

DANMARKS NATIONALBANK

28. APRIL 2023 — NR. 4

Overvågning af den finansielle infrastruktur 2022

- Danmark har en sikker, effektiv og stabil betalingsinfrastruktur, hvor forstyrrelser er sjældne. Systemerne og løsningerne i infrastrukturen efterlever i høj grad internationale standarder.
- Der er et vedvarende og stort fokus på truslen fra cyberkriminelle, og systemerne og løsningerne i den danske betalingsinfrastruktur er generelt godt rustet til at modgå cyberangreb.
- De mest sofistikerede hackere bliver løbende mere specialiserede i deres metoder, og det er ikke muligt at sikre sig fuldt ud mod deres angreb. Det er derfor vigtigt fortsat at arbejde med beredskabsplanlægning og evnen til at håndtere alvorlige cyberhændelser, hvis eller når de indtræffer.

Samfundskritisk infrastruktur

724 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](#)

INDHOLD

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

Danmark har en sikker og effektiv betalingsinfrastruktur

En velfungerende og sikker betalingsinfrastruktur er afgørende for, at varer og tjenester kan udveksles nemt og effektivt. Nedbrud eller forstyrrelser i de centrale betalingssystemer kan skade samfundsøkonomien og i værste fald også true den finansielle stabilitet.

Betalingsinfrastrukturen er det netværk af forskellige systemer, der gør det muligt for borgere, virksomheder og finansielle aktører at udveksle betalinger og værdipapirer med hinanden. Den danske betalingsinfrastruktur er beskrevet i boks 1. I 2022 blev der på en gennemsnitsdag sendt elektroniske betalinger for 724 mia. kr. gennem systemerne i den danske betalingsinfrastruktur, jf. betalingsflowet i oversigtsfiguren i boks 1.

For di betalingsinfrastrukturen spiller en så kritisk rolle i samfundsøkonomien, overvåger Nationalbanken, at de centrale systemer i infrastrukturen efterlever internationale standarders høje krav til sikkerhed og effektivitet. Overvågningen omfatter også de vigtigste betalingsløsninger.

I denne rapport præsenteres hovedkonklusioner fra Nationalbankens overvågning og den væsentligste udvikling på områder, der har haft betydning for den danske finansielle infrastruktur i 2022.

Infrastrukturen er sikker, effektiv og stabil

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

De centrale systemer og løsninger efterlever i høj grad de krav, der stilles i internationale standarder til bl.a. organisering, risikostyring og beredskab, og ejerne af systemerne og løsningerne arbejder løbende med at styrke sikkerheden og efterleve Nationalbankens anbefalinger til forbedringer.

I 2022 var der i enkelte tilfælde problemer med den rettidige afvikling af betalinger, men generelt var driftsstabiliteten høj, og forstyrrelser i udvekslingen af betalinger og afviklingen af værdipapirhandler er sjældne.

Nationalbanken og flere andre organisationer, både i den finansielle sektor og andre dele af samfundet, blev i starten af 2023 ramt af en række over-

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, Betalingservice 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](#)).

belastningsangreb (også kaldet DDoS-angreb), hvor hackere forsøgte at lægge organisationernes hjemmesider ned. Ingen dele af betalingsinfrastrukturen, hverken hos Nationalbanken eller andre, blev påvirket. Angrebene medførte alene, at nogle brugere havde vanskeligheder med at tilgå organisationernes hjemmesider i kortere perioder.

Cyberrobustheden er god, men sektoren skal forberede sig på brud på sikkerheden

Center for Cybersikkerhed, CFCS, vurderer, at truslen fra cyberkriminalitet er meget høj, og de dygtigste hackere bliver løbende mere specialiserede og sofistikerede i deres metoder. Cybertrusselsbilledet er beskrevet nærmere i boks 2.

Ejerne af de centrale systemer og løsninger i den danske betalingsinfrastruktur har vedvarende og stort fokus på cybertruslen, og den danske betalingsinfrastruktur er generelt godt rustet til at modgå cyberangreb. Det er dog ikke muligt at sikre sig fuldt ud mod fejl eller brud på sikkerheden. Derfor er det vigtigt, at ejerne også har fokus på beredskab og evnen til at håndtere hændelser, der måtte indtræffe, fx hvis det lykkes cyberkriminelle at trænge igennem det ydre forsvar.

Betalingsinfrastrukturen i Danmark

Boks 1

Hver bankdag¹ sendes i gennemsnit betalinger for 724 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 mellemed, ender de alt efter type med at blive opgjort og afstemt i Sum-, Intradag- eller Straks-clearingen, der er den finansielle sektors detailbetalingssystemer kaldet Detailclearingerne. Afviklingen sker efterfølgende på konti i Nationalbanken via Kronos2. Detailclearingerne ejes af Finans Danmark.

Værdipapirhandler kan indgås på forskellige måder: På børsen, gennem en multilateral handelsplatform eller "over-the-counter" via bank eller fondsmægler. Afviklingen af handler med dansk udstedte værdipapirer håndteres af værdipapircentralen Euronext Securities Copenhagen, ES-CPH. Værdipapirhandler mellem banker og deres kunder afvikles via ES-CPH-afviklingen, der er ES-CPH's eget afviklingssystem, mens værdipapirhandler mellem de professionelle aktører (herunder banker) afvikles via den fælleseuropæiske platform Target2-Securities,

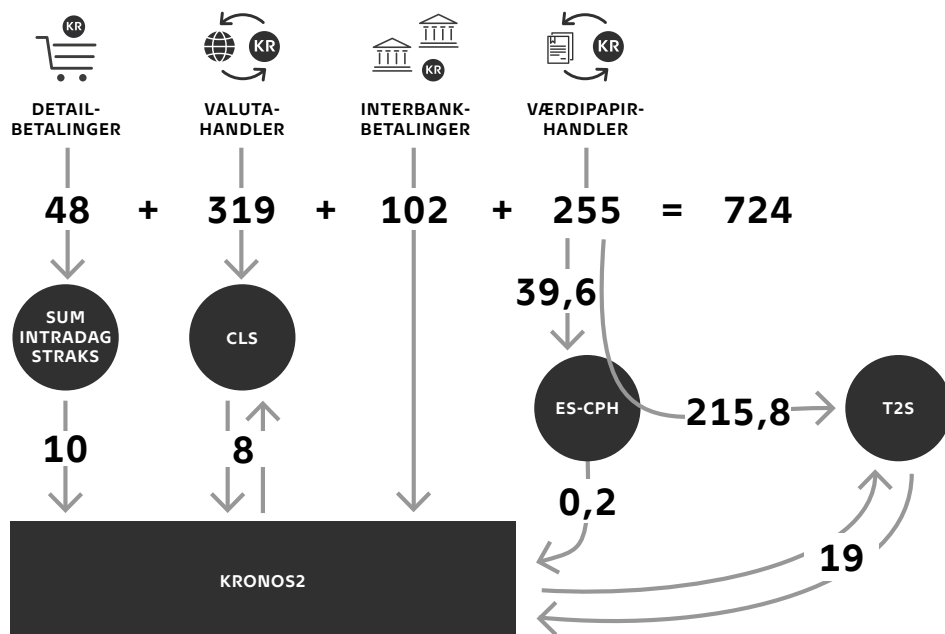
T2S, der ejes af Den Europæiske Centralbank, ECB, og de nationale centralbanker i Eurozonen. Deltagelse på T2S kræver bl.a. pengekonti i Nationalbanken og værdipapirkonti i ES-CPH. ES-CPH er således som værdipapircentral ansvarlig for at føre løbende regnskab med beholdningerne af alle dansk udstedte værdipapirer på vegne af investorerne.

Valutahandler afvikles gennem CLS, der er et internationalt system til valutahandler. Nationalbanken stiller konti til rådighed for de pengeinstitutter, der gennemfører handler via CLS. Deltagerne reserverer likviditet til CLS-afviklingen ved at overføre beløb til disse konti. CLS ejes af store internationale banker.

De tre detailbetalingssystemer 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. Denne såkaldte netting reducerer deltagernes likviditetsbehov betydeligt sammenlignet med en situation, hvor alle betalinger afvikles enkeltvist, fx reducerer netting likviditetsbehovet til afvikling af detailbetalinger fra 48 mia. kr. til 10 mia. kr. dagligt, svarende til en reduktion på 79 pct.

På T2S sker afviklingen af de professionelle aktørers handler også ved brug af netting. Likviditeten til afviklingen overføres fra deltagernes pengekonti i Nationalbanken. Nettingen reducerer deltagernes likviditetsbehov fra 216 mia. kr. til 19 mia. kr. (reservation af likviditet), hvilket svarer til en reduktion på 91 pct.

Betalingsflow, mia. kr., gennemsnit pr. bankdag i 2022



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

Ifølge internationale retningslinjer for cyberrobusthed¹ skal der i beredskabsarbejdet lægges specifikke planer for, hvordan alvorlige cyberhændelser skal håndteres. Planerne skal både adressere evnen til at foretage en sikker genopretning af centrale it-systemer (recovery) og evnen til at videreføre kritiske forretningsområder, i den tid genopretningen pågår. Det skal endvidere løbende testes, om planerne er tilstrækkelige til at håndtere ekstreme men plausible scenarier for cyberangreb.

Nationalbanken følger i sin overvågning af betalingsinfrastrukturen løbende systemejernes arbejde med cybersikkerhed og med at forberede sig på at håndtere cyberangreb. Som led i overvågningen gennemfører Nationalbanken også vurderinger af, om systemerne i betalingsinfrastrukturen lever op til kravene i internationale retningslinjer for cyberrobusthed.

I 2022 afsluttede Nationalbanken en vurdering af Detailclearingernes efterlevelse af retningslinjerne. Vurderingen viste, at Detailclearingerne har en høj modenhed og efterlever retningslinjerne på de fleste områder. Som led i vurderingen gav Nationalbanken Finans Danmark, der ejer Detailclearingerne, anbefalinger til, hvordan arbejdet på få men centrale områder kan styrkes.

Nationalbanken udarbejdede i 2020 også cyberanbefalinger til Euronext Securities Copenhagen, EC-CPH, efter de internationale retningslinjer. ES-CPH har i 2022 arbejdet videre med anbefalingerne. Endelig har Nationalbanken også arbejdet videre med at styrke robustheden for Kronos2.

Samarbejde på tværs af sektoren bruges aktivt til at øge robustheden

En del af arbejdet med at modgå cybertruslen sker på sektorniveau i forskellige samarbejdsfora, jf. boks 3.

Ejerne af de centrale systemer og løsninger i den danske betalingsinfrastruktur bruger arbejdet i Finansielt Sektorforum for Operationel Robusthed, FSOR, til at understøtte eget arbejde med at forebygge og håndtere cyberhændelser. Det sker bl.a. via drøftelse af risici, videndeling og fælles mitigerende initiativer.

Cybertruslen udvikler sig og ændrer karakter

Boks 2

Center for Cybersikkerhed, CFCS, vurderer, at truslen fra cyberkriminalitet mod den danske finanssektor er meget høj.¹ Som følge af krigen i Ukraine hævede CFCS 31. januar 2023 sin vurdering af truslen fra cyberaktivisme til høj.

Spændingerne mellem Rusland og Vesten har medført en høj aktivitet blandt pro-russiske cyberaktivister, som udfører angreb mod mål inden for en bred vifte af NATO-lande, herunder også Danmark. Det så man eksempelvis med de DDoS-angreb, der blev rettet mod Nationalbanken, andre dele af den finansielle sektor og offentlige myndigheder i starten af 2023.

CFCS vurderer, at truslen fra destruktive cyberangreb mod danske mål er lav. Cybertruslen kan dog hurtigt ændre karakter, hvis den sikkerhedspolitiske situation eskaleres. Blandt statslige aktører findes der kapacitet til at udføre avancerede cyberangreb. Der har indtil videre ikke været vilje til at gennemføre den type angreb mod Danmark, men det kan ændre sig.

1. Center for Cybersikkerhed: Cybertruslen mod finanssektoren, 8. februar 2023 ([link](#)).

I regi af FSOR's kriseberedskab blev der i forbindelse med Ruslands invasion af Ukraine delt viden om risici og mulige påvirkninger af den danske finansielle sektor. I efteråret 2022 blev risici i lyset af energisituationen i Europa adresseret, og systemejerne i betalingsinfrastrukturen har, ligesom den øvrige finansielle sektor, forberedt sig på risikoen for såkaldte brown-outs. Dette arbejde har vist, at systemejerne vil være i stand til at håndtere en sådan situation med kortvarige strømafbrydelser. Endelig er der i regi af kriseberedskabet i starten af 2023 delt viden om de gentagne DDoS-angreb mod den finansielle sektor. Det har medvirket til afklaring af, at de kritiske dele af betalingsinfrastrukturen ikke er blevet påvirket.

FSOR's kriseberedskab er etableret med henblik på at sikre en koordineret indsats på tværs af den finansielle sektor i tilfælde af en krise, som kan true den finansielle stabilitet. FSOR's kriseberedskabsplan supplerer medlemmernes egne beredskabsplaner og er ko-

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

ordineret med det nationale kriseberedskab varetaget af den nationale operative stab, NOST. Ved at deltage i kriseberedskabet og i de halvårige test af samme efterlever systemejerne internationale standarders anbefaling om deltagelse i tværgående sektortest.

FSOR har som del af sine risikoanalyser fremhævet behovet for at arbejde videre med databeskyttelse og recovery. På den baggrund igangsatte systemejerne i betalingsinfrastrukturen i regi af Risikoforum for Gensidige Afhængigheder, RGA, i 2021 et arbejde med at identificere de data, der ud fra et samfundsperspektiv skal passes særligt på, og hvis tilgængelighed er kritisk i en genetableringssituation. RGA har i begyndelsen af 2023 færdiggjort en fælles oversigt over relevante data og opnået en fælles forståelse for datas kritikalitet, der skal danne udgangspunkt for det videre arbejde.

Systemejerne har i RGA også fortsat arbejdet fra 2021 med fælles nedluknings- og genåbningsscenerier, der understøtter en kontrolleret nedlukning af den kritiske infrastruktur i tilfælde af operationelle hændelser, fx et alvorligt cyberangreb. Der er i 2022 udarbejdet køreplaner, og de første fælles test af planerne er gennemført.

De centrale systemer og løsninger i infrastrukturen deltager alle i Nordic Financial CERT, NFCERT, der er et fælles nordisk sektorsamarbejde om indsamling og deling af information om cybertrusler og cyberangreb. Derved styrkes deres muligheder for at opdage, forhindre og respondere hurtigt på eventuelle cyberangreb. Ved at deltage i NFCERT efterlever internationale standarders anbefalinger om at deltage i denne type tværgående informationsdeling.

TIBER-DK har testet kritiske aktører i den finansielle sektor

Endelig deltager systemejerne i betalingsinfrastrukturen også i Nationalbankens TIBER²-DK-testprogram. I TIBER-DK koordinerer Nationalbanken trusselsbase-rede tests af cyberrobustheden hos kritiske aktører i den finansielle sektor, hvor avancerede cyberangreb simuleres i faktiske produktionsmiljøer. I 2022 er læring på tværs af TIBER-testene blevet analyseret og delt med deltagerne med henblik på at styrke cyberrobustheden.

Fælles arbejde i FSOR, RGA og NFCERT

Boks 3

Finansielt Sektorforum for Operationel Robusthed, FSOR, har siden 2016 samlet myndigheder og centrale private aktører i den finansielle sektor i et fælles samarbejdsforum, der arbejder på at øge sektorens operationelle robusthed, herunder robustheden over for cyberangreb. Læs mere i FSOR's årsberetning for 2022 ([link](#)).

Nationalbanken varetager formandskab og sekretariat for samarbejdet, der – ud over systemerne og løsningerne i infrastrukturen – også har deltagelse af de største danske banker, datacentraler, pensions- og forsikringsselskaber samt relevante myndigheder og Nordic Financial CERT.

FSOR's arbejde tager udgangspunkt i en risikoanalyse, der identificerer de største risici for sektoren. Det giver retning for arbejdet med fælles mitigerende tiltag. Blandt disse er der fx et kriseberedskab, som koordinerer på tværs af sektoren i tilfælde af en systemisk krise. Nationalbanken varetager formandskab og sekretariat for FSOR-kriseberedskabet.

Risikoforum for Gensidige Afhængigheder, RGA, er et samarbejdsforum mellem de ansvarlige for de centrale betalings- og afviklingssystemer i infrastrukturen, dvs. Nationalbanken (interbankbetalinger), Euronext Securities Copenhagen (værdipapirhandler), Finans Danmark (detailbetalinger) og e-nettet (kommunikationsnetværk). RGA identificerer og adresserer gensidige afhængigheder og operationelle risici, der går på tværs af de centrale systemer og netværk i infrastrukturen.

Arbejdet i RGA koordineres med FSOR.

Nordic Financial CERT,¹ **NFCERT**, 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. I NFCERT indsamles og deles information om cybertrusler og cyberangreb.

1. Computer Emergency Response Team. Dette kaldes også Computer Security Incident Response Team, CSIRT.

2. Threat Intelligence Based Ethical Red team.

Konsolidering af infrastrukturen i færre og større systemer fortsætter

Gennem de seneste år har ejerne af systemerne i betalingsinfrastrukturen arbejdet på at samle forskellige dele af infrastrukturen i større fælles systemer. Dette arbejde er fortsat i 2022.

Øgede faste udgifter til driften af systemerne gør det i stigende grad attraktivt at samle aktiviteterne, så udgifterne i højere grad kan deles mellem flere systemejere og deltagere. Konsolideringen i færre og større systemer indebærer på den ene side en koncentrationsrisiko i form af en større afhængighed af enkelte systemer. Rationalet bag konsolidering er, at den risiko mere end opvejes af, at samlingen af ressourcer på den anden side gør det muligt at øge sikkerheden.

En del af værdipapirhandlerne i danske kroner er siden 2018 blevet afviklet på den fælleseuropæiske værdipapirafviklingsplatform T2S, og i 2020 besluttede Nationalbanken på baggrund af en foranalyse og dialog med den finansielle sektor at flytte al afvikling af betalinger i danske kroner til det fælleseuropæiske system TARGET Services. Projektet kaldes TARGET DKK. Migreringen er fastsat til påsken 2025, og arbejdet henimod migreringen forløb planmæssigt i 2022. Se boks 4, side 10, for en nærmere beskrivelse af TARGET DKK.

Ejeren af det danske system for afvikling af værdipapirhandler, Euronext Securities Copenhagen, besluttede i 2022 at udfase afviklingen af handler i danske kroner og euro fra ES-CPH's egen afviklingsplatform. Det betyder, at alle handler med værdipapirer i danske kroner og euro, der er registreret i ES-CPH, fra udgangen af 2024 vil blive afviklet på T2S.

På europæisk niveau gennemførte ECB i marts 2023 den planlagte konsolidering af interbankbetalingsystemet TARGET2 og T2S. I den forbindelse blev TARGET2 erstattet af et nyt centralt system for afvikling af betalinger kaldet T2. Med konsolideringen samles en række systemer, der understøtter T2 og T2S, på én samlet it-plattform kaldet TARGET Services.

De forskellige projekter er i høj grad indbyrdes afhængige og koordineres tæt mellem de forskellige systemejere, deltagerne i systemerne og øvrige interessenter.

Konsolideringen af infrastrukturen i færre og større systemer vil samtidig betyde, at Nationalbankens overvågning i tiltagende grad vil komme til at foregå i samarbejde med ECB og de øvrige europæiske centralbanker.

Interbankbetalinger og den centrale afvikling af betalinger i danske kroner

Nationalbankens betalingssystem, *Kronos2*, er en af de vigtigste dele af den finansielle infrastruktur i Danmark. Kronos2 står i centrum for afviklingen af betalinger i danske kroner – herunder de store, tidskritiske betalinger mellem bankerne (interbankbetalinger). Derudover anvendes Kronos2 også til at afvikle Nationalbankens pengepolitiske operationer og nettopositioner fra de tilsluttede betalings- og afviklingssystemer vedrørende borgeres og virksomheders betalinger, værdipapirhandler og valutahandler i danske kroner.³

Brug

Ved udgangen af 2022 var der 77 direkte deltagere i Kronos2. Deltagerne er primært danske banker og realkreditinstitutter samt filialer af udenlandske banker.

Både i antal og værdi udgør interbankbetalinger hovedparten af overførslerne mellem deltagernes konti i Kronos2. I 2022 blev der gennemført interbankbetalinger i Kronos2 med en værdi af 101,5 mia. kr. i gennemsnit pr. bankdag, jf. tabel 1. Værdien af interbankbetalinger er steget med 14 pct. siden 2021. Denne stigning har været drevet af en øget betalingsaktivitet hos de to største deltagere, Danske Bank og Nordea.

Antallet og værdien af de pengepolitiske operationer var fortsat faldende i 2022 på grund af den tilpasning af de pengepolitiske instrumenter, som Nationalbanken foretog i marts 2021, hvor loftet over bankernes indestående på foliokonti blev fjernet, så de ikke længere har behov for at flytte likviditet ved at købe og sælge indskudsbeviser.

Driftsstabilitet

I løbet af 2022 har der været flere hændelser, som har påvirket Kronos2, hvorved driftsstabiliteten ikke var helt tilfredsstillende.

I to tilfælde var Nationalbanken og deltagerne uden adgang til Kronos2 i henholdsvis 3 timer og 1 time. Begge gange var årsagen en fejl i opsætningen af servere. Selve Kronos2's funktion og opetid blev ikke påvirket.

Der har også været problemer med Nationalbankens sikkerhedsstillelsessystem, *Calypso*⁴, hvor adgangen til systemet for Nationalbanken og deltagerne flere gange var forsinket i begyndelsen af dagen på grund af manglende opdateringer af servere.

I to tilfælde har der endvidere været brud på Nationalbankens politik om, at deltagere ikke må være i overtræk ved lukningen af det pengepolitiske døgn (overtrækkene skete dog mod sikkerhed). Begge episoder medførte forsinkelser af lukningen af det pengepolitiske døgn og af afviklingen af værdipapirhandler hos ES-CPH. Derudover blev afviklingen af værdipapirhandler hos T2S i det ene tilfælde forsinket for både danske kroner og euro. Årsagen til hændelserne var manglende likviditetsstyring og utilstrækkelige procedurer for inddækning af overtræk hos de involverede deltagere.

Hen mod slutningen af året oplevede Kronos2 desuden en uautoriseret nedlukning i over tre timer på grund af en menneskelig fejl. Eftersom det skete omkring kl. 18.00 en lørdag aften, var der ikke forretningsmæssige konsekvenser som følge af hændelsen.

Endelig har der været en hændelse, hvor der efter en forsinkelse af CLS-afviklingen (se også afsnittet 'Valutahandelsafvikling' på side 24) og efterfølgende udskydelse af lukningen af det pengepolitiske døgn i Kronos2 opstod fejl i kommunikationen mellem Nationalbanken og ES-CPH. Det ledte til forsinkelser af afviklingen af værdipapirhandler hos ES-CPH og brug af nødprocedurer for genindsættelse af likviditet på konti i Kronos2 til afvikling af værdipapirhandler hos ES-CPH.

³ Se også boks 1 om betalingsinfrastrukturen i Danmark.

⁴ Calypso er det system, som Nationalbanken stiller til rådighed med henblik på, at deltagerne i Kronos2 kan stille sikkerhed og få en kreditlinje herfor, som kan anvendes til at gennemføre betalinger i Kronos2.

Transaktioner i Kronos2

Tabel 1

Mia. kr., gennemsnit pr. bankdag	2018	2019	2020	2021	2022
Interbankbetalinger	83,0	87,4	87,6	88,7	101,5
- Heraf kundebetalinger	13,6	14,0	14,0	16,6	20,7
Pengepolitiske operationer	36,9	48,4	34,5	6,1	0,3
- Heraf salg af indskudsbeviser	36,9	48,4	33,3	5,6	0,0
- Heraf pengepolitiske udlån	0,0	0,0	1,3	0,5	0,3
Overførsler til afviklingssystemer	237,3	115,1	113,8	106,1	97,9
- Heraf til Sum-, Intradag- og Straksclearingen	177,2	40,5	39,9	40,6	40,1
- Heraf til ES-CPH-afviklingen (tidligere VP-afviklingen)	40,6	46,4	41,2	38,3	35,2
- Heraf til CLS	19,6	28,2	32,8	27,2	22,5
Afviklede nettopositioner	24,1	16,3	16,6	17,0	17,9
- Heraf Sum-, Intradag- og Straksclearingen	8,1	8,3	8,3	9,3	10,0
- Heraf ES-CPH-afviklingen	9,1	1,0	0,9	0,8	0,2
- Heraf CLS	6,8	7,0	7,3	6,8	7,7
Overførsler til T2S (Reservation af likviditet til afviklinger) *	20,1	21,5	22,2	22,1	18,6

* Deltagernes overførsler fra Kronos2 til T2S sker med henblik på at reservere likviditet på konti i T2S til at kunne gennemføre afvikling af værdipapirhandel. Dette svarer til den reservation af likviditet, der finder sted på konti i Kronos2 til at gennemføre afviklinger af detailbetalinger, værdipapirhandel og valutahandel. Når afviklingerne af værdipapirhandel i T2S er færdige, føres pengene hver dag tilbage fra T2S til deltagerens konti i Kronos2.

Nationalbankens overvågning har gennemgået ovennævnte hændelsesforløb og vurderer, at håndteringen og opfølgningen på hændelserne har været tilfredsstillende. Dette omfatter tekniske forbedringer, skærpet monitorering, proceduremæssige tiltag og dialog med deltagere og andre involverede parter.

Likviditet

I 2022 har deltagerne fortsat haft rigelig likviditet til at gennemføre betalinger i Kronos2, både interbank-

betalinger og de betalinger, der følger af afviklingsinstrukser fra de tilsluttede betalings- og afviklingssystemer (Detailclearingerne, ES-CPH og CLS), jf. figur 1.

Internationale standarder

Som beskrevet nedenfor er der i 2022 blevet arbejdet videre med de forbedringspotentialer, der blev identificeret i overvågningens vurdering af Kronos2 efter CPMI-IOSCO's principper for finansiel markedsinfrastruktur, PFMI, i 2021.⁵ Dermed er det eneste

⁵ Danmarks Nationalbank, Vurdering af Kronos2, *Danmarks Nationalbank Rapport*, nr. 4, december 2021 ([link](#)).

udestående fra vurderingen at gennemføre en test af Nationalbankens eget kriseberedskab og sektorens fælles beredskab (FSOR's kriseberedskab⁶) samtidigt.

I begyndelsen af året godkendte Nationalbankens øverste ledelse en årsplan for operationel risikostyring i 2022. I årsplanen fastlægges, hvilke konkrete opgaver og projekter der skal forfølges og prioriteres for at gennemføre målsætningerne i Nationalbankens Risikopolitik – herunder specifikke forretningsmæssige og it-relaterede risikovurderinger, kritiske projekter, tests og it-sikkerhedsinitiativer af relevans for Kronos2. Ledelsen har efterfølgende fulgt op på, om årsplanen for 2022 – og dermed risikopolitikken – er blevet efterlevet. Årsplanen for operationel risikostyring i 2023 er desuden blevet godkendt.

Nationalbanken har i 2022 gennemført tekniske risikovurderinger af alle de væsentligste systemkomponenter i Kronos2. Processen for opdatering af tekniske risikovurderinger er blevet styrket med en hyppigere ajourføring af risici og kontroller. Placeringen af ansvaret for opdatering af de tekniske risikovurderinger er endvidere blevet tydeligere.

Nationalbankens nødløsning i tilfælde af et længerevarende nedbrud i Kronos2 er blevet testet mere udførligt – dvs. test af Extreme Contingency Facility, ECF, sammen med Intradagclearingen. Det er i den forbindelse også blevet afklaret, hvilke betalinger der skal sendes til henholdsvis ECF (kun kritiske betalinger) og Intradagclearingen.

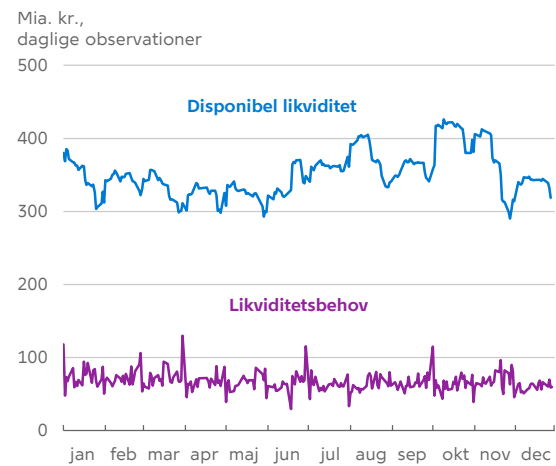
Mere overordnet er der blevet etableret et overblik og en samling af de eksisterende planer for test (med prioritering ud fra et forretningskritisk synspunkt), der omfatter de tekniske tests, sikkerhedstests og tests af nødløsninger, der skal gennemføres årligt.

Cyberrobusthed

I 2022 er der blevet arbejdet med flere it-sikkerhedsmæssige initiativer af betydning for Kronos2 i forbindelse med SWIFT CSP⁷-gennemgangen af den tekniske platform, som systemet kører på. Dette har omfattet sårbarhedsscanninger, hærkning (med secure zone-komponenter) og firewall review.

Disponibel likviditet versus likviditetsbehov hos deltagerne i Kronos2 i 2022

Figur 1



Anm: Deltagernes disponible likviditet består af indestående på deres hovedkonti i Nationalbanken tillige med deres mulighed for at låne inden for dagen mod sikkerhed.

Kilde: Danmarks Nationalbank.

Der er ligeledes blevet foretaget periodiske test, bl.a. af Nationalbankens nød-pc'er, det interne beredskab og kontrolleret nedlukning af kritisk it-infrastruktur. Dette skal sikre, at Kronos2 er velforberedt i tilfælde af en skarp situation som fx et cyberangreb.

I 2022 har Nationalbanken påbegyndt arbejdet med en vurdering af sikkerhedsstillelses-systemet for betalinger i Kronos2, Calypso, efter CPMI-IOSCO's retningslinjer for cyberrobusthed, der uddyber de mere generelle principper fra CPMI-IOSCO (PFMI). Disse retningslinjer er også kendt som Cyber Guidance.

Systemændringer

Der er ikke blevet foretaget større systemændringer af Kronos2 i 2022.

Der arbejdes fortsat på den planlagte migrering af afviklingen i danske kroner fra Kronos2 til det fælles-europæiske system TARGET Services i påsken 2025, se boks 4.

⁶ Se en kort beskrivelse af FSOR's kriseberedskab på Nationalbankens hjemmeside ([link](#)).

⁷ SWIFT Customer Security Programme, CSP, omfatter en række sikkerhedskontroller.

Danske kroner på Target Services i 2025

Boks 4

I 2020 besluttede Nationalbanken på baggrund af en foranalyse og dialog med den finansielle sektor at migrere afviklingen i danske kroner fra Kronos2 til det fælleseuropæiske system TARGET Services. TARGET Services omfatter det centrale system for afvikling af betalinger T2, værdipapirafviklingssystemet T2S og afviklingssystemet for straksbetalinger TIPS. Migreringen er planlagt til at finde sted i påsken 2025.

En del af de danske værdipapirhandler er blevet afviklet i danske kroner på T2S siden 2018. Med migreringen af afviklingen i danske kroner til T2 og TIPS i 2025 vil al afvikling i danske kroner derefter være samlet på TARGET Services.

I forlængelse af den foranalyse, der førte til beslutningen om at migrere afviklingen i danske kroner fra Kronos2 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 de likviditetsmæssige og tekniske aspekter samt til at planlægge og koordinere test- og go-live-aktiviteter i sektoren.

Programmets analyse- og designfase blev afsluttet ved udgangen af 1. kvartal 2023. Med hensyn til TARGET Services er det afstemt, hvilke tilpasninger hos ECB/4CB der er nødvendige for at imødekomme danske behov.

Fokus er nu i højere grad rettet mod test af løsningerne. Nationalbanken starter medio 2023 med at teste op mod TARGET Services, og herefter vil der planmæssigt være test med sektoren frem mod go-live i Påsken 2025. Der vil også være test af Nationalbankens system for pengepolitiske instrumenter og sikkerhedsstillelse, Calypso, som ikke er omfattet af TARGET Services. Derudover fortsætter forberedelserne til selve migreringen og den fremtidige organisering af driften og forvaltningen af de nye løsninger.

Detailbetalinger

Dankort, internationale betalingskort (VISA og Mastercard), MobilePay, Apple Pay, overførsel via netbank og Betalingservice er blandt de danske borgeres og virksomheders foretrukne betalingsløsninger, når der skal foretages betalinger af køb og regninger. I 2022 blev der gennemført transaktioner med disse og andre elektroniske betalingsløsninger for 33,2 mia. kr. i gennemsnit pr. dag.⁸

Nationalbanken overvåger de vigtigste betalingsløsninger i Danmark. For øjeblikket er Dankort og Betalingservice under overvågning. Konto til konto-overførsler overvåges 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 større betydning på det danske marked.

I 2022 var det gennemsnitlige transaktionsomfang for de internationale betalingskort 0,8 mia. kr. pr. dag,⁹ og for MobilePay lå det på 0,5 mia. kr. pr. dag.¹⁰ Til sammenligning udgjorde værdien af betalinger med Dankort, som er omfattet af Nationalbankens overvågning, i gennemsnit 1 mia. kr. pr. dag.¹¹

Dankort

Nationalbankens overvågning af Dankort er rettet mod Nets, der er systemejer for Dankort.

Siden begyndelsen af 2022 har Nets indgået i en koncern (Nexi Group), som er en fusion af Nets og de italienske virksomheder Nexi og SIA.¹² Det nye selskabsmæssige grundlag for virksomheden og de organisatoriske ændringer har ikke haft betydning for driften af Dankort eller Nationalbankens overvågning.

I 2022 er der blevet gennemført forskellige tiltag, der kan have betydning for Dankorts konkurrencemæssige stilling i markedet.

I januar indførte Nets en ny og mere enkel prismodel for forretninger, der tager imod betaling med Dankort på internettet.¹³ Den nye model er især en fordel for forretninger, der gennemfører transaktioner med et lavt gennemsnitligt beløbsniveau.¹⁴

I april sænkede Nets priserne for Dankort for forretningerne i den fysiske handel med 8 pct. som følge af en afgørelse fra Konkurrence- og Forbrugerstyrelsen.¹⁵ I afgørelsen blev der fastlagt et lavere loft for det årlige beløb, som Nets må opkræve i gebyr af forretningerne for brugen af Dankort i butikkerne.¹⁶

I august forhøjede og ensrettede Nets sine betalingsgarantier til forretningerne. Herefter er forretningerne sikret betaling ved et beløb på op til 8.000 kr. i tilfælde af efterfølgende indsigelse (krav om tilbageførsel af en betaling) fra en bank på grund af manglende dækning på kortholders konto eller en tredjeparts misbrug af kortet til køb på internettet eller i en butik.¹⁷

I oktober gjorde Danske Bank det muligt for sine kunder at anvende Dankort i Apple Pay i stedet for VISA eller Mastercard. Dette er første gang, at Dankort-brugere får mulighed for at anvende Dankort i Apple Pay til betalinger.¹⁸ Samme måned lukkede Nets for muligheden for betaling med Dankort app med henvisning til, at Nets vil arbejde for, at Dankort i stedet skal kunne anvendes i Apple Pay og Google Pay.¹⁹

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

9 Nationalbankens statistikbank – DNBSTS-tabellen – sammenholdt med oplysninger fra Nets' statistik for Dankort.

10 MobilePay, MobilePay i rekordår: Passerede 500 mio. transaktioner, den 2. januar 2023 ([link](#)).

11 Nets' statistik for Dankort.

12 Nexi Group, Nexi Group's Transformation Path ([link](#)).

13 Nets, Tag nemt og billigt imod Dankort på din webshop ([link](#)).

14 Nets, Nets ændrer prismodel for handel med Dankort på nettet, den 16. november 2021 ([link](#)).

15 Dansk Erhverv, Lavere priser på Dankort, den 30. marts 2022 ([link](#)).

16 Konkurrence- og Forbrugerstyrelsen, Lavere loft for Nets' dankort-opkrævninger hos fysiske butikker, den 9. december 2021 ([link](#)).

17 Betalingskortaftale for Dankort (jf. ændring den 18. august 2022) ([link](#)).

18 Nets, Danske Bank to bring domestic scheme, Dankort, to Apple Pay, den 12. oktober 2021 ([link](#)).

19 Finanswatch, Nets vil flytte fokus fra app til Apple Pay, den 13. september 2022 ([link](#)).

Dankort – driftsstabilitet

Driften af Dankort var tilfredsstillende i 2022. I løbet af året har der været en enkelt hændelse med betydning for Dankort.

Den 21-25. juni 2022 var der driftsforstyrrelse af NemID. Det gav problemer ved betalinger med Dankort på internettet, som skulle godkendes med autentifikation af kortholder via NemID.²⁰ Nets har ikke fuldt overblik over, hvad hændelsen har betydet for Dankort. Det er dog Nets' vurdering, at hændelsen havde begrænset indvirkning på kortbetalingerne.

Efterfølgende er der med den endelige overgang til MitID i slutningen af oktober 2022 blevet lukket for brugen af NemID. Eftersom MitID og NemID er grundlæggende forskellige løsninger, vurderer Nets, at en lignende hændelse ikke vil kunne ske for MitID.

Nationalbanken har fulgt op på Nets' håndtering af og rapportering om hændelsen.

Dankort – misbrug

I 2022 lå det samlede misbrug af Dankort på 20,9 mio. kr., hvilket svarer til en stigning på 17 pct. i forhold til niveauet i 2021. Set i forhold til det samlede forbrug med Dankort udgjorde misbruget 0,06 promille i 2022 mod 0,05 promille i 2021. Nets vurderer, at stigningen i misbruget af Dankort hovedsageligt kan henledes til genåbningen af samfundet i 2022 efter perioden med restriktioner på grund af covid-19 i 2020 og 2021. Misbruget lå på 0,08 promille i 2019 (før covid-19) og var dermed højere end i 2022.

Størstedelen af misbruget af Dankort sker i butikker og hæveautomater på grund af tyveri eller tab af kort. Denne type af misbrug steg med 28 pct. i 2022 til 16,4 mio. kr. Efter stigninger i både 2021 og 2022 er misbrugsniveauet således omtrent det samme, som det var i 2019, hvor det lå på 15,9 mio. kr.

Misbruget af Dankort ved handel på internettet lå i 2022 på 4,5 mio. kr., svarende til et fald på 9 pct. i sammenligning med året inden.²¹ Betragtet som andel af forbruget med Dankort på internettet lå misbrugsniveauet dog uændret på 0,05 promille.²²

I begyndelsen af 2022 introducerede Nets *Dankort Advarselsservice*. Det er en service, som skal bidrage til at nedbringe misbruget i webshops. Hvis Nets har registreret misbrug af et Dankort, og det er blevet brugt til køb i en forretning på internettet, vil forretningen modtage en notifikation fra Nets på e-mail med en advarsel om potentielt misbrug. Det giver forretningen mulighed for at stoppe forsendelsen af varerne.²³

Betalingservice

Nationalbankens overvågning af Betalingsservice er rettet mod Mastercard Payment Services Denmark A/S, MPS, der er systemejer for Betalingsservice.

I 2022 har MPS taget yderligere skridt i processen med at overtage driften af Betalingsservice, som de købte af Nets i 2021. Aftalen mellem MPS og Nets forpligter Nets til at understøtte driften af Betalingsservice i 3 år frem til marts 2024, der altså er fristen for MPS's etablering af de nødvendige processer og it-infrastruktur m.v. til driften af Betalingsservice.

MPS har i august 2022 indgået aftale med Kyndryl om levering af det system og tilhørende tjenester, der ligger til grund for Betalingsservice (tidligere et aftaleforhold mellem Nets og Kyndryl). Kyndryl fortsætter således med at være den centrale leverandør i forhold til Betalingsservice.

Det er Nationalbankens vurdering, at MPS's overtagelse af driften af Betalingsservice er præget af kontinuitet, både personalemæssigt og teknisk.

20 Kortholdere, der havde oprettet MitID eller betalingsvalidering med kodeord og sms-kode, havde mulighed for at bruge disse som alternativer, mens NemID var ude af funktion.

21 Ved handel på internettet kan Dankort kun anvendes i danske forretninger. Når et co-branded Dankort anvendes til køb på en webshop i udlandet, er det altså VISA-siden af kortet, der anvendes.

22 Nets' statistik for misbrug af Dankort. Bemærk, at Nets' misbrugstal ikke er direkte sammenlignelige med Nationalbankens statistik over misbrug med betalingskort, der viser misbruget med rene Dankort og co-brandede Dankort i Danmark.

23 Nets, Dankort Advarselsservice ved formodet misbrug ([link](#)).

Betalingservice – driftsstabilitet og misbrug

Der har ikke været nedbrud eller andre hændelser af betydning i Betalingservice i 2022. Driftsstabiliteten var således høj i 2022.

Der har ikke været misbrug af Betalingservice i 2022.

Internationale standarder

Nationalbanken har i 2022 været i dialog med Nets og MPS om de nye ECB-standarder (PISA)²⁴ for betalingsløsninger som Dankort og Betalingservice. I Eurosystemet blev overgangen til PISA formelt fastsat til den 15. november 2022.²⁵ Eftersom PISA i vidt omfang viderefører kravene i de nuværende ECB-standarder, herunder kravene på de centrale områder, ser Nationalbanken ikke umiddelbart behov for større tilpasninger hos Nets og MPS vedrørende Dankort og Betalingservice eller i Nationalbankens overvågning.

24 Payment Instruments, Schemes & Arrangements (Eurosystem oversight framework). Danmarks Nationalbank, Overvågning af den finansielle infrastruktur 2021, *Danmarks Nationalbank Rapport*, nr. 3, maj 2022, boks 4, side 1 ([link](#)).

25 *Eurosystem publishes new framework for overseeing electronic payments*, November 2021 ([link](#)).

Clearing og afvikling af detailbetalinger

Sum-, Intradag- og Straksclearingen – også kaldet *Detailclearingerne* – er den finansielle sektors systemer til clearing og afvikling af danske detailbetalinger. Systemerne ejes af Finans Danmark, forvaltes af e-nettet, der er den finansielle sektors projekt- og forvaltningsselskab, og leveres af Mastercard Payment Services Danmark A/S, MPS.

I Sumclearingen afvikles betalinger foretaget med bl.a. kort og Betalingservice én gang i døgnet på bankdage. I Intradagclearingen afvikles konto til konto-overførsler som fx netbank-overførsler, løn-udbetalinger og offentlige udbetalinger fem gange i døgnet på bankdage. 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 Mobile-Pay.

Brug

Ved udgangen af 2022 var der 47 direkte deltagere i Detailclearingerne og 23 indirekte deltagere, som afvikler gennem en direkte deltager. Værdien af transaktionerne i systemerne udgjorde i gennemsnit 48,1 mia. kr. pr. bankdag i 2022, jf. tabel 2.

Antallet af transaktioner i Straksclearingen er steget i både 2021 og 2022 efter et uændret niveau fra 2019 til 2020, jf. figur 2.

Driftsstabilitet

Driften af Detailclearingerne er i 2022 forløbet tilfredsstillende. Der har dog været enkelte mindre hændelser, hvor der i korte perioder ikke kunne gennemføres betalinger via Straksclearingen. En af disse skyldtes tekniske problemer hos en datacenter, der resulterede i, at et udsnit af kunder ikke havde mulighed for at sende straksoverførsler.

Værdi af transaktioner i Sum-, Intradag- og Straksclearingen

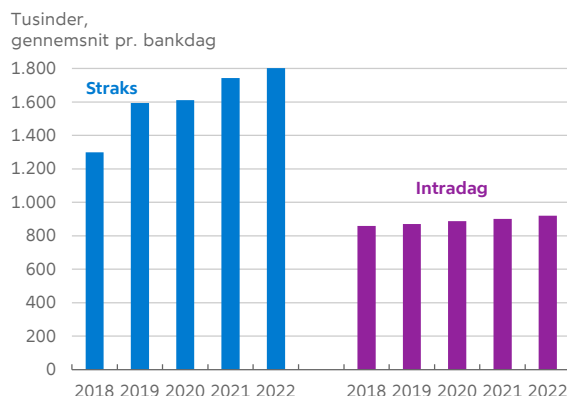
Tabel 2

Mia. kr., gennemsnit pr. bankdag	2018	2019	2020	2021	2022
Sumclearingen	18,3	19,2	18,7	20,5	21,3
Intradagclearingen	20,1	20,8	21,9	23,9	25,0
Straksclearingen	1,2	1,4	1,6	1,7	1,8
I alt	39,6	41,4	42,2	46,1	48,1

Kilde: Mastercard Payment Services Danmark A/S, MPS.

Antal transaktioner i Intradag og Straksclearingen, 2018-22

Figur 2



Kilde: Mastercard Payment Services Danmark A/S, MPS.

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 Detailclearingernes automatiserede værktøjer til likviditetsstyring, og der har i 2022 ikke været tilfælde, hvor deltagere er blevet henlagt på grund af manglende likviditet.

I Straksclearingen forekommer der ikke likviditetsrisiko mellem deltagerne. Det skyldes, at Straksclearingen er et reeltidsafviklingssystem, hvor deltagerne på forhånd afsætter likviditet i form af sikkerhedsstillelse for betalingerne, der løbende afvikles på kundernes konti, i takt med at de foretages. Er der ikke afsat tilstrækkelig likviditet, afvises betalingerne.

Cyberrobusthed

Finans Danmark arbejder løbende på at styrke cyberrobustheden i detailbetalingsinfrastrukturen. Centralt i dette arbejde er en cybersikkerhedshåndbog for clearingerne, som blev introduceret i 2021. I håndbogen stiller Finans Danmark krav til it-sikkerheden hos MPS og de deltagende banker, der årligt skal evaluere og rapportere deres efterlevelse af kravene til Finans Danmark.

Finans Danmark har i starten af 2022 fulgt op på den første rapportering og været i dialog med deltagerne om håndbogens bestemmelser. Dialogen resulterede i en opdateret og præciseret version af håndbogen.

Den seneste rapportering ud fra cybersikkerhedshåndbogen, som blev gennemført ultimo 2022, viser, at modenheden på cyberområdet er tilfredsstillende. På baggrund af deltagernes rapportering har Finans Danmark udpeget en række emner, som deltagerne og deres datacentraler anbefales at arbejde videre med for at øge modenheden yderligere.

Internationale standarder

I maj 2022 afsluttede Nationalbanken en vurdering af Detailclearingernes efterlevelse af CPMI-IOSCO's retningslinjer for cyberrobusthed (Cyber Guidance). Vurderingen viser, at Detailclearingerne har en høj modenhed og efterlever Cyber Guidance på de fleste

områder. Der er dog få, men centrale områder, hvor Detailclearingerne ikke efterlever de internationale retningslinjer fuldt ud. Nationalbanken har anbefalet Finans Danmark at styrke arbejdet på disse områder, og Finans Danmark har lagt en plan for, hvordan de vil imødekomme anbefalingerne.

Systemændringer

Finans Danmark arbejder på at forhøje beløbsgrænsen i Straksclearingen. På nuværende tidspunkt er beløbsgrænsen 500.000 kr., men ifølge Finans Danmark oplever bankerne et stigende behov for at lave større betalinger i realtid.

Finans Danmark har udarbejdet en række krav for bankernes brug af Straksclearingen, som skal efterleves, inden beløbsgrænsen kan hæves. Der er bl.a. krav om differentierede beløbsgrænser for afsendelse af straksbetalinger, bl.a. via kundesegmentering. Dertil er der krav om overvågning af betalinger, så mistænkelige overførsler opdages, og mulighed for hurtig tilbagekaldelse af betalinger.

Nationalbanken har derudover anbefalet Finans Danmark, at der udarbejdes en analyse af risikoen for kriminelle transaktioner og potentielle cyberrisici, der kan følge af en forhøjelse af beløbsgrænsen. Finans Danmark arbejder fortsat på risikoanalysen og forventer, at ændringen i beløbsgrænsen kan træde i kraft i løbet af 2023.

Mastercards overtagelse af driften af Detailclearingerne

I 2021 købte og overtog MPS de områder af Nets' infrastruktur, der omfatter drift af Detailclearingerne. I 2022 modtog MPS betinget samtykke fra Finans Danmark til at igangsætte en datacenter-flytning, således at driften af Intradag- og Straksclearingen flyttedes fra Nets' datacentre i Norge til nye datacentre i henholdsvis Norge og Sverige.

Det nye datacenter-setup vil bestå af et primært driftssted med en duplikeret opsætning i to fysisk adskilte datacentre og et sekundært driftssted i et andet land, hvorfor der i praksis vil være 3 datacentre i alt. Parallelt migreres driften af Sumclearingen fra Nets' produktionsmiljø hos Kyndryl til MPS's produktionsmiljø hos samme.

Flytningen af datacentrene, herunder tidspunkt, er koordineret med TARGET DKK-projektet og sektorens program for fremtidens betalingsinfrastruktur, jf. nedenfor.

Den fremtidige detailbetalingsinfrastruktur

I 2018 etablerede seks nordiske banker²⁶ selskabet P27 Nordic Payments i Sverige og valgte MPS som it-leverandør til det tilhørende betalingssystem. I 2021 besluttede en samlet dansk sektor at arbejde henimod, at de eksisterende detailbetalingssystemer (Detailclearingerne) skulle erstattes med P27's nordiske detailbetalingssystem. Det var planen, at P27 skulle gå live med danske kroner i påsken 2025, samtidig med at systemet tilsluttede sig TARGET DKK. Grundet forsinkelser har en samlet dansk sektor i marts 2023 i stedet besluttet at integrere de eksisterende detailbetalingssystemer, Sum- og Intradagclearingen, til TARGET DKK. Det er samtidig besluttet, at straksbetalinger skal afvikles direkte i TIPS på TARGET Services.

Arbejdet med den fremtidige detailbetalingsinfrastruktur er forankret i et sektorprogram under Finans Danmarks bestyrelse, og der er nedsat en styregruppe med bred sektorrepræsentation. Programmet drives af e-nettet i tæt samarbejde med Finans Danmark. Programmet er tæt koordineret med Nationalbankens TARGET DKK-projekt.

Lovgrundlag for detailbetalingssystemer

I januar 2022 trådte en ny dansk lov i kraft rettet imod virksomheder, der forestår clearing og afvikling af detailbetalinger i danske kroner, og for it-operatører af detailbetalingssystemer.²⁷ Loven har to overordnede formål:

- 1) At sikre, at Nationalbanken altid kan føre tilsyn/overvågning med udenlandske betalingssystemer under dansk lov.²⁸
- 2) At sikre, at Finanstilsynet har lovhjemmel til at foretage it-tilsyn med en it-operatør af et detailbetalingssystem. Som aktuel operatør af Detailclearingerne i Danmark modtog MPS i oktober 2022 tilladelse fra Finanstilsynet til at varetage den nuværende it-drift af Detailclearingerne. Dette var en lovpligtig procedure som følge af MPS's overtagelse af Nets' clearinginfrastruktur.²⁹

26 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.

27 Lov nr. 2382 af 14/12/2021: *Lov om ændring af lov om finansiel virksomhed, lov om kapitalmarkeder, lov om investeringsforeninger m.v. og forskellige andre love.*

28 Det følger af § 180 i kapitalmarkedsloven, at tilsynsbeføjelser udøves af Nationalbanken for så vidt angår systemer omfattet af Nationalbankens overvågning.

29 Jf. Danmarks Nationalbank, *Overvågning af den finansielle infrastruktur 2021, Danmarks Nationalbank Rapport, nr. 3, maj 2022 (link)* for yderligere information om MPS's køb af clearinginfrastrukturen.

Værdipapirafvikling

Værdipapirhandler kan indgås på forskellige måder: på børsen, gennem en multilateral handelsfacilitet eller bilateralt mellem parterne via en bank eller en fondsmægler. Den endelige afvikling af handlerne, dvs. hvor penge og værdipapirer udveksles mellem deltagerne, sker i to centrale systemer for afvikling af værdipapirhandler i henholdsvis den danske og europæiske finansielle infrastruktur samt i Kronos2.

I juridisk forstand finder den endelige afvikling af alle handler med dansk udstedte værdipapirer sted på konti i værdipapircentralen *Euronext Securities Copenhagen*, ES-CPH,³⁰ dvs. registreringen af ændringer i beholdningerne af værdipapirer sker på deltagerens konti i ES-CPH.

Værdipapirhandler mellem de professionelle aktører (herunder bankerne) – både deres egne handler og handler på vegne af deres kunder – afvikles teknisk set på konti i *TARGET2-Securities*, T2S, som ES-CPH har outsourcet afviklingsprocessen til ("T2S-afviklingen"). Flytninger af værdipapirer på konti i T2S spejles efterfølgende på konti i ES-CPH's systemer.

Værdipapirhandler mellem bankerne og deres kunder afvikles i ES-CPH's eget afviklingssystem ("ES-CPH-afviklingen").

Afviklingen af pengesiden finder sted på konti i Kronos2 for handler behandlet i ES-CPH-afviklingen og på konti i T2S for handler behandlet i T2S-afviklingen. Hver dag overfører deltagerne derfor likviditet til deres afviklingskonti i danske kroner på T2S.

ES-CPH står også for håndtering af periodiske betalinger, emissioner, indfrielse mv. og er den eneste virksomhed i Danmark med tilladelse fra Finanstilsynet til at udstede og opbevare værdipapirer.

Brug

ES-CPH har 88 deltagere, hvoraf 40 er udenlandske markedsdeltagere, herunder fire CCP'er³¹. 48 af deltagerne i ES-CPH har også en konto i Kronos2, så de kan overføre likviditet til deres afviklingskonto på T2S. Der er også mulighed for at overføre likviditet til afviklingskonti på T2S uden at være deltager i Kronos2.

J.P. Morgan blev i sommeren 2022 direkte deltager hos ES-CPH i stedet for at benytte en indirekte tilslutning gennem en anden deltager. Det er en generel tendens, at store globale banker (global custodians) tilslutter sig direkte til de lokale værdipapircentraler i EU, hvor man hidtil har benyttet såkaldte subcustodians.³² Dette kan blandt andet tilskrives den standardisering blandt europæiske værdipapircentraler, der er sket med ikrafttrædelsen af den fælleseuropæiske regulering af værdipapircentraler, CSDR, som har mindsket behovet for subcustodians med kendskab til lokale forhold.³³

I 2022 blev der i gennemsnit afviklet 91.300 handler om dagen i danske kroner gennem ES-CPH-afviklingen og T2S, hvilket er fald på ca. 10 pct. fra 2021, jf. tabel 3 og figur 3. Det skyldes især et fald i antallet af aktiehandler. Værdien af de afviklede handler var dog med et dagligt gennemsnit på 255,4 mia. kr. det højeste nogensinde for værdipapirer i danske kroner.

30 ES-CPH hed indtil november 2020 VP Securities. Her blev VP Securities opkøbt af den paneuropæiske børs- og markedsinfrastruktur-koncern Euronext Group. Navneskiftet er alene kommercielt, og den danske virksomhed er stadig registreret som VP Securities A/S i CVR-registeret.

31 De fire udenlandske CCP'er i ES-CPH er hhv. Cboe Clear Europe N.V., 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 Cboe Clear Europe N.V. og Nasdaq Clearing AB.

32 Subcustodians er banker eller andre markedsdeltagere, der i forvejen er tilsluttet værdipapircentralen og typisk har haft bedre kendskab til lokale forhold i det konkrete land. Den generelle harmonisering mellem værdipapircentraler i EU har nu mindsket betydningen af lokale forhold.

33 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.

Aktier, investeringsbeviser og obligationer afviklet i ES-CPH pr. gennemsnitlig bankdag

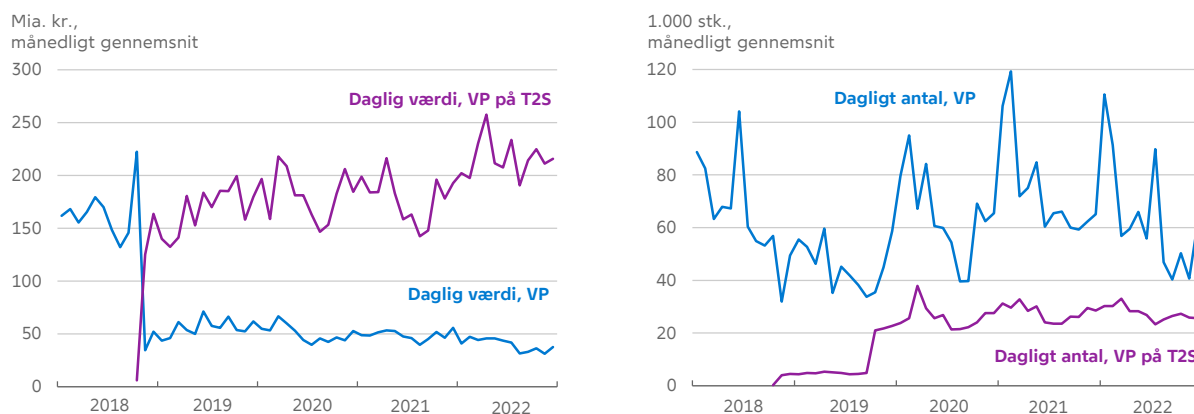
Tabel 3

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
2022	91,3	255,4	5,2	194,6	39,6	51,3	46,5	9,5

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 3



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.

Det skyldes særligt en stigning i værdien af obligationshandler på 31 mia. kr. pr. bankdag i gennemsnit. Mellem 2018 og 2021 steg markedsværdien af værdipapirer opbevaret i ES-CPH med næsten 50 procent, jf. figur 4. Det skyldtes primært, at værdien af dansk udstedte aktier blev næsten fordoblet i den periode. I 2022 skete et mindre fald i markedsværdien af de opbevarede værdipapirer, hvilket på tilsvarende vis skyldtes de generelle kursfald i dansk udstedte værdipapirer i 2022.

Driftsstabilitet

Driftsstabiliteten i afviklingen af danske værdipapirer i ES-CPH-afviklingen har i 2022 været tilfredsstillende og uden større hændelser. Der har i løbet af året været enkelte mindre hændelser, der ikke i større omfang har påvirket driften af ES-CPH-afviklingen.

I T2S forårsagede indførelsen af det nye fælleseuropæiske sanktionssystem³⁴ i februar 2022 en række udfordringer og mindre hændelser i systemet. Det medførte en lavere driftsstabilitet i ES-CPH's afvikling på T2S i februar og marts 2022. Problemerne blev løst, og driftsstabiliteten var normaliseret resten af året.

Afviklingsprocent

Afviklingsprocenten måler andelen af handelsomsætningen, der afvikles rettidigt.

Ifølge CSDR, artikel 5, skal værdipapirer afvikles to dage efter, at handlerne er indgået.

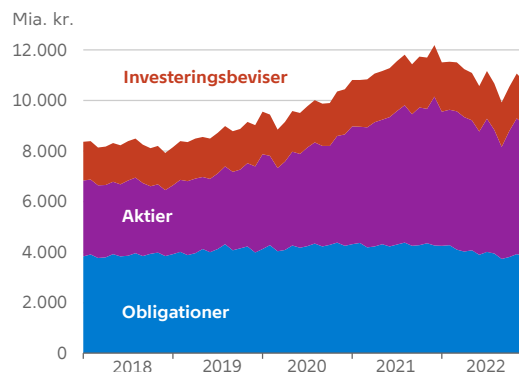
Figur 5 viser afviklingsprocenten for hhv. ES-CPH's eget system og for ES-CPH's afvikling på T2S. Det er i den forbindelse positivt, at der generelt har været en tendens til en forbedring af afviklingsprocenten i løbet af 2022, både i den lokale ES-CPH-afvikling og på T2S.

Internationale standarder

Nationalbanken overvåger, at afviklingen af danske værdipapirer i ES-CPH og T2S lever op til internationale standarder for finansielle markedsinfrastrukturer som bl.a. værdipapirafviklingssystemer.

Markedsværdi af værdipapirer opbevaret i ES-CPH

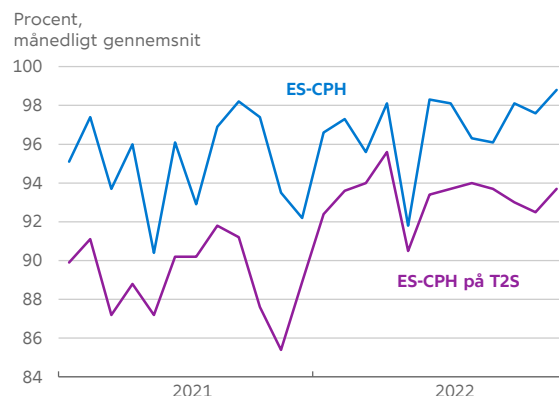
Figur 4



Kilde: ES-CPH.

Afviklingsprocent

Figur 5



Anm.: I figuren er afviklingsprocenten opgjort for antal transaktioner (handelsvolumen). Grundet databrud er data ikke tilgængelige længere tilbage end 2021.

Kilde: ES-CPH.

³⁴ Hvis en deltagers handler ikke afvikles rettidigt, kan det give problemer for deltagerens modparter, der på grund af de faldne handler måske ikke kan opfylde andre forpligtelser. I februar 2022 blev der derfor indført et nyt fælleseuropæisk sanktionssystem som en del af CSDR. Systemet skal sanktionere deltagere, hvis handler ikke kan afvikles rettidigt som følge af manglende værdipapirer eller likviditet.

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

Nationalbankens overvågning af ES-CPH koordineres med Finanstilsynet, der fører tilsyn med, at kravene i fælles EU-lovgivning, herunder CSDR, efterleves. I det omfang, der er overlap mellem overvågningsstandarder og lovkrav, inddrages dokumentation fra Finanstilsynet om efterlevelsen af lovkrav i Nationalbankens overvågning.³⁵

Cyberrobusthed

Nationalbanken færdiggjorde i 2020 en vurdering af ES-CPH's efterlevelse af CPMI-IOSCO's retningslinjer for cyberrobusthed. Vurderingen viser, at ES-CPH har en høj modenhed og efterlever cyber guidance på de fleste områder. Der er dog også få men centrale områder, hvor ES-CPH ikke fuldt ud efterlever de internationale retningslinjer. ES-CPH har i 2022 arbejdet videre med de af Nationalbankens anbefalinger, der fortsat er åbne.

ES-CPH modtog i november 2022 påbud fra Finanstilsynet i forbindelse med en it-inspektion gennemført i foråret 2022. Nationalbanken deltog i inspektionen som observatør. Ifølge Finanstilsynets påbud skal ES-CPH sikre en bedre metode for vedligeholdelse af it-beredskabet, samt at it-beredskabet understøttes af forretningsgange. Finanstilsynet gav derudover påbud for at sikre, at ES-CPH styrker sine processer og metode til styring af sit it-beredskab og sikrer en tydelig sammenhæng på tværs af beredskabsplanlægningen og -rapporteringen.

Nationalbanken forventer, at ES-CPH's arbejde med at efterleve Finanstilsynets påbud også vil medvirke til at efterleve Nationalbankens anbefalinger efter CPMI-IOSCO's cyber guidance.

Nationalbanken og Finanstilsynet koordinerer ES-CPH's opfølgning på de udstedte påbud og anbefalinger.

Systemændringer

Efter tilslutningen af danske kroner til T2S i oktober 2018 afvikles en stigende del af handler med dansk udstedte værdipapirer på T2S (se figur 3).

På den baggrund har ES-CPH valgt at udfase afviklingen af handler i danske kroner og euro fra ES-CPH-afviklingen. Det betyder, at fra udgangen af 2024 vil alle handler i danske kroner og euro blive afviklet på T2S. Afvikling af værdipapirhandel via den lokale ES-CPH-afvikling vil derefter kun finde sted i svenske kroner eller som såkaldte Free-of-Payment-handler (FoP)³⁶.

Samtidig udfases den såkaldte sikkerhedsret, der anvendes til sikkerhedsstillelse for intradagkredit i Kronos2.³⁷ Ændringen er bl.a. muliggjort af, at delta-gernes behov for sikkerhedsstillelse til afvikling på T2S i dag dækkes af auto-collateralisation, hvor T2S håndterer sikkerhedsstillelse for afviklingskredit.

35 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.

36 Ved Free-of-Payment-handler udveksles kun værdipapiret mellem sælger og køber, og der er ikke penge involveret i afviklingen af handlen. Er handlen indgået mellem en kunde og kundens egen bank, kan den dog fortsat godt gennemføres samtidig med udveksling af penge (såkaldt Delivery-versus-Payment, DvP), da pengebetonet, der udveksles internt i banken, ikke vil kræve pengeafvikling i Kronos2.

37 Under sikkerhedsretten stiller en deltager i Kronos2 sikkerhed i værdipapirer i et eller flere udpegede værdipapirdepoter i ES-CPH. Sikkerhedsretten binder i modsætning til traditionel pant ikke bestemte aktiver i et sikkerhedsdepot.

Betalinger og værdipapirafvikling i euro

TARGET Services bruges af de danske banker til at afvikle betalinger og værdipapirhandler i euro. TARGET Services består af T2 (tidligere TARGET2)³⁸, TARGET Instant Payments Service (TIPS) og TARGET2Securities (T2S). Systemerne ejes af Den Europæiske Centralbank, ECB, og de nationale centralbanker i Eurozonen og drives af 4CB (de fire centralbanker i Tyskland, Frankrig, Italien og Spanien) med ECB som koordinator.

T2 er det fælleseuropæiske RTGS-system, der bruges til afvikling af store tidskritiske betalinger i euro. I T2 kan deltagere derudover overføre likviditet til brug for afvikling i andre eurosystemer, herunder T2S. T2S er det fælleseuropæiske system til afvikling af værdipapirhandler i euro og danske kroner.³⁹ TIPS anvendes til at gennemføre straksbetalinger i euro.⁴⁰

Overvågningen af TARGET Services sker i samarbejde med ECB og de øvrige centralbanker, der er tilsluttet T2 eller T2S. Nationalbanken deltager i den fælles overvågning, som ledes af ECB og foregår i arbejdsgrupper med deltagelse af de nationale centralbanker.

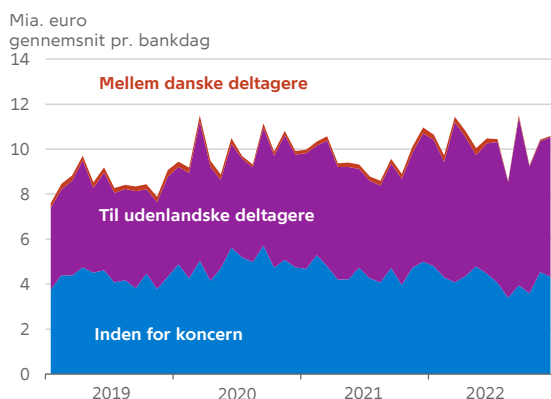
Brug

Der er 21 danske deltagere i T2. I 2022 gennemførte de interbankbetalinger for i gennemsnit 10,2 mia. euro om dagen. De danske deltagere bruger hovedsageligt T2 til at gennemføre koncerninterne betalinger og betalinger til udenlandske deltagere, jf. figur 6. Der udveksles flest euro med deltagere i Finland, Tyskland, Frankrig og Belgien.

Der er i alt 19 værdipapircentraler med aktiviteter i 20 EU-lande tilsluttet T2S, herunder ES-CPH. En bank kan afvikle værdipapirhandler på T2S, enten som direkte deltager, hvis banken har en såkaldt T2S-afviklingskonto, eller som indirekte deltager via en direkte deltagers adgang.

Interbankbetalinger i T2

Figur 6



Anm.: Figuren angiver betalinger afsendt af danske deltagere igennem TARGET2. Gennemsnit pr. dag er beregnet på månedsbasis.

Kilde: Danmarks Nationalbank.

En T2S-afviklingskonto oprettes via en af centralbankerne i EU, herunder Nationalbanken. 11 danske deltagere har en T2S-afviklingskonto via Nationalbanken til betaling eller modtagelse af euro i forbindelse med T2S-afviklingen. Andre danske deltagere kan have oprettet en T2S-afviklingskonto via andre EU-centralbanker.⁴¹

Driftsstabilitet

Driftsstabiliteten i de lokale komponenter af T2, som Nationalbanken har ansvaret for, har været tilfredsstillende i 2022.

Som beskrevet i afsnittet om værdipapirafvikling påvirkede idriftsættelsen af et nyt sanktionssystem i T2S dog driftsstabiliteten i systemet i februar og marts 2022. ECB's overvågning har sammen med de nationale centralbanker fulgt op på problemerne.

38 TARGET2 blev i marts 2023 erstattet af det nye RTGS-system, T2, som del af konsolideringen i TARGET Services (se nærmere beskrivelse under 'Systemændringer').

39 T2S kan håndtere flere valutaer. Ud over euro er danske kroner den eneste anden valuta tilsluttet til T2S. Læs om afvikling af værdipapirhandler i danske kroner i afsnittet Værdipapirafvikling.

40 Ingen banker i Danmark anvender på nuværende tidspunkt TIPS.

41 Da der ikke kan placeres euro permanent på T2S-afviklingskontoen, skal bankerne også have adgang til en T2-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 T2-konto i en centralbank i euroområdet.

Tilbage i 2020 var der fem alvorlige it-relaterede hændelser (ikke cyber-hændelser), der påvirkede afviklingen af betalinger og værdipapirhandler i T2 og T2S. Som opfølgning på hændelserne bestilte ECB en ekstern undersøgelse hos Deloitte, ligesom ECB's overvågning og interne revision fulgte op på hændelserne. Det resulterede i anbefalinger til, hvordan ECB kan styrke risikostyringsarbejdet på flere områder, herunder ændringsstyring, forretningsvireførelse, governance mfl.⁴² ECB udarbejdede på den baggrund en handlingsplan med en længere række tiltag⁴³. I 2021 og 2022 har ECB igangsat og implementeret tiltag, der skal imødekomme de fleste af anbefalingerne. Hovedparten af tiltagene i handlingsplanen er gennemført, og ECB forventer, at arbejdet med handlingsplanen er endeligt afsluttet i løbet af 2023. Nationalbanken deltager i ECB's opfølgning på handlingsplanen i regi af den fælles overvågning af TARGET Services, jf. nedenfor.

Internationale standarder

ECB afsluttede i starten af 2022 en vurdering af T2S efter Cyber Resilience Oversight Expectations, CROE, der er ECB's udmøntning af CPMI-IOSCO's Cyber Guidance. Nationalbanken har deltaget i arbejdet. Vurderingen har ført til en række anbefalinger, som T2S nu arbejder på at følge.

Systemændringer

ECB igangsatte i 2016 en større modernisering af den europæiske betalingsinfrastruktur og har siden arbejdet på en konsolidering af T2, T2S og TIPS på én it-plattform. Formålet er at imødekomme nye markedskrav og optimere deltagernes likviditetsstyring på tværs af alle TARGET Services.

Konsolideringen var planlagt til at blive lanceret 21. november 2022, men blev udskudt til 20. marts 2023. Ustabilitet i systemet og midlertidig manglende tilgængelighed til testmiljøet gjorde, at alle deltagere ikke havde testet det nye system tilstrækkeligt, før den planlagte lancering i november 2022. Lanceringen blev derfor udskudt. Den 20. marts 2023 migrerede alle centralbanker og deltagere planmæssigt over på den konsoliderede platform, TARGET Services.

42 Jf. ECB, ECB publishes an independent review of TARGET incidents in 2020, *pressemeddelelse*, 28. juli 2021 (*link*).

43 Handlingsplanen har haft et bredt sigte og dækker tiltag inden for change and release management, business continuity management, fail-over and recovery tests, communication protocols, governance og data centre and IT operations.

Valutahandelsafvikling

Globalt er valutamarkedet det største af alle finansielle markeder i verden målt på omsætning. Valutahandler i danske kroner kan enten afvikles via korrespondentbanker eller gennem det internationale valutahandelsafviklingsystem, CLS.

En valutahandel består af to modsatrettede betalinger i to forskellige valutaer. Hvis de to betalinger ikke gennemføres samtidig, påføres parterne i handlen en afviklingsrisiko. Afviklingsrisikoen er risikoen for, at én part i en valutahandel betaler som aftalt, men ikke modtager den købte valuta, hvilket kan resultere i betydelige tab og potentielt føre til systemiske konsekvenser.

Ved afvikling gennem korrespondentbanker afvikles de to betalinger i en valutahandel ikke samtidigt, hvilket udsætter parterne i handlen for afviklingsrisiko. Hvis betalinger i forskellige valutaer skal udveksles på tværs af tidszoner, kan betalingerne være mange timer eller dage undervejs, hvilket medfører en betydelig afviklingsrisiko.

Afviklingsrisikoen kan reduceres ved at afvikle begge sider af en valutahandel samtidigt⁴⁴ (Payment-versus-Payment, PVP), hvilket bl.a. er muligt i CLS. CLS afvikler valutahandler i p.t. 18 tilsluttede valutaer, herunder danske kroner, euro og US dollar. Kun valutahandler, hvor begge valutaer i handlen er tilsluttet CLS, kan afvikles i CLS. Hver dag afvikles der samlet set i gennemsnit valutahandler for over 6 billioner US dollar i CLS.

Afviklingsrisikoen kan også reduceres ved bilateral netting af indbyrdes betalingsforpligtelser inden afvikling. CLS tilbyder en bilateral nettingberegningsservice i 120 valutaer, som giver brugerne en samlet oversigt over deres nettobetalingsforpligtelser. Netting reducerer afviklingsrisikoen ved valutahandler, da netting reducerer de beløb, som skal udveksles mellem parterne i valutahandler.

⁴⁴ Jf. FX settlement risk: an unsettled issue, *BIS Quarterly Review*, december 2022 ([link](#)).

Overvågning af CLS

Boks 5

Overvågningen af CLS foregår i en fælles overvågningskomite, CLS Oversight Committee¹, der er et forum for samarbejde mellem de tilsluttede valutaer centralbanker, som derigennem kan varetage deres nationale overvågningsforpligtelse. Nationalbanken deltager i samarbejdet, der ledes af den amerikanske centralbank, Federal Reserve, FED, som også er tilsynsmyndighed for CLS. Nationalbankens overvågning har fokus på forhold, der har betydning for afviklingen af handler i danske kroner.

Overvågningen af CLS tager udgangspunkt i CPMI-IOSCO's principper for sikre og effektive betalings-systemer (Principles for Financial Market Infrastructures, PFMI). CLS offentliggjorde senest i september 2022 en beskrivelse af, hvordan systemet efterlever CPMI-IOSCO's principper.²

1. Federal Reserve System, Protocol for the Cooperative Oversight Arrangement of CLS ([link](#)).
2. CLS, Principles for Financial Market Infrastructures (PFMI) Disclosure, 2022 ([link](#)).

Nationalbanken deltager sammen med centralbanker for de øvrige tilsluttede valutaer i en fælles overvågning af CLS, jf. boks 5.

Brug

Danske kroner er den 20. mest omsatte valuta i verden. Den globale handel med danske kroner er steget med over en tredjedel de seneste tre år og udgjorde i april 2022 i gennemsnit 378 mia. kr. pr. bankdag. Stigningen skyldes bl.a. øget volatilitet på de finansielle markeder, bl.a. i forbindelse med corona-epidemien og krigen i Ukraine.⁴⁵

For danske kroner gælder det, at ca. 90 procent af alle valutahandler med danske kroner som det ene ben i valutahandlen, afvikles i CLS.⁴⁶ Den gennemsnitlige daglige værdi af handler i danske kroner i

⁴⁵ Jf. Danmarks Nationalbank, Undersøgelse af valuta- og derivatmarkedet, 2022, *Statistik – indsiget*, 12. december 2022 ([link](#)).

⁴⁶ Anslået på baggrund af BIS Triennial Central Bank Survey 2022, OTC foreign exchange turnover in April 2022, Bank for International Settlements, oktober 2022 ([link](#)) og data fra CLS Bank.

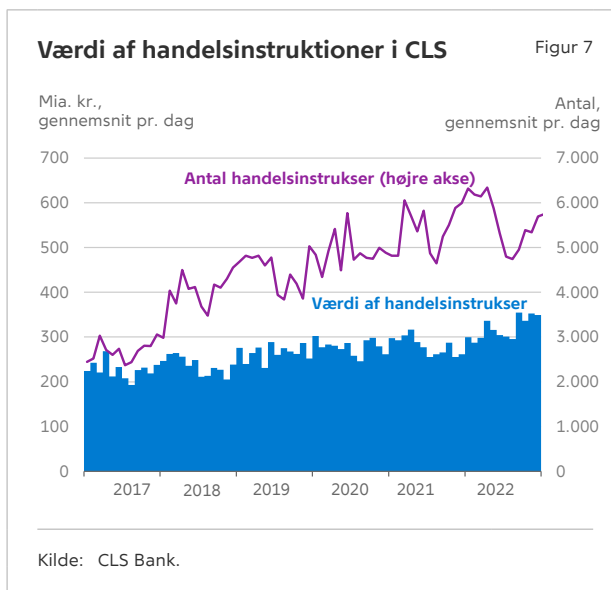
CLS var på 319 mia. kr. i 2022. Det er en stigning på 14 pct. i forhold til 2021, jf. figur 7.

Både danske banker og erhvervsvirksomheder kan afvikle valutahandler via CLS. Der er én dansk bank, som deltager direkte i CLS-afviklingen. Hvis man ikke selv er direkte deltager, kan man afvikle via en af de inden- og udenlandske deltagere, der tilbyder indirekte deltagelse til det danske marked. Det er der en række danske banker og virksomheder, der benytter sig af.

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 de tilsluttede centralbankers RTGS-systemer, dvs. for danske kroner via Kronos2. Driftsstabiliteten i CLS er derfor afhængig af stabiliteten i de tilsluttede RTGS-systemer. Som følge af de gensidige afhængigheder mellem CLS og RTGS-systemerne for de 18 tilknyttede valutaer kan en hændelse i ét RTGS-system forplante sig til andre systemer.

I 2022 var der ingen hændelser i Kronos2, som påvirkede CLS-afviklingen, og de danske deltagere reserverede tilstrækkelig likviditet til CLS-afviklingen. Til gengæld fik en hændelse i en anden centralbanks RTGS-system i ét tilfælde konsekvenser for afviklingen i danske kroner, idet der opstod problemer med udbetalinger fra CLS. Som konsekvens heraf måtte lukningen af det pengepolitiske døgn i Danmark udskydes. Se også afsnittet 'Interbankbetalinger og den centrale afvikling af betalinger i danske kroner' på side 7.



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
31. marts 2023



**DANMARKS
NATIONALBANK**

KONTAKT

Teis Hald Jensen
Kommunikations-
og presserådgiver

tehj@nationalbanken.dk
+45 3363 6066

SEKRETARIAT
OG KOMMUNIKATION