target2, som Nationalbanken har ansvaret for, har været tilfredsstillende i 2020.

Interbankbetalinger i Target2 Figur 6



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

I 2020 var der en alvorlig hændelse i eurosystemets Target2. Et nedbrud i Target2 medførte fredag 23. oktober, at der ikke kunne afvikles betalinger eller overføres likviditet til/fra de tilsluttede systemer, herunder T2S i flere timer. Target2 har flere driftscentre, og driften blev genoprettet efter skift til et center i en anden region. Årsagen til hændelsen var en netværksfejl, der påvirkede Target2-infrastrukturen. ECB har igangsat tiltag, der skal mindske risikoen for, at det samme sker igen.

Der har været få større hændelser på T2S-platformen i 2020. Da disse også har haft betydning for afviklingen af værdipapirhandler i danske kroner, er de beskrevet i afsnittet om værdipapirafvikling ovenfor.

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

24 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 har via deres filial etableret en Target2-konto ved en centralbank i euroområdet.

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 2020 har Nationalbanken deltaget i arbejdet med diverse vurderinger af T2S mod internationale standarder for værdipapirafviklingssystemer. Arbejdet er nærmere beskrevet i afsnittet om værdipapirafvikling ovenfor.

Systemændringer
ECB igangsatte i 2016 en større modernisering af den europæiske betalingsinfrastruktur og har siden arbejdet med at konsolidere Target2, T2S og TIPS på én it-platform. Målet er at imødekomme nye markedskrav og optimere deltagernes likviditetsstyring på tværs af alle Target Services.

Idriftsættelsen af konsolideringen var planlagt til november 2021, men er blevet udskudt et år til november 2022. Baggrunden for beslutningen var en anmodning fra den samlede europæiske finansielle industri, der bad om udskydelse bl.a. på grund af covid-19-pandemien og SWIFT's forsinkelse med den globale migrering af grænseoverskridende betalinger til ISO 20022-format fra november 2021 til slutningen af 2022.

I marts 2020 påbegyndte deltagerne på Target2 den nødvendige softwareudvikling for at tilpasse deres interne systemer til den nye konsoliderede platform.

Valutahandelsafvikling

En valutahandel består af to modsatrettede betalinger i to forskellige valutaer. Valutahandler kan afvikles via korrespondentbanker eller via det internationale valutahandelsafviklingssystem, CLS, der afvikler handler i 18 tilsluttede valutaer. Langt størstedelen af valutahandler i danske kroner afvikles i CLS.

CLS Bank International (CLS) ejes af store internationale banker. I CLS reduceres afviklingsrisikoen, der er forbundet med valutahandler, som afvikles via korrespondentbanker. Det sker ved, at de to betalinger i en valutahandel afvikles samtidigt (Payment-versus-Payment, PvP) i CLS.

Nationalbanken deltager i den fælles overvågning af CLS, jf. boks 10.

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.[25] Den gennemsnitlige daglige værdi af handler i danske kroner var 278 mia. kr. i 2020, jf. figur 7. Det er en stigning på 5 pct. i forhold til 2019.

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.

I 2020 var der en enkelt hændelse i Kronos2, som påvirkede CLS-afviklingen. Mandag formiddag 23. november var Kronos2 nede i 1,5 time. Der blev igangsat manuelle procedurer, men Kronos2 nåede

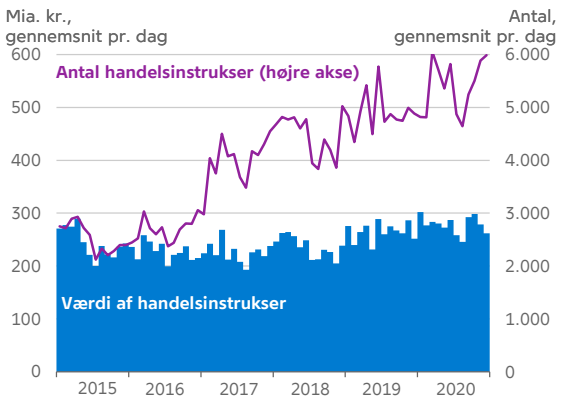
25 Anslået på baggrund af BIS, Triennial Central Bank Survey, Foreign exchange turnover in April 2019, Bank for International Settlements, September 2019 (*link*) og data fra CLS Bank.

Overvågning af CLS Boks 10

Overvågningen af CLS tager udgangspunkt i CP-MI-IOSCO's principper for sikre og effektive betalingssystemer. 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, 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, 2019 (*link*).
2. Federal Reserve System, Protocol for the Cooperative Oversight Arrangement of CLS (*link*).

Handelsinstruktioner i CLS Figur 7



Kilde: CLS Bank.

at komme op at køre igen og kunne overføre deltagernes indbetalinger til CLS-afviklingen, som blev gennemført inden for de fastsatte tidsfrister. Der er fulgt op med tiltag, der skal forebygge, at en lignende hændelse sker igen.

De danske deltagere reserverer tilstrækkelig likviditet til CLS-afviklingen.

Brexit
Brexit har ikke haft nogen indvirkning på dansk deltagelse i CLS eller på afviklingen i danske kroner.

Da Storbritannien forlod EU 31. januar 2020, og overgangsperioden udløb 31. december 2020, mistede CLS sin tidligere beskyttelse af direktivet om endelig afregning i betalingssystemer og værdipapirafvikling (Settlement Finality Directive, SFD). For at sikre at deltagerne i EU kunne fortsætte med at afvikle valutahandler i CLS, krævede det, at landene præciserede i deres nationale lovgivning, at direktivets bestemmelser vedr. endelig afregning også gælder for betalingssystemer uden for EØS.

Direktivet er i Danmark implementeret i kapitalmarkedsloven. I henhold hertil har Finanstilsynet, forud for Brexit, godkendt CLS som et tredjelands-betalingssystem. Dermed er CLS-afviklingen af handler i danske kroner fortsat beskyttet af SFD.

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. 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
14. april 2021.

DANMARKS NATIONALBANK

KONTAKT

Ole Mikkelsen
Kommunikations- og presserådgiver

omi@nationalbanken.dk
+45 3363 6027

SEKRETARIAT
OG KOMMUNIKATION