DANMARKS NATIONALBANK

RAPPORT | Overvågning af den finansielle infrastruktur
1. maj 2025 | Nr. 3

Overvågning af den finansielle infrastruktur 2024

Nationalbanken overvåger de systemer og løsninger i den danske finansielle infrastruktur, som gør det muligt for borgere og virksomheder at udveksle betalinger og værdipapirer. I denne rapport præsenterer Nationalbanken konklusionerne fra overvågningsarbejdet i 2024.

Skrevet af

Lone Natorp
Chef for overvågningen

ln@nationalbanken.dk
+45 3363 6161

Anne Hye Hedemann
Overvåger af Kronos2

anhk@nationalbanken.dk
+45 3363 6262

Jonas Moltke-Aaen
Overvåger af betalingsløsninger og værdipapircentraler

jmaa@nationalbanken.dk
+45 2191 7443

Line Bolding Holmegaard
Overvåger af detailbetalingssystemer

lbh@nationalbanken.dk
+45 3363 6087

36 sider

Danmark har en sikker, effektiv og stabil betalingsinfrastruktur

Forstyrrelser i udveksling af betalinger og afvikling af værdipapirhandler i Danmark er sjældne. De centrale systemer og løsninger i infrastrukturen efterlever i høj grad de krav, som internationale standarder stiller til bl.a. organisering, risikostyring og beredskab.

Systemejerne arbejder løbende med at beskytte sig mod cyberangreb

Systemejerne har generelt en høj modenhed i arbejdet med cyberrobusthed. Udviklingen i trusselsbilledet betyder imidlertid, at der løbende er behov for at tilpasse og styrke robustheden.

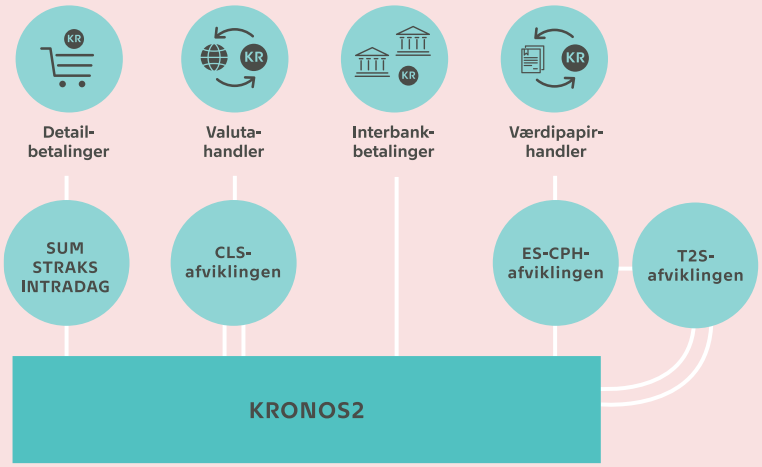
Infrastrukturen skal forberede sig på ekstreme scenarier

Det er ikke muligt at beskytte sig fuldt ud mod cyberangreb. Derfor anbefaler Nationalbanken, at systemejerne forbereder sig på at kunne håndtere ekstreme men plausible scenarier, herunder at de er i stand til at genoprette driften hurtigt og sikkert også efter en ekstrem situation.

Hvorfor er det vigtigt?

I 2024 blev der på en gennemsnitlig bankdag sendt betalinger for 732 mia. kr. gennem de systemer, der udgør den danske betalingsinfrastruktur, og det er helt afgørende for samfundsøkonomien, at betalinger og værdipapirer kan udveksles uden problemer. Derfor overvåger Nationalbanken, at de centrale systemer og løsninger i betalingsinfrastrukturen fungerer sikkert og effektivt og lever op til de internationale standarder på området. Det er med til at opfylde ét af Nationalbankens hovedformål, som er at bidrage til sikre og effektive betalinger.

Hovedfigur: Nationalbanken overvåger de centrale systemer og løsninger i betalingsinfrastrukturen



Emner

Overvågning af den finansielle infrastruktur | Overvågning | Cybersikkerhed | Finansiel stabilitet

01
Sammenfatning og vurdering

Betalingsinfrastrukturen i Danmark består af en række forbundne systemer og løsninger, der gør det muligt for borgere, virksomheder og finansielle aktører at udveksle betalinger og værdipapirer med hinanden. Hver dag bliver der sendt betalinger for 732 mia. kr. gennem betalingsinfrastrukturen, og det er afgørende for samfundsøkonomien, at systemerne og løsningerne fungerer uden forstyrrelser og nedbrud, så det er nemt og effektivt at betale for varer og tjenester.

Nationalbanken overvåger, at de centrale systemer og løsninger i betalingsinfrastrukturen er velfungerende, sikre og effektive. Som led i denne opgave gennemfører Nationalbanken vurderinger af, om de overvågede systemer og løsninger efterlever internationale standarders høje krav til sikkerhed og effektivitet, herunder krav til cyberrobusthed. Nationalbanken anbefaler ændringer til systemerne og løsningerne, hvis dette ikke er tilfældet. Nationalbankens overvågning er nærmere beskrevet i boks 1.

BOKS 1

Nationalbankens overvågning i 2024

Nationalbanken overvåger de centrale systemer og løsninger i den danske betalingsinfrastruktur:

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

Nationalbankens overvågning sker med udgangspunkt i internationale standarder og retningslinjer, der stiller krav til sikkerhed og effektivitet. Nationalbanken overvåger de centrale danske betalings- og afviklingssystemer med udgangspunkt i CPMI-IOSCO's[1] *Principles for financial market infrastructures*, PFMI[2], og PFMI's supplerende retningslinjer for cyberrobusthed, *Guidance on cyber resilience for market infrastructures*[3]. Nationalbankens overvågning inddrager også ECB's *Cyber resilience oversight expectations*[4], CROE, der udmønter PFMI's retningslinjer for cyberrobusthed i ECB's overvågningsarbejde. Overvågningen af de vigtigste danske betalingsløsninger sker med udgangspunkt i ECB's rammer for overvågning af betalingsløsninger, PISA[5]. Tilrettelæggelsen af overvågningen er nærmere beskrevet i Nationalbankens overvågningspolitik[6].

Nationalbanken koordinerer med Finanstilsynet på området. Samarbejdet skal sikre, at man undgår dobbelt myndighedskontrol, udnytter kompetencerne i de respektive myndigheder og sikrer deling af relevant information.

Nationalbanken samarbejder med andre centralbanker om overvågningen af de internationale systemer, der har relevans i Danmark.

[1] Committee on Payment and Market Infrastructures, CPMI, er en komité, som er knyttet til Bank for International Settlements, BIS. International Organization of Securities Commissions, IOSCO, er et internationalt samarbejde mellem myndigheder, der fører tilsyn med værdipapirmarkeder.
[2] Se CPMI-IOSCO, *Principles for financial market infrastructures*, 2012 *(link)*.
[3] Se CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, 2016 (*link*).
[4] Se ECB, *Cyber resilience oversight expectations for financial market infrastructures*, 2018 (*link*).
[5] Se ECB, *The Eurosystem Oversight Framework for Payment Instruments, Schemes and Arrangements, PISA*, 2021 (*link*).
[6] Se nationalbanken.dk, *Overvågningspolitik*, 2024 (*link*).

Den danske betalingsinfrastruktur er beskrevet i boks 2. Her beskrives også de ændringer, der er sket i infrastrukturen, i forbindelse med at Nationalbanken i påsken 2025 flyttede afviklingen af danske kroner til den fælleseuropæiske betalings- og værdipapirafviklingsplatform TARGET Services.

BOKS 2

Betalingsinfrastrukturen i Danmark

Hver bankdag[1] i 2024 blev der i gennemsnit sendt betalinger for 732 mia. kr. gennem den danske betalingsinfrastruktur, svarende til omkring en fjerdedel af BNP.

Nationalbankens betalingssystem 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. Nationalbanken har i påsken 2025 flyttet afviklingen af danske kroner fra Nationalbankens eget afviklingssystem, Kronos2, til den fælleseuropæiske platform for afvikling af betalinger og værdipapirhandler, TARGET Services[2].

TARGET Services, der ejes af den Europæiske Centralbank, ECB, og de nationale centralbanker i Euroområdet, består af tre services:

- T2 (tidligere TARGET2), som er et betalingssystem til store tidskritiske betalinger mellem deltagerne og afvikling af nettopositioner fra tilsluttede betalings- og afviklingssystemer
- T2S (TARGET2-Securities), som er systemet til værdipapirafvikling
- TIPS (TARGET Instant Payment Settlement), som bruges til straksbetalinger.

Danmark har sin egen pengepolitik og sikkerhedsstillelse, som fortsat håndteres i Nationalbankens system for sikkerhedsstillelse og pengepolitiske instrumenter, SPI. Den samlede betegnelse for den nye betalingsinfrastruktur, som både omfatter TARGET Services og SPI, er TARGET DKK. Nationalbanken er systemejer for TARGET DKK og har indgået aftale med ECB om brugen af TARGET Services. Den danske betalingsinfrastruktur, som den så ud i 2024, er vist i figur A, mens betalingsinfrastrukturen, som den ser ud efter påsken 2025, er vist i figur B.

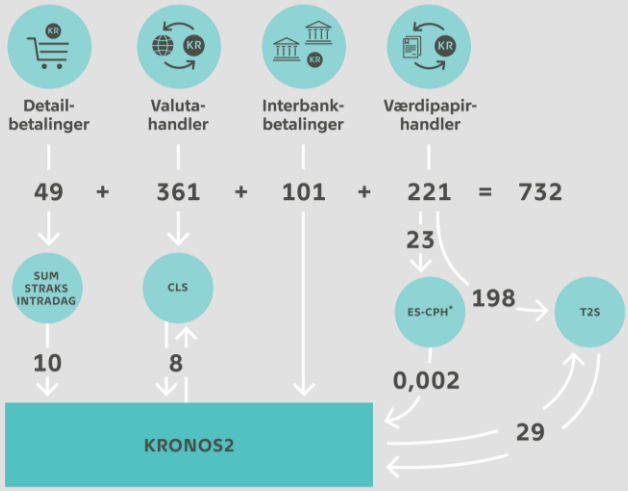
Detailbetalinger er betalinger mellem borgere, virksomheder og offentlige myndigheder, med fx betalingskort og konto-til-konto-overførsler. Betalingerne bliver afhængigt af type opgjort og afstemt i et af den finansielle sektors detailbetalingssystemer. Afviklingen sker efterfølgende på deltagernes konti i Nationalbanken. Før påsken 2025 blev betalingerne opgjort og afstemt i Sum-, Intradag- og Straksclearingen (Detailclearingene), der ejes af Finans Danmark, og efterfølgende afviklet i Kronos2. Efter påsken 2025 afvikles nettopositioner fra Sum- og Intradagclearingen nu i TARGET DKK via T2. Straksbetalinger afvikles efter påsken 2025 gennem TIPS. I TIPS bliver alle straksbetalinger afviklet enkeltvist og i realtid. Nationalbanken er systemejer for TIPS-DKK. TIPS-DKK har erstattet Straksclearingen, der nu er lukket.

Værdipapirhandler kan indgås på forskellige måder: På børsen, gennem en multilateral handelsplatform eller bilaterale handler via en bank eller fondsmægler (også kaldet "over-the-counter"). Afviklingen af handler med dansk udstedte værdipapirer håndteres af værdipapircentralen Euronext Securities Copenhagen, ES-CPH. Værdipapirhandler mellem bankerne og deres egne kunder afvikles via ES-CPH's eget afviklingssystem, ES-CPH-afviklingen, mens værdipapirhandler mellem banker og andre finansielle institutioner afvikles via T2S. ES-CPH er som værdipapircentral ansvarlig for at føre løbende regnskab med beholdningerne af alle dansk udstedte værdipapirer på vegne af investorerne, og flytninger af værdipapirer på konti i T2S spejles efterfølgende på konti i ES-CPH's systemer. Afviklingen af værdipapirhandler er blevet gennemført i danske kroner på T2S via Kronos2 siden 2018. Overgangen til TARGET DKK har derfor kun medført mindre tilpasninger.

Fortsættes ...

FIGUR A

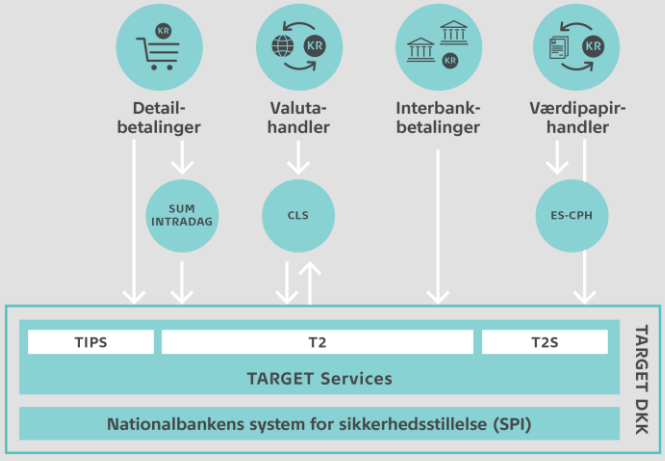
Betalingsflow, mia. kr., gennemsnit pr. bankdag i 2024



Anm.: *Hovedparten af handlerne i ES-CPH-afviklingen er transaktioner, hvor der ikke udveksles penge mellem parterne i Kronos2.
Kilde: Danmarks Nationalbank.

FIGUR B

Den danske betalingsinfrastruktur efter påsken 2025



Kilde: Danmarks Nationalbank.

... fortsat

Valutahandler afvikles gennem CLS, der er et internationalt system til afvikling af valutahandler i p.t. 18 tilsluttede valutaer, herunder danske kroner. 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. Før påsken 2025 reserverede deltagerne likviditet til afviklingen af valutahandler i CLS på konti i Kronos2. Efter påsken 2025 reserveres likviditeten i TARGET DKK via T2. CLS ejes af en række store internationale banker.

Netting har stor betydning for afviklingen af betalinger
De tre detailbetalingssystemer afviklede i 2024 deres deltageres nettopositioner på deltagernes konti i Kronos2. 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 49 mia. kr. til 10 mia. kr. dagligt, svarende til en reduktion på ca. 80 pct. På T2S sker afviklingen også ved brug af netting. Likviditeten til afviklingen på T2S overføres fra deltagernes pengekonti i Nationalbanken. Nettingen reducerer deltagernes behov for at reservere likviditet fra 198 mia. kr. til 29 mia. kr., hvilket svarer til en reduktion på ca. 85 pct.

[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.
[2] Se nationalbanken.dk, *Notat om TARGET DKK*, oktober 2024 (*link*).

Infrastrukturen er sikker, effektiv og stabil

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

De centrale systemer og løsninger i infrastrukturen efterlever i høj grad de krav, der stilles i internationale standarder til bl.a. organisering, risikostyring og beredskab. Ejerne af systemerne og løsningerne har generelt en høj modenhed i arbejdet med operationel stabilitet og cyberrobusthed. Udviklingen i trusselsbilledet betyder imidlertid, at der løbende er behov for at styrke robustheden, se nedenfor.

Driftsstabiliteten i infrastrukturen var i 2024 generelt høj, og der er sjældent forstyrrelser i udveksling af betalinger og afvikling af værdipapirhandler i Danmark. Der var i 2024 enkelte problemer med den rettidige afvikling af betalinger, og Nationalbankens overvågning har fulgt op over for ejerne af systemerne for at sikre, at opfølgningen på hændelserne er tilfredsstillende.[1]

Infrastrukturen var heller ikke påvirket i nævneværdig grad af CrowdStrike-hændelsen i juli 2024, der forårsagede systemnedbrud på ca. 8,5 millioner Windows-enheder på tværs af verden, herunder i finans-, luftfarts- og sundhedssektoren. Den kritiske drift af infrastrukturen er ikke afhængig af Windows-systemer, hvorfor hændelsen kun havde begrænset påvirkning her. Hændelsen skyldtes fejl i en opdatering af sikkerhedssoftware fra leverandøren CrowdStrike.

[1] Hændelserne og den efterfølgende opfølgning er nærmere beskrevet nedenfor i afsnittene om de respektive systemer.

Infrastrukturen arbejder løbende med at øge cyberrobustheden

Cybertruslen er fortsat høj og udvikler sig løbende. Trusselsbilledet er bl.a. påvirket af ændringerne i den geopolitiske situation og udviklingen af ny teknologi, fx kunstig intelligens. Dertil kommer, at hackere løbende bliver dygtigere og mere specialiserede. Center for Cybersikkerhed vurderer, at truslen mod finanssektoren og den finansielle infrastruktur er vedvarende.[2]

Truslen fra cyberangreb betyder, at ejerne af systemerne og løsningerne i infrastrukturen løbende skal arbejde med at styrke deres cyberrobusthed for at være på forkant med udviklingen, i takt med at trusselsbilledet ændres, og cyberkriminelle udvikler nye metoder.

De internationale standarder[3] på området stiller krav til arbejdet med cyberrobusthed på en række indsatsområder, se boks 3.

BOKS 3

Cyberrobustheden styrkes gennem en kontinuerlig og holistisk tilgang til styring af cyberrisci

Nationalbanken vurderer de centrale systemers robusthed med udgangspunkt i CPMI-IOSCO's *Guidance on cyber resilience for financial market infrastructures,* Cyber Guidance[1], og ECB's *Cyber resilience oversight expectation for financial market infrastructures*, CROE[2].

Standarderne stiller krav til systemernes arbejde med cyberrobusthed på følgende områder:

- **Governance**, der fastlægger rammer, roller og ansvar i forhold til cyberrobusthed
- **Identifikation** af kritiske forretningsaktiviteter, understøttende processer, procedurer og systemer samt risikovurderinger af disse
- **Beskyttelse** via effektive sikkerhedskontroller og procesdesign
- **Opdagelse** af cyberhændelser tidligt i forløbet gennem monitorering
- **Afværgelse** af angreb og **genopretning** af kritiske forretningsaktiviteter hurtigt og sikkert efter et alvorligt og omfattende nedbrud.

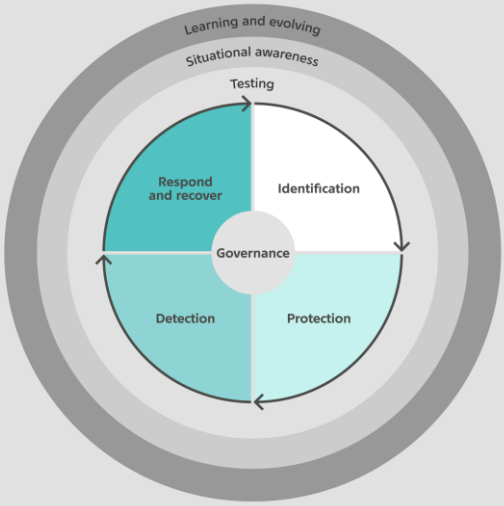
Dertil kommer også krav til arbejdet med tre tværgående elementer:

- **Test** på tværs af alle områder for at sikre arbejdets effektivitet
- **Opmærksomhed på situationsbilledet**, herunder efterretninger om cybertrusselslandskabet og sårbarheder
- **Læring og udvikling** for løbende at styrke cyberrobustheden, da trusselslandskabet også udvikler sig.

Det er vigtigt, at systemejerne løbende har fokus på alle områder, se figur, for at styrke cyberrobustheden.

FIGUR

De fem primære indsatsområder og de tre tværgående elementer i arbejdet med cyberrobusthed



Kilde: CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, Cyber Guidance.
ECB, *Cyber resilience oversight expectations for financial market infrastructures*, CROE.

[1] Se CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, 2016 (*link*).
[2] Se ECB, *Cyber resilience oversight expectations for financial market infrastructures*, 2018 (*link*).

I arbejdet med cyberrobusthed skal systemejerne som udgangspunkt *identificere* de kritiske forretningsprocesser og understøttende it-systemer. Disse skal *beskyttes* med effektive sikkerhedskontroller. De ansvarlige skal være i stand til at

[2] Se Center for Cybersikkerhed, *Cybertruslen mod finanssektoren*, 1. november 2024 (*link*).
[3] CPMI-IOSCO Cyber Guidance, CROE og PISA.

opdage, hvis der alligevel sker uberettiget adgang og påvirkning af systemerne. De skal være i stand til så vidt muligt at kunne *afværge* situationen og begrænse skaderne, og endelig skal de kunne *genoprette* den normale drift på sikker vis, hvis systemerne er blevet påvirket af et cyberangreb.

Arbejdet med cyberrobusthed skal dække alle disse områder, og det skal løbende *testes*, at tiltagene effektivt beskytter de kritiske it-systemer. Her skal systemejerne både teste evnen til at beskytte sig mod og afværge et angreb, og de skal teste evnen til sikkert at genoprette den normale drift efter et angreb og i videst muligt omfang videreføre de mest kritiske dele af driften, indtil genopretningen er gennemført.

Arbejdet med at beskytte sig mod cyberangreb bør indgå som en central del af organisationernes strategi, og arbejdet bør have et stort fokus hos ledelsen.

Nationalbankens overvågning viser, at ejerne af de centrale systemer og løsninger i betalingsinfrastrukturen generelt har en høj modenhed i arbejdet med cyberrobusthed og er godt rustede til at forebygge og beskytte sig mod cyberangreb. Selvom der løbende lægges en stor indsats i arbejdet med cybersikkerhed, er det imidlertid ikke muligt at beskytte sig fuldt ud. Det er derfor vigtigt, at systemejerne fortsætter arbejdet med at udvikle de beredskaber, der skal håndtere konsekvenserne af eventuelle angreb, der ikke har kunnet afværges.

Nationalbankens overvågning har løbende fokus på systemejernes arbejde med at styrke og tilpasse deres cyberrobusthed til udviklingen i trusselsbilledet. Nationalbanken anbefaler i den forbindelse bl.a. systemejerne at forberede sig på at kunne håndtere ekstreme men plausible cyberscenarier. Det indbefatter, at de er i stand til at genoprette driften hurtigt og sikkert – også efter en ekstrem situation, fx i en situation, hvor der er sket omfattende skadelig påvirkning af kritiske data.[4]

Nationalbanken har i 2024 desuden fulgt systemejernes arbejde med at efterleve DORA-forordningen og NIS2-direktivet[5], som bl.a. skal medvirke til at styrke leverandørstyringen og de beredskabsenheder, der skal håndtere konkrete cyberangreb.

Nationalbankens overvågning drøfter også konsekvenserne af den geopolitiske situation med systemejerne, herunder rækken af hændelser med brud på undersøiske kabler i bl.a. Østersøen. Nationalbanken har påpeget vigtigheden af, at systemejerne sikrer sig, at der er tilstrækkelig redundans i de kritiske kabelforbindelser, som systemerne anvender, og Nationalbanken følger løbende systemejernes arbejde med området.

Sektorsamarbejder leverer vigtige bidrag til at styrke cyberrobustheden

Systemerne i den finansielle infrastruktur er tæt forbundne, og det er vigtigt, at systemejerne koordinerer arbejdet med cyberrobusthed og deler erfaringer på

[4] Nationalbanken har udarbejdet vurderinger efter de internationale retningslinjer for cyberrobusthed af ES-CPH i 2020, Detailclearingerne i 2022 og af Dankort og Nationalbankens sikkerhedsstillelsessystem, Calypso, i 2024.
[5] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148. Directive on Security of Network and Information Systems, NIS2, finder anvendelse fra 18. oktober 2024.

området. Derfor deltager systemejerne sammen med andre dele af den finansielle sektor i en række sektorsamarbejder.

Finansielt Sektorforum for Operationel Robusthed, FSOR, er et offentlig-privat samarbejdsforum, hvis formål er at øge sektorens operationelle robusthed, herunder robustheden over for cyberangreb.[6] Ejerne af de centrale systemer og løsninger i infrastrukturen deltager i FSOR og bruger samarbejdet til at understøtte deres eget arbejde med cyberrobusthed. Det sker bl.a. via drøftelse af risici, videndeling, deltagelse i test af FSOR's kriseberedskab[7] og implementering af fælles mitigerende initiativer.

Risikoforum for Gensidige Afhængigheder, RGA[8], er et samarbejdsforum mellem de ansvarlige for de centrale systemer i infrastrukturen, hvis formål er at identificere og adressere operationelle risici, der går på tværs af systemerne. I 2024 har RGA fokuseret på at tilpasse arbejdet til de nye systemlandskaber efter overgangen til afvikling af betalinger i danske kroner på TARGET Services i påsken 2025, se boks 2. I 2023 afsluttede RGA arbejdet med fælles planer for kontrolleret nedlukning og genåbning i en række scenarier. Nationalbanken forventer, at systemejerne fortsætter deres eget arbejde med planer for kontrolleret nedlukning og test heraf i 2025. Ved at deltage i RGA efterlever systemejerne de internationale standarders anbefalinger om at styre risici fra gensidige afhængigheder.

De centrale systemer og løsninger i infrastrukturen deltager derudover alle i *Nordic Financial CERT*, NFCERT[9], der er et fællesnordisk sektorsamarbejde om indsamling og deling af information om cybertrusler og cyberangreb. Ved at deltage i NFCERT efterleves internationale standarders anbefalinger om at deltage i denne type tværgående informationsdeling.

Endelig deltager ejerne af systemer og løsninger i infrastrukturen alle i Nationalbankens TIBER[10]-DK-program. Nationalbanken har siden 2019 gennem TIBER-DK-programmet faciliteret og koordineret gennemførelsen af trusselsbaserede tests, hvor avancerede cyberangreb simuleres i faktiske produktionsmiljøer. Deltagerne i TIBER-DK deler desuden læring fra disse tests med hinanden for at styrke cyberrobustheden yderligere.

Internationalisering af infrastrukturen fortsætter

Gennem en årrække er den danske betalingsinfrastruktur blevet tættere integreret i den europæiske infrastruktur, og flere af ejerne af danske systemer og løsninger er blevet integreret i internationale koncerner. Denne tendens er fortsat i 2024 og starten af 2025.

[6] Nationalbanken varetager formandskab og sekretariat for FSOR, der ud over systemerne og løsningerne i infrastrukturen også har deltagelse af banker, datacentraler, pensions- og forsikringsselskaber samt relevante myndigheder og Nordic Financial CERT. Se FSOR's årsberetning for 2024 (*link*).
[7] FSOR's kriseberedskab er etableret med henblik på at koordinere indsatsen på tværs af den finansielle sektor i tilfælde af en krise, som kan true den finansielle stabilitet. FSOR's kriseberedskab supplerer medlemmernes egne kriseplaner og det nationale kriseberedskab, NOST.
[8] Risikoforum for Gensidige Afhængigheder er et samarbejdsforum mellem de organisationer, der er ansvarlige for de centrale betalings- og afviklingssystemer i infrastrukturen, dvs. Nationalbanken (interbankbetalinger), ES-CPH (værdipapirhandler), Finans Danmark (detailbetalinger) og e-nettet (kommunikationsnetværk). Arbejdet i RGA koordineres med FSOR.
[9] Nordic Financial CERT, NFCERT, er en medlemsdrevet nonprofit-organisation, der har til formål at styrke den nordiske finansindustris 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.
[10] Threat Intelligence-based Ethical Red Teaming.

Som beskrevet ovenfor er afviklingen af betalinger i danske kroner blevet flyttet fra Nationalbankens afviklingssystem, Kronos2, til det fælleseuropæiske system TARGET Services, se boks 2.

Finans Danmark har i 2024 underskrevet et såkaldt "Memorandum of Understanding" med EBA CLEARING, der foretager clearing af detailbetalinger i euro, om udvikling af en ny clearingløsning i danske kroner. Løsningen skal afløse den eksisterende Intradagclearing.[11] Dette er beskrevet nærmere i kapitel 4, *Clearing og afvikling af detailbetalinger*.

ES-CPH har fortsat arbejdet med at integrere sine systemer i Euronext-koncernen, og i 2024 begyndte ES-CPH at anvende Euronext-koncernens platform til håndtering af corporate actions, dvs. periodiske betalinger, emissioner, indfrielser mv. Målsætningen er, at de fire værdipapircentraler i Euronext-koncernen[12] på sigt alle skal anvende den samme tekniske platform til håndtering af værdipapirer. ES-CPH har i 2024 desuden fortsat arbejdet med at udfase den lokale afviklingsplatform, ES-CPH-afviklingen, sådan at al afvikling af værdipapirhandler i danske kroner fra september 2027 vil foregå på den fælleseuropæiske platform T2S. Dette er beskrevet nærmere i kapitel 5, *Værdipapirafvikling.*

Endelig har Nets, der driver Dankort, og MPS, der driver Betalingsservice, i 2024 fortsat deres integration i de internationale koncerner, de er en del af. Dette er bl.a. sket i forhold til risikostyring og beredskabsplanlægning. Dette er beskrevet nærmere i kapitel 3, *Detailbetalinger.*

[11] Se nærmere i kapital 4, *Clearing og afvikling af detailbetalinger*.
[12] Ud over ES-CPH indgår værdipapircentralerne i Italien, Norge og Portugal i Euronext-koncernen.

02

Interbankbetalinger og den centrale afvikling af betalinger i danske kroner

En interbankbetaling er en betaling mellem finansielle institutioner. Betalingerne er typisk karakteriseret ved at være tidskritiske og af høj værdi.

Interbankbetalinger i danske kroner blev i 2024 og indtil 16. april 2025 afviklet i Nationalbankens betalingssystem, Kronos2. Den centrale afvikling af kronebetalinger sker nu i TARGET DKK, se boks 2. TARGET DKK består af ECB´s systemer T2, T2S og TIPS (TARGET Services) samt af Nationalbankens eget system til sikkerhedsstillelse og pengepolitiske instrumenter, SPI.

Kronos2 var ligesom TARGET DKK et RTGS-system. RTGS står for *Real Time Gross Settlement*, hvilket betyder, at betalingerne afvikles enkeltvist og øjeblikkeligt.

Nationalbankens RTGS-system er et centralt omdrejningspunkt i den danske betalingsinfrastruktur, se boks 2. Ud over interbankbetalinger afvikles også pengepolitiske operationer og nettopositioner fra bl.a. Detailclearingerne, og der bliver overført likviditet til afvikling af værdipapirhandler og valutahandler, som foregår i andre systemer.

Hidtil har hovedsageligt banker kunnet deltage i afviklingen af betalinger i Nationalbankens afviklingssystem. Som følge af ændringer i EU-lovgivningen har betalingsinstitutter og e-pengeinstitutter siden april 2025 kunnet ansøge om at deltage i de centrale betalingssystemer, herunder i TARGET DKK.[13]

I de følgende afsnit beskrives brug og drift af Kronos2. Afsnittet om internationale standarder og arbejdet med cyberrobusthed omhandler også Kronos2, men arbejdet er samtidig relevant for Nationalbankens systemmæssige landskab efter overgangen til TARGET DKK.

Brug

De fleste danske banker og realkreditinstitutter har konto i Nationalbanken på samme måde, som privatpersoner har konto i en privat bank. Desuden deltager også filialer af udenlandske banker. I slutningen af 2024 var der 70 deltagere i betalingsafviklingen i Kronos2.

I 2024 blev der gennemført interbankbetalinger i Kronos2 for 100,9 mia. kr. i gennemsnit pr. bankdag. Det er en stigning på 5,4 pct. fra 2023, se tabel 1.

[13] I april 2025 trådte ændringer i det såkaldte finality-direktiv i kraft (Europa-Parlamentets og Rådets forordning (EU) 2024/886 af 13. marts 2024 om ændring af forordning (EU) nr. 260/2012 og (EU) 2021/1230 og direktiv 98/26/EF og (EU) 2015/2366 for så vidt angår strakskreditoverførsler i euro). Ændringerne gør det muligt for betalingsinstitutter (udbydere af betalingstjenester, der ikke er banker) og e-pengeinstitutter at deltage direkte i afviklingen af betalinger i de centrale betalingssystemer, herunder TARGET DKK, uden at skulle gå igennem en bank. Dog vil betalingsinstitutterne udelukkende have adgang til afviklingskonti i Nationalbanken og vil ikke få adgang til at anvende de pengepolitiske instrumenter.

TABEL 1

Transaktioner i Kronos2, gennemsnit pr. bankdag

Mia. kr., løbende priser	2020	2021	2022	2023	2024
Interbankbetalinger	**87,6**	**88,7**	**101,5**	**95,8**	**100,9**
- Heraf kundebetalinger	14,0	16,6	20,7	19,8	21,5
Pengepolitiske operationer	**34,4**	**6,0**	**0,3**	**0,01**	**0,0**
- Heraf salg af indskudsbeviser	33,2	5,5	0,5	0,01	0,0
- Heraf pengepolitiske udlån	1,3	0,5	0,3	0,0	0,0
Reservation af likviditet til afviklinger	**113,9**	**106,2**	**97,9**	**75,8**	**68,4**
- Heraf til Sum-, Intradag- og Straksclearingen	39,9	40,6	40,1	32,9	32,9
- Heraf til ES-CPH-afviklingen	41,2	38,3	35,2	21,2	13,5
- Heraf til CLS	32,8	27,2	22,5	21,7	22,0
Afviklede nettopositioner	**16,6**	**17,0**	**17,9**	**17,9**	**18,1**
- Heraf i Sum-, Intradag- og Straksclearingen	8,3	9,3	10,0	9,8	10,2
- Heraf i ES-CPH-afviklingen	0,9	0,8	0,2	0,01	0,002
- Heraf i CLS	7,3	6,8	7,7	8,1	7,9
Overførsler til T2S (reservation af likviditet til afviklinger)*	**22,2**	**22,2**	**18,6**	**18,0**	**29,4**

* Deltagernes overførsler fra Kronos2 til T2S sker med henblik på at reservere likviditet på konti i T2S til at kunne gennemføre afvikling af værdipapirhandel. Det 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 deltagernes konti i Kronos2.

Kilde: Danmarks Nationalbank.

Drift

I 2024 har driftsstabiliteten for Kronos2 været tilfredsstillende.

En enkelt hændelse i Kronos2 i oktober medførte, at deltagerne ikke havde adgang til systemet i kortere tidsrum. Den forretningsmæssige konsekvens af udfaldene var begrænset, men førte til en forsinkelse på ca. 15 minutter af den første natlige clearing af detailbetalinger. Dertil var risikoen, at hændelsen kunne have ført til forsinkelse i afviklingen af valutahandler på CLS. Årsagen til hændelsen i oktober skyldtes en systemfejl i et teknisk hjælpeværktøj, som efterfølgende blev afinstalleret.

I 2024 har der været flere hændelser i andre betalings- og afviklingssystemer, der har påvirket Kronos2 som følge af den gensidige afhængighed i betalingsinfrastrukturen:

I januar 2024 var der forsinkelser på T2S, der påvirkede afviklingen af danske kroner og førte til en udskydelse af lukningen af det pengepolitiske døgn. Årsagen til hændelsen på T2S var en systemopdatering, der indeholdt en fejl, der medførte, at en besked på T2S blokerede for gennemførelsen af andre beskeder i T2S. Den relevante del af systemopdateringen blev efterfølgende rullet tilbage.

Ved udgangen af 3. kvartal 2024 var Kronos2 påvirket af problemer hos ES-CPH. Hændelsen i ES-CPH førte til, at lukningen af det pengepolitiske døgn i Kronos2 blev udskudt, fordi afviklingen i T2S med danske kroner blev forsinket. Hændelsen var i første omgang forårsaget af en fejl i ES-CPH's corporate actions-system, se kapitel 5, *Værdipapirafvikling*.

I februar 2025 betød en større hændelse i TARGET Services, at T2 og T2S var utilgængelige i flere timer. Det medførte en udskydelse af lukningen af det pengepolitiske døgn i Kronos2 fra kl. 16.45 til 23.45, da døgnet ikke kunne lukkes, før likviditet fra T2S blev sendt tilbage til Kronos2. Se nærmere beskrivelse af hændelsen i kapitel 6, *Betalinger og værdipapirafvikling i euro*.

Likviditet

I 2024 har deltagerne fortsat haft rigelig likviditet til at gennemføre betalinger i Kronos2, både interbankbetalinger og de betalinger, der følger af afviklingsinstruktioner fra de tilsluttede betalings- og afviklingssystemer (Detailclearingerne, ES-CPH og CLS), se figur 1.

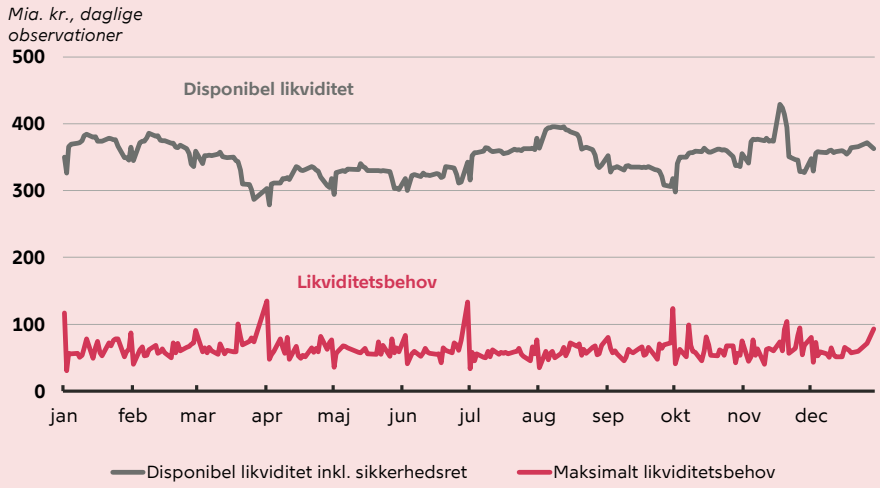
Nationalbanken har siden idriftsættelsen af Kronos2 i 2018 gennemført jævnlige stresstest af likviditeten i overensstemmelse med krav i CPMI-IOSCO's principper for finansielle markedsinfrastrukturer, PFMI.

Likviditetsstresstesten fra 2024 viste, at betalingsafviklingen generelt fremstår robust.[14] Stresstesten fandt enkelte dage med større likviditetseffekter i scenarier, hvor de største deltagere i systemet ikke kan afsende betalinger. Stresstesten viste dog samtidig, at de eksisterende nødprocedurer er effektive til at reducere negative likviditetseffekter af et operationelt nedbrud på 1-2 dage. Dertil viste stresstesten, at det øger robustheden, at TARGET DKK har en indbygget kø-funktionalitet. Det betyder, at betalinger ikke bliver afvist af systemet ved manglende likviditet, men afvikles, når der atter er likviditet til rådighed.

[14] Se nationalbanken.dk for en nærmere beskrivelse af resultaterne af likviditetsstresstesten (*link*).

FIGUR 1

Disponibel likviditet versus likviditetsbehov hos deltagerne i Kronos2 i 2024



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.

Cyberrobusthed

Nationalbanken arbejder løbende med at styrke cyberrobustheden i sine systemer og forretningsprocesser. Et vigtigt element i dette arbejde er at sikre, at Nationalbanken efterlever SWIFT's Customer Security Programme, CSP, som er obligatoriske sikkerhedskontroller, der har til formål at styrke robustheden i tilfælde af cyberangreb. I 2024 har arbejdet med efterlevelse af SWIFT's CSP både omfattet Kronos2 og Nationalbankens nye platform, som understøtter afviklingen af kroner på TARGET DKK.

Nationalbanken er i 2024 begyndt at anvende en ny testmetode, der har til formål at forbedre forsvaret mod cyberangreb. Testen bliver kaldt for purple teaming test, fordi den foregår i et samarbejde mellem på den ene side blue team, dvs. de medarbejdere, der til daglig arbejder med de kritiske systemer og holder øje med mistænkelig adfærd, og på den anden side red team, dvs. medarbejdere fra en ekstern virksomhed, som forsøger at kompromittere systemerne ved at simulere angreb, der efterligner realistiske cyberangreb. I testen trænes blue team i at opfange og stoppe ondsindede aktører, der er trængt ind i systemerne. Red team tester sikkerhedsforanstaltningerne i tæt dialog med blue team, og undervejs i testen deles læring om bl.a. identificerede svagheder eller områder med forbedringspotentialer, som skal udbedres for at styrke systemerne mod faktiske angreb. Eventuelle udbedringer foretages og gentestes så vidt muligt inden for testperioden. Purple teaming test vil løbende blive anvendt og er et supplement til Nationalbankens deltagelse i TIBER-DK-testprogrammet.

I det løbende arbejde med risikostyring har der været et stort fokus på styrkelse af beredskabsplaner. Arbejdet har bl.a. omfattet en gennemgang af Nationalbankens beredskabsfunktioner og -forpligtelser med henblik på at sikre

den nødvendige beredskabskapacitet ved kritiske hændelser. Derudover blev der i juni afholdt en test af FSOR's kriseberedskab, hvor hændelsesscenariet medførte, at både sektorens fælles beredskab og Nationalbankens interne kriseberedskab var aktiveret samtidigt. Gennemgangen af beredskabet og den gennemførte test imødekom et udestående forbedringspotentiale identificeret ved vurderingen af Kronos2's efterlevelse af PFMI[15] i 2021.

Internationale standarder

Nationalbankens overvågning har i 2024 færdiggjort en vurdering af Calypsos efterlevelse af CPMI-IOSCO's Cyber Guidance[16]. Calypso er Nationalbankens system for sikkerhedsstillelse og pengepolitiske instrumenter, SPI. Systemet er vigtigt for afviklingen i danske kroner og anvendes af deltagerne til at stille sikkerheder i form af værdipapirer for til gengæld at kunne få kredit, som de kan anvende til betalingsafviklingen. CPMI-IOSCO's Cyber Guidance beskriver de foranstaltninger, som systemisk vigtig betalingsinfrastruktur bør have på plads for at styrke sin robusthed i forhold til de risici, som cybertrusselslandskabet medfører.

Vurderingen pegede på enkelte områder med forbedringspotentiale. Nationalbanken skal bl.a. styrke arbejdet med beredskab for cyberhændelser, herunder evnen til at håndtere ekstreme men plausible scenarier.

Nationalbankens overvågning har vurderet bankens efterlevelse af CPMI's strategi for end point-sikkerhed. Strategien har til formål at reducere risikoen for kriminelle transaktioner i centrale betalingssystemer ved at rette fokus på sikkerheden omkring end points[17]. Som opfølgning på vurderingen er der lagt en plan for, hvornår Nationalbanken forventer at efterleve identificerede udeståender.

For fuldt ud at efterleve strategien skal der etableres en årlig proces, hvor Nationalbanken sammen med deltagerne analyserer risici relateret til end points og gennemgår beskyttende kontroller for på den måde bedre at kunne forstå og modgå risici i økosystemet omkring Nationalbankens RTGS-system. Desuden skal det fælles beredskab testes mod et svindelscenarie. Dele af strategien er blevet efterlevet, i forbindelse med at afviklingen af danske kroner er migreret til TARGET Services. I overensstemmelse med strategien stilles der i TARGET Services krav om, at alle deltagere skal have etableret generelle sikkerhedskontroller til bl.a. at modgå svindel eller svindelforsøg. Deltagerne skal herudover årligt dokumentere, at disse sikkerhedskontroller og foranstaltninger (end point-sikkerhed) er etableret og effektive.

[15] Se Danmarks Nationalbank, Vurdering af Kronos2, *Danmarks Nationalbank Rapport*, nr. 4, december 2021 (*link*).
[16] *CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures*.
[17] Et *end point* defineres i strategien som et punkt, hvor information om betalingsinstruktioner udveksles mellem to parter i økosystemet, fx mellem et betalingssystem og en deltager.

03
Detailbetalinger

Når borgere og virksomheder i Danmark køber varer og betaler regninger, bruger de som oftest Dankort, internationale betalingskort fra Visa og Mastercard, MobilePay, Betalingsservice og konto-til-konto-overførsel via netbank eller mobilbank. I 2024 blev der foretaget betalinger med disse og andre digitale betalingsløsninger for 33,4 mia. kr. i gennemsnit pr. dag.

Nationalbanken overvåger Dankort og Betalingsservice. Konto-til-konto-overførsler overvåges som led i Nationalbankens overvågning af Detailclearingerne. Visa og Mastercard overvåges af Eurosystemet. Overvågningen er baseret på PISA-standarderne, se boks 4. 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.

BOKS 4

Betalingsløsninger overvåges efter PISA-standarderne

Nationalbanken baserer overvågningen af betalingsløsninger på ECB's standarder for betalingsløsninger[1], PISA, der blev offentliggjort i 2022.

PISA viderefører de centrale dele af ECB's tidligere standarder for betalingsløsninger, men på nogle områder er PISA mere eksplicit i de krav, der stilles, særligt i forhold til risikostyring og cybersikkerhed og -beredskab. PISA er baseret på PFMI men med tilpasninger, der skal sikre, at standarderne er relevante for betalingsløsninger.

[1] Se ECB's standarder for betalingsløsninger, *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements, PISA* (*link*).

Dankort

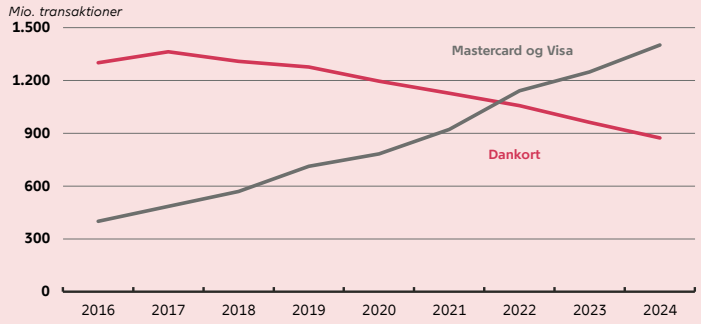
Nationalbankens overvågning af Dankort er rettet mod Nets, der er systemejer for Dankort.

Siden 2017 er der sket et væsentligt fald i anvendelsen af Dankort. Faldet i brugen af Dankort skyldes især øget anvendelse af Visa og Mastercard, se figur 2 og figur 3. Dankort spiller dog stadig en central rolle for danske detailbetalinger.

FIGUR 2

Brugen af Dankort og internationale kort i Danmark (antal)

Samlet antal transaktioner foretaget med betalingskort i Danmark

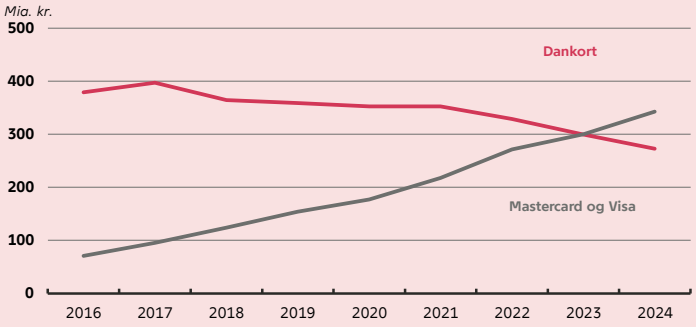


Anm.: Opgørelsen dækker kortbetalinger i fysisk handel, på internettet og selvbetjeningsmiljøer i Danmark.
Kilde: Nets og Danmarks Nationalbank.

FIGUR 3

Brugen af Dankort og internationale kort i Danmark (værdi)

Samlet værdi betalt med betalingskort i Danmark



Anm.: Opgørelsen dækker kortbetalinger i fysisk handel, på internettet og selvbetjeningsmiljøer i Danmark.
Kilde: Nets og Danmarks Nationalbank.

Udviklingen i kortanvendelsen er bl.a. drevet af en øget brug af internationale kort til at gennemføre mobilbetalinger via Apple Pay og Google Pay, som blev indført i Danmark i henholdsvis oktober 2017 og 2018.[18]

Frem til udgangen af 2024 var det kun Danske Bank og senest Nordea[19], som tilbød deres kunder at betale med Dankort i Apple Pay. Banker tilknyttet datacentralerne BEC og SDC, bl.a. Nykredit Bank, Spar Nord, Arbejdernes Landsbank, Sparekassen Danmark, Sparekassen Kronjylland og Lån & Spar Bank, har fra marts 2025 tilbudt deres kunder at betale med Dankort i Apple Pay.[20] Fra starten af 2025 har Nets stillet krav om, at når en kortudsteder/bank muliggør anvendelsen af et kort co-badged med Dankort i en Wallet-løsning, skal Dankort-siden også kunne anvendes. Udsteder en bank et Visa/Dankort, hvor Visa-siden kan anvendes i Apple Pay, skal banken altså sørge for, at Dankort-siden også kan anvendes i Apple Pay. Nets forventer, at dette på sigt vil styrke Dankorts position på markedet.

Driftsstabilitet

Driften af Dankort var tilfredsstillende i 2024 med høj driftsstabilitet og kun enkelte mindre hændelser. Hændelserne har ikke givet anledning til yderligere opfølgning fra Nationalbankens side.

Nets har i 2024 implementeret en teknisk løsning, der fordeler behandlingen af korttransaktioner bredere ud over dagen, så forsinkelser i fremsendelsen til afvikling og bogføring undgås. Løsningen indebærer også, at eventuelle forsinkelser i behandlingen af Dankort-betalinger ikke kan påvirke betalinger med internationale kort og omvendt. Løsningen er implementeret som opfølgning på problemer i 2023, hvor forsinket fremsendelse af Dankort-transaktioner i nogle tilfælde betød, at butikker modtog betalinger for salg en

[18] Se nationalbanken.dk, *Markedet for digitale betalinger forandrer sig*, 2025 (*link*).
[19] Nordeas kunder kunne fra november 2024 anvende Dankort i Apple Pay.
[20] Se FinansWatch, *40 banker åbner for Dankort i Apple Pay*, 25. marts 2025 *(link)*.

dag senere end sædvanligt. Nationalbanken har fulgt Nets' arbejde med at implementere løsningen.

Misbrug

Misbruget af Dankort er fortsat lavt. Det udgjorde i alt 29,4 mio. kr. i 2024, svarende til 0,10 promille af de samlede Dankort-betalinger.

Selvom misbruget med Dankort er lavt, har der været en betydelig stigning i misbruget i de seneste år. Fra 2023 til 2024 er misbruget således steget med 21 pct.[21] Dette afspejler en stigning både i forbindelse med tyveri og tabte kort samt misbrug ved handel på internettet.

Misbrug relateret til tyveri eller tab af kort udgør fortsat størstedelen af misbruget. Denne type misbrug beløb sig til 22,1 mio. kr. i 2024, mens misbruget ved handel på internettet var på 7,3 mio. kr.

Anvendelsen af stærk kundeautentifikation har nedbragt misbrug med stjålne eller kopierede kort online. Misbruget ved handel på internettet sker ifølge Nets nu primært, ved at kortholder manipuleres til at gennemføre svigagtige betalinger.

I den fysiske handel og ved hæveautomater sker misbruget ifølge Nets i stigende grad, ved at kortholder franarres kort og PIN-kode, fx ved at svindleren udgiver sig for at være fra politiet.

Internationale standarder

Nationalbanken har i 2024 fortsat dialogen med Nets om Dankorts efterlevelse af PISA. Nationalbanken har i den forbindelse vurderet Dankort efter PISA's krav til risikostyring og beredskab og givet anbefalinger til Nets' arbejde med disse områder. Nationalbanken har bl.a. anbefalet, at Nets styrker arbejdet med sit cyberberedskab og evnen til at håndtere ekstreme men plausible scenarier. Nationalbanken vil i 2025 følge op på Nets' arbejde med anbefalingerne.

Nationalbanken har i 2024 desuden fulgt Nets' arbejde med at sikre efterlevelse af DORA-forordningen, der finder anvendelse fra januar 2025. Det har bl.a. indebåret opdateringer af Nets' rammeværk for risikostyring og beredskabsplanlægning. Som del af denne proces har Nets også yderligere arbejdet med integrationen af Dankort i den europæiske betalingskoncern Nexi Group, som Nets blev en del af i begyndelsen af 2022.

Betalingsservice

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

Nationalbanken har i 2024 aftalt med MPS, at overvågningen af Betalingsservice udvides til også at omfatte PBS-clearingen, der anvendes til at samle transaktioner fra Betalingsservice og kortbetalinger, før de sendes til Sumclearingen.[22]

[21] Som andel af de samlede transaktioner. Stigningen i kroner er mindre på grund af den faldende anvendelse af Dankort.
[22] Vedrørende Sumclearing og de øvrige detailclearinger, se kapitel 4, *Clearing og afvikling af detailbetalinger.*

MPS købte i 2021 Betalingsservice og PBS-clearingen af Nets. I den forbindelse indgik MPS en aftale med Nets om, at Nets i en overgangsperiode skulle bidrage til at understøtte driften af de to systemer. MPS har løbende overtaget flere dele af driften af Betalingsservice og PBS-clearingen, og størstedelen af driften var overtaget i 2023 i forbindelse med overflytningen af de bagvedliggende systemer fra Nets' produktionsmiljø til MPS' eget produktionsmiljø i Kyndryls datacenter. Overgangsaftalen udløb i marts 2025, og MPS varetager nu den fulde drift af Betalingsservice og PBS-clearingen. Nationalbanken vurderer, at overgangen er foregået hensigtsmæssigt og har sikret den nødvendige kontinuitet i driften.

Driftsstabilitet og misbrug

Driftsstabiliteten i Betalingsservice i 2024 var ligesom tidligere år høj uden nedbrud eller andre hændelser af betydning. Der har ikke været misbrug af Betalingsservice i 2024.

Der var en hændelse i PBS-clearingen i november 2024, hvor fejl i bogføringsfiler skabte problemer med nogle bankers afstemning af kundernes konti. Nationalbanken har drøftet opfølgningen på hændelsen med MPS.

Internationale standarder

Nationalbanken har i 2024 fortsat dialogen med MPS om planerne for Betalingsservices efterlevelse af PISA, og MPS har i løbet af året arbejdet på at gennemføre planen. I den forbindelse har MPS bl.a. arbejdet med at styrke sit beredskab for at være i stand til at håndtere ekstreme men plausible scenarier. Arbejdet med PISA-efterlevelse indebærer tiltag i både første og anden forsvarslinje med kvartalsvis opfølgning på efterlevelsen af PISA samt rapportering til bestyrelsen. Nationalbanken vil drøfte resultaterne af dette arbejde med MPS i 2025.

Nationalbanken har i 2024 fulgt MPS' arbejde med implementering af kravene i DORA-forordningen, særligt hvad angår risikostyring og beredskabsplanlægning. Dette arbejde har også bestået i at integrere MPS yderligere i Mastercard-koncernens arbejde med disse områder. Nationalbanken har i den forbindelse drøftet med MPS, hvordan dette arbejde kan medvirke til at efterleve kravene i PISA.

04
Clearing og afvikling af detailbetalinger

I 2024 blev de danske detailbetalinger clearet og afviklet i Sum-, Intradag- og Straksclearingen, også kaldet Detailclearingerne. Detailclearingerne er ejet af Finans Danmark, forvaltes af e-nettet og leveres af Mastercard Payment Services A/S, MPS.

I Sumclearingen afvikles betalinger foretaget med bl.a. betalingskort, indbetalingskort og Betalingsservice én gang i døgnet på bankdage. I Intradagclearingen afvikles konto-til-konto-overførsler, fx netbank-overførsler, lønudbetalinger 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 Nationalbankens RTGS-system – i 2024 Kronos2 – hvor beløbene udveksles mellem bankerne. Derefter bogføres betalingerne på kundernes konti i bankerne.

I 2024 blev der i Straksclearingen gennemført konto-til-konto-overførsler på få sekunder døgnet rundt alle ugens dage. Dette lod sig gøre, fordi bankerne på forhånd reserverede likviditet i Kronos2 til overførslerne. Selve udvekslingen af likviditet mellem bankerne skete seks gange om dagen på bankdage. Straksclearingen blev primært anvendt til netbank-overførsler og til betalinger via MobilePay.

Detailbetalingsinfrastrukturen har i forbindelse med Nationalbankens udfasning af Kronos2 og flytning til TARGET DKK gennemgået en række forandringer, se boks 2. I påsken 2025 blev Sum- og Intradagclearingen integreret med T2 via TARGET DKK. Samtidig blev Straksclearingen udfaset. I stedet afvikles straksbetalinger i danske kroner nu i TIPS gennem TARGET DKK.

Hidtil har hovedsageligt banker kunnet deltage i Detailclearingerne. Som følge af ændringer i EU-lovgivningen har betalingsinstitutter og e-pengeinstitutter siden april 2025 kunnet ansøge om at deltage i de centrale betalingssystemer, herunder Detailclearingerne.[23]

Brug

Ved udgangen af 2024 var der 45 direkte deltagere i Detailclearingerne og 22 indirekte deltagere, som afvikler gennem en direkte deltager.

Værdien af transaktionerne i Detailclearingerne udgjorde i gennemsnit 48,6 mia. kr. pr. bankdag i 2024, se tabel 2. Det er en stigning på 3,2 pct. sammenlignet med 2023.

[23] I april 2025 trådte ændringer i det såkaldte finality-direktiv i kraft (Europa-Parlamentets og Rådets forordning (EU) 2024/886 af 13. marts 2024 om ændring af forordning (EU) nr. 260/2012 og (EU) 2021/1230 og direktiv 98/26/EF og (EU) 2015/2366 for så vidt angår strakskreditoverførsler i euro). Ændringerne gør det muligt for betalingsinstitutter (udbydere af betalingstjenester, der ikke er banker) og e-pengeinstitutter at deltage direkte i afviklingen af betalinger i de centrale betalingssystemer, herunder Detailclearingerne, uden at skulle gå igennem en bank.

TABEL 2

Værdi af transaktioner i Sum-, Intradag- og Straksclearingen, 2020-2024, gennemsnit pr. bankdag

Mia. kr., løbende priser	2020	2021	2022	2023	2024
Sumclearingen	18,7	20,5	21,3	21,2	21,8
Intradagclearingen	21,9	23,9	25	24	24,9
Straksclearingen	1,6	1,7	1,8	1,9	1,9
I alt	42,2	46,1	48,1	47,1	48,6

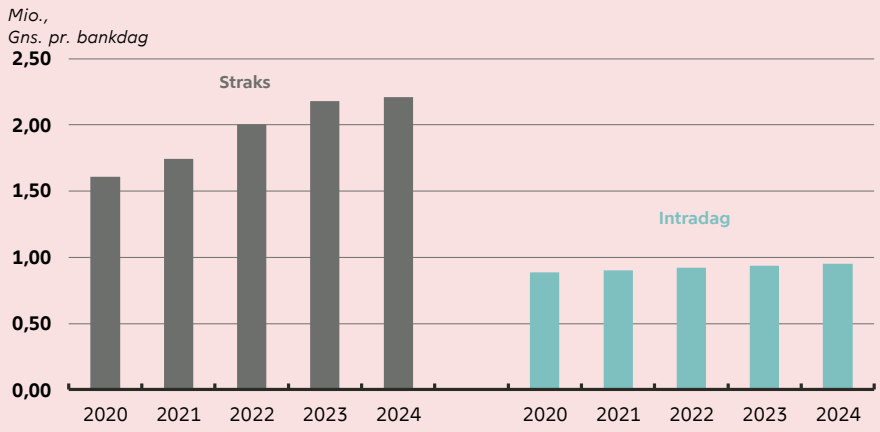
Kilde: Mastercard Payment Services A/S, MPS.

Antallet af transaktioner i Straksclearingen er steget siden årene under covid-19-pandemien, se figur 4.

FIGUR 4

Antal transaktioner i Straks- og Intradagclearingen, 2020-2024

Samlet antal transaktioner clearet og afviklet i Straks- og Intradagclearingen



Kilde: Mastercard Payment Services A/S, MPS.

Driftsstabilitet

Detailclearingerne har i 2024 haft en høj driftsstabilitet med enkelte hændelser af mindre betydning. Hændelserne har ikke givet anledning til yderligere opfølgning fra Nationalbankens side.

Likviditet

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

Der har ikke været henlæggelser på grund af manglende likviditet i 2024.

Internationale standarder og cyberrobusthed

Finans Danmark arbejder løbende på at styrke cyberrobustheden i clearingerne og har i 2024 fortsat arbejdet med at efterleve Nationalbankens anbefalinger fra vurderingen efter CPMI-IOSCO's Cyber Guidance fra 2022. Finans Danmark har bl.a. stillet styrkede krav i driftsaftalen med leverandøren Mastercard Payment Services, MPS. Dette har bl.a. muliggjort en gennemgang af MPS' efterlevelse af ECB's Cyber resilience oversight expectations for financial market infrastructures, CROE. Gennemgangen viste, at MPS i høj grad efterlever forventningerne i CROE. På enkelte områder er der lagt en plan for yderligere forbedringer. Herudover har Finans Danmark styrket håndteringen af legacy-udstyr/end-of-life-assets og udarbejdet en analyse af behovet for yderligere kryptering.

Finans Danmark fortsætter arbejdet med at styrke cyberrobustheden i clearingerne. Der arbejdes bl.a. på at styrke evnen til at kunne genoprette og/eller opretholde driften inden for fastsatte tidsrammer efter både likviditetsmæssige, tekniske og cyberrelaterede hændelser, herunder også i ekstreme men plausible scenarier.

Et andet element i arbejdet med cyberrobusthed er Finans Danmarks Cybersikkerhedshåndbog for clearingerne. I håndbogen stilles der krav til it-sikkerheden hos datacentralerne og de deltagende banker, der årligt skal evaluere og rapportere deres efterlevelse af disse krav. Finans Danmark har som vanligt fulgt op på den årlige evaluering efter kravene i cybersikkerhedshåndbogen i 2024.

I 3. kvartal 2024 opdaterede Finans Danmark cybersikkerhedshåndbogen, så der nu også stilles krav til, at deltagerne og datacentralerne arbejder mere aktivt med deres robusthed, nødplaner og mulighed for genoprettelse, herunder beredskabsplaner og nødprocedurer. Formålet er at sikre, at sektoren holder et kontinuerligt fokus på disse områder. Implementeringsperioden for ændringerne løber frem til udgangen af 2025.

Fokus på at nedbringe svindel

Finans Danmark nedsatte i december 2023 en særlig svindel-taskforce for at adressere misbrug og svindel rettet mod private. Formålet var at kortlægge de kriminelles processer, metoder og systemer samt komme med anbefalinger til forbedringer i forhold til bekæmpelse af digital svindel.[24] Taskforcen afsluttede sit arbejde i 2024 og præsenterede 18 konkrete anbefalinger[25]. Nogle anbefalinger er allerede implementeret eller i gang med at blive det, mens andre afhænger af ændringer i lovgivningen enten nationalt eller i EU.

Særligt relevant for clearingdeltagerne er en anbefaling om at etablere en fastfrysningsordning. En sådan ordning skal kunne fastfryse svindeltransaktioner, så svindlere ikke kan flytte svindlede beløb videre fra deres konti. Finans Danmark undersøger muligheden for at etablere en fælles løsning for den danske finansielle sektor. Det kræver bl.a. en lovændring at gennemføre anbefalingen.[26]

[24] Se også Finans Danmark, *Kampen mod digital svindel*, december 2023 (*link*), og Finans Danmark, *Netbanksvindel*, 2023 *(link*).
[25] Se Finans Danmark, *Her er 18 anbefalinger, der kan bremse it-svindlen i Danmark*, november 2024 (*link*).
[26] Se Europa-Kommissionen, Revision af det andet betalingstjenestedirektiv, PSD3, og en ny betalingstjenesteforordning, PSR (*link*).

Finans Danmark planlægger yderligere at etablere en Verification of Payee-tjeneste, VoP, til bankerne. VoP er, ligesom fastfrysningsordningen, et værktøj, der er designet til at bekæmpe svindel og misbrug. I kommende EU-lovgivning[27] stilles der bl.a. krav til, at en betalers betalingstjenesteudbyder skal tilbyde en service, der sikrer verifikation af modtageren, som betaleren ønsker at foretage en standard- eller straksbetaling til.

Systemændringer i clearinginfrastrukturen i 2024

MPS har i 2024 afsluttet arbejdet med at flytte driften af clearingerne fra Nets' produktionsmiljøer til egne miljøer.[28] Flytningen blev i tæt koordination med Finans Danmark opdelt i flere migreringsfaser. Driften af Sumclearingen blev i maj 2024 flyttet fra Nets' produktionsmiljø hos Kyndryl til MPS' produktionsmiljø hos samme. Driften af Intradag- og Straksclearingen blev i september 2024 flyttet fra Nets' datacentre i Norge til nye MPS-datacentre i henholdsvis Norge og Sverige. Med datacenterflytningen kører al clearingdrift nu i MPS' egne miljøer, uafhængigt af Nets.

Sektorprogram for modernisering af detailbetalingsinfrastrukturen

Der er i regi af Finans Danmark udarbejdet en samlet sektorplan, som skal sikre en fortsat modernisering af den danske detailbetalingsinfrastruktur. Arbejdet er forankret i et sektorprogram under Finans Danmarks bestyrelse, hvor der er nedsat en styregruppe med bred sektorrepræsentation. Programmet drives af e-nettet i tæt samarbejde med Finans Danmark og bliver koordineret med Nationalbanken som systemejer af TARGET DKK.

Under sektorprogrammet har Finans Danmark udarbejdet en langsigtet, strategisk plan for den danske clearinginfrastruktur, hvor et af målene er etableringen af en ny batchclearing. Dette er bl.a. drevet af en sektorbeslutning om at anvende de betalingsstandarder, der forvaltes af Nordic Payments Council, NPC[29]. Det betyder, at clearingsystemer skal være i stand til at sende og modtage NPC-kompatible beskedformater i forbindelse med konto-til-konto-overførsler. Sum- og Intradagclearingen bruger i dag ældre beskedformater og er derfor ikke NPC-kompatible.

Finans Danmark har underskrevet et memorandum of understanding med EBA CLEARING om en ny STEP2 DKK-clearingløsning, der skal afløse den eksisterende Intradagclearing. Med den nye STEP2 DKK-clearing vil batchclearingen blive løftet til en standardplatform, der er NPC-kompatibel. Derudover forventer Finans Danmark, at STEP2 DKK-clearingen vil øge resiliensniveauet. Finans Danmark forventer, at den nye clearing bliver igangsat i slutningen af 2026 eller begyndelsen af 2027.

[27] Se ECB vedr. EU-lovgivningen for standardkredit og straksoverførsler, Instant Payment Regulation, IPR (*link*).
[28] MPS købte i 2021 de områder af Nets' infrastruktur, der omfatter drift af Detailclearingerne, og har siden 2022 arbejdet med at flytte driften af clearingerne til egen infrastruktur. Se også Mastercard Payment Services Denmark A/S, *Mastercard gennemfører købet af Nets konto-til-konto betalingsenhed,* marts 2021 (*link*).
[29] NPC blev etableret i 2018 som en selvstændig nonprofit-forening af de fire nordiske bankforeninger (Bits A/S (Norge), Finans Danmark (Danmark), Finassiala (Finland) og Svenska Bankföreningen (Sverige). NPC's hovedformål er at harmonisere betalingsstandarderne i Norden, og der arbejdes fortsat på dette på tværs af de nordiske banker. NPC's betalingsstandarder er baseret på European Payment Councils, EPC, regelbøger og vejledninger, dog med visse tilpasninger bl.a. til svensk lovgivning og konteksten i lokale betalingslandskaber i Norden.

Udvikling af et straksbetalingssystem på tværs af valutaer

Nationalbanken indgik i januar 2024 en aftale med ECB og den svenske centralbank, Sveriges Riksbank, om at deltage i et projekt kaldet TIPS cross-currency. Projektet skal gøre det muligt for en borger eller virksomhed at foretage en betaling i fx danske kroner, som betalingsmodtageren derefter straks kan modtage i euro eller svenske kroner. Systemet skal gøre det hurtigere og billigere at foretage grænseoverskridende betalinger. På sigt kan systemet udvides til også at håndtere øvrige EU-valutaer, hvis de bliver en del af TIPS, eller potentielt forbindes til straksbetalingssystemer uden for EU.

05
Værdipapirafvikling

Værdipapirhandler kan indgås på forskellige måder: på børsen, gennem en multilateral handelsfacilitet eller bilateralt mellem parterne via en bank eller en fondsmægler. Efter handlerne er indgået, skal der ske en endelig afvikling af handlerne, dvs. hvor penge og værdipapirer udveksles mellem deltagerne.

Værdipapircentralen Euronext Securities Copenhagen, ES-CPH[30], varetager afviklingen af handler med dansk udstedte værdipapirer, og registreringer af ændringer i beholdningerne af værdipapirer sker på deltagernes konti i ES-CPH.

Værdipapirhandler mellem bankerne og andre finansielle investorer afvikles i første omgang på konti i det fælleseuropæiske system TARGET2-Securities, T2S, som varetager afviklingsprocessen på vegne af ES-CPH. Flytninger af værdipapirer på konti i T2S spejles efterfølgende på konti i ES-CPH's systemer. I juridisk forstand har den endelige afvikling af værdipapirhandlerne først fundet sted, når de relevante værdipapirkonti i ES-CPH opdateres. Afviklingen af pengesiden finder også sted på konti i T2S. Deltagerne skal derfor overføre likviditet til deres afviklingskonti i danske kroner på T2S.[31] Handler mellem bankerne og deres egne kunder afvikles fortsat i ES-CPH's eget afviklingssystem, ES-CPH-afviklingen.[32] ES-CPH har i de seneste år gradvist indskrænket brugen af ES-CPH-afviklingen og vil i løbet af 2027 helt udfase denne.[33]

ES-CPH står også for håndtering af periodiske betalinger, emissioner, indfrielser mv.[34] ES-CPH er den eneste virksomhed i Danmark med tilladelse fra Finanstilsynet til at drive værdipapircentral.

Brug

ES-CPH har 89 deltagere, hvoraf 38 er udenlandske markedsdeltagere, herunder 4 centrale modparter (Central Counterparties, CCP'er)[35]. 46 af deltagerne i ES-CPH havde i 2024 også en konto i Kronos2, så de kunne overføre likviditet til deres afviklingskonto på T2S. Det var også muligt at overføre likviditet til afviklingskonti på T2S via en deltager i Kronos2 uden selv at være deltager i Kronos2. Efter påsken 2025 sker denne overførsel af likviditet på samme vis blot fra konti i TARGET DKK i stedet for Kronos2, se kapitel 2, *Interbankbetalinger*.

I 2024 blev der i gennemsnit afviklet ca. 93.600 handler om dagen i danske kroner gennem ES-CPH, hvilket er en stigning på 10,6 pct. i forhold til 2023, se

[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] Frem til påsken 2025 kunne likviditeten overføres fra Nationalbankens betalingssystem Kronos2. Efter migreringen af danske kroner fra Kronos2 til T2 (se nærmere i kapitel 2 om interbankbetalinger) i påsken 2025 sker overførslen fra T2 til T2S. En stor del af likviditetsbehovet håndteres dog, ved at deltagerne stiller sikkerhed i deres værdipapirer.
[32] Opdelingen af afviklingen på henholdsvis T2S og ES-CPH-afviklingen kaldes også den lagdelte afviklingsmodel.
[33] Se også nærmere om denne udvikling i afsnittet *Systemændringer* nedenfor.
[34] Også kaldet corporate actions.
[35] De fire udenlandske CCP'er i ES-CPH er henholdsvis 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.

tabel 3 og figur 5. Det skyldes særligt en stigning i handler med investeringsforeningsbeviser på 15,3 pct. Værdien af de afviklede handler var i gennemsnit ca. 221,9 mia. kr. pr. bankdag, hvilket er et fald på 1,9 pct. i forhold til 2023, se tabel 3 og figur 6. Det skyldes særligt et fald i værdien af handler med obligationer.

TABEL 3

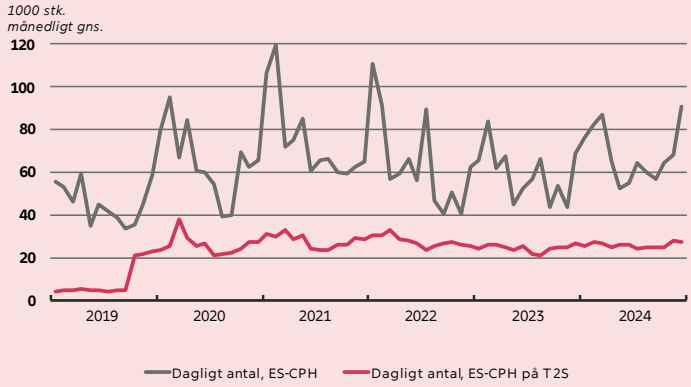
Antal og værdi af værdipapirhandler

	I alt		Obligationer		Aktier		Investeringsforenings-beviser	
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.
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	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
2023	84,7	226,3	4,6	165,0	39,8	53,1	40,4	8,2
2024	**93,6**	**221,9**	**3,8**	**144,4**	**43,3**	**68,6**	**46,5**	**9,0**

Kilde: ES-CPH.

FIGUR 5

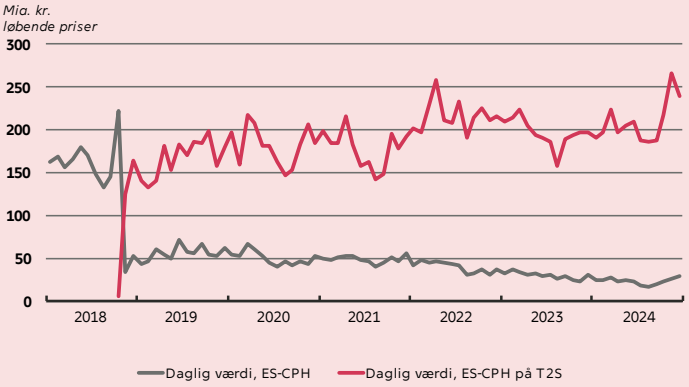
Antal værdipapirhandler



Kilde: ES-CPH.

FIGUR 6

Værdi af værdipapirhandler

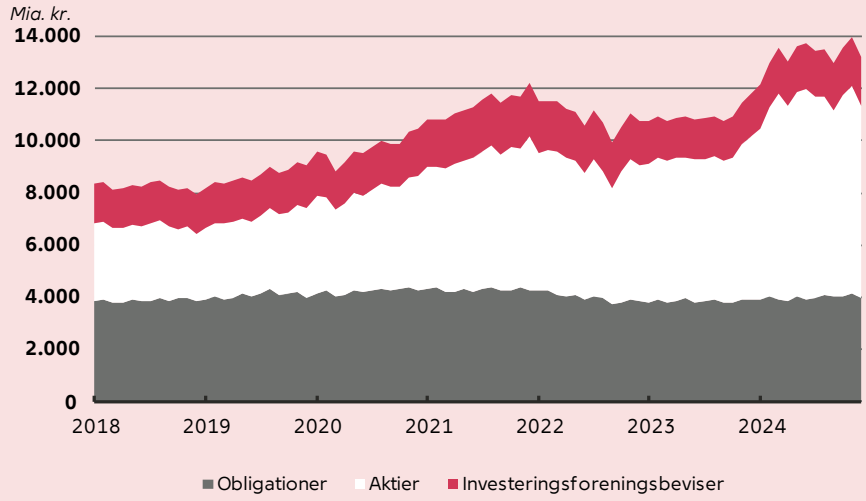


Kilde: ES-CPH.

Markedsværdien af værdipapirer opbevaret i ES-CPH steg i 2024 med 11,6 pct., se figur 7. Stigningen skyldes særligt stigninger i værdien af aktier og investeringsforeningsbeviser.

FIGUR 7

Markedsværdi af værdipapirer opbevaret i ES-CPH



Kilde: ES-CPH.

Afviklingsprocent

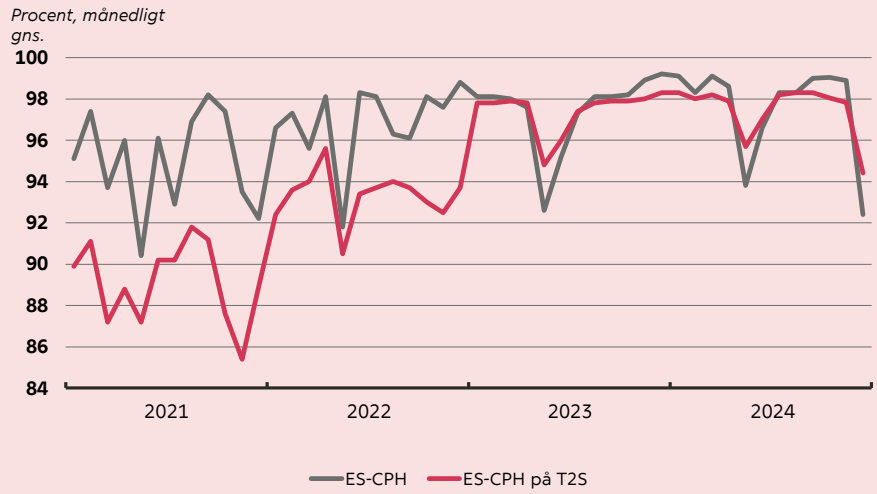
Afviklingsprocenten måler andelen af handelsomsætningen, der afvikles rettidigt, det vil sige senest to dage efter handlerne er indgået.[36]

Figur 8 viser afviklingsprocenten for henholdsvis ES-CPH's afvikling på T2S og for ES-CPH's eget system. Det er tilfredsstillende, at afviklingsprocenten i 2024 generelt er fastholdt på et højt niveau.[37]

[36] Ifølge CSDR, artikel 5, skal værdipapirhandler afvikles senest to dage efter handelsdagen. Der er igangsat et arbejde med at forkorte afviklingstiden, så handler afvikles senest dagen efter handelsdagen, se boks 5.
[37] Der var som tidligere år et fald i maj måned, som skyldes en særlig dansk banklukkedag, hvor T2S var åben (19. maj, dagen efter Kristi himmelfartsdag). I december måned var der desuden et større fald i afviklingsprocenten, som skyldes, at T2S var åben 24. og 31. december, som er danske banklukkedage. Der var ikke et lignende fald i december i 2022 og 2023, da dagene i de år faldt på weekenddage.

FIGUR 8

Afviklingsprocent



Kilde: ES-CPH.

Drift

Driftsstabiliteten i afviklingen af danske værdipapirhandler i ES-CPH-afviklingen har i 2024 overordnet været tilfredsstillende.

Siden det nye corporate actions-system, Megara, blev sat i drift i juni[38], har der dog været en række mindre hændelser og en større hændelse i september bl.a. grundet kapacitetsproblemer og fejlkonfigurationer i systemet. Hændelserne har bl.a. medført forsinkelser og fejlagtige betalinger, der efterfølgende skulle tilbageføres. Håndteringen af den større hændelse påvirkede desuden også Kronos2 og T2S.

ES-CPH har foretaget en grundig opfølgning på disse hændelser og håndteret de identificerede problemer. Nationalbankens overvågning vurderer, at opfølgningen på hændelserne har været tilfredsstillende.

En større hændelse i TARGET Services i februar 2025 medførte desuden, at ES-CPH måtte udskyde lukningen af afviklingsdøgnet næsten seks timer og efterfølgende foretage et større arbejde for at kunne gennemføre korrekt afstemning af deltagernes værdipapirkonti. Se nærmere om hændelsen i kapitel 6, *Betalinger og værdipapirafvikling i euro.*

Internationale standarder og cyberrobusthed

Nationalbanken overvåger, at afviklingen af danske værdipapirhandler i ES-CPH og T2S lever op til de internationale standarder for finansielle markedsinfrastrukturer, særligt CPMI-IOSCO's principper for finansiel markedsinfrastruktur, PFMI, og tilhørende retningslinjer for cyberrobusthed.

[38] Se nærmere beskrivelse i afsnittet *Systemændringer* nedenfor.

Nationalbankens overvågning af ES-CPH koordineres tæt med Finanstilsynet, da overvågningen berører mange af de samme elementer, som dækkes af Finanstilsynets tilsyn med, at ES-CPH efterlever kravene i den fælleseuropæiske lovgivning om værdipapircentraler, CSDR[39]. Nationalbanken bidrager i den forbindelse til Finanstilsynets løbende evalueringer af, om ES-CPH lever op til kravene i CSDR (også kaldet review and evaluation).

Overvågningen af T2S sker i samarbejde med alle de centralbanker, der er tilsluttet platformen, med ECB som hovedovervåger og koordinator, se kapitel 6, *Betalinger og værdipapirafvikling i euro*.

ES-CPH arbejder løbende på at forbedre cyberrobustheden i systemerne og har i 2024 fortsat arbejdet med Nationalbankens anbefalinger fra vurderingen af ES-CPH efter CPMI-IOSCO's Cyber Guidance fra 2020. Nationalbankens vurdering viste, at ES-CPH efterlever Cyber Guidance på de fleste områder. På få, men centrale, områder har Nationalbanken givet anbefalinger til ES-CPH om, hvordan cyberrobustheden bør styrkes. Det gælder bl.a. arbejdet med at styrke ES-CPH's cyberberedskab, herunder evnen til at håndtere ekstreme men plausible cyberscenarier. Dele af anbefalingerne er fortsat åbne.[40]

Systemændringer

I 2024 har ES-CPH fortsat arbejdet med at integrere sine systemer i Euronext-koncernen. Målsætningen er, at de fire værdipapircentraler i Euronext-koncernen[41] på sigt alle skal anvende den samme tekniske platform.

I juni 2024 begyndte ES-CPH at anvende Euronext-koncernens nye platform til håndtering af corporate actions, CA4U. Anvendelsen af CA4U skal føre til en øget automatisering, gennemsigtighed og standardisering af håndteringen af corporate actions på tværs af de fire CSD'er i Euronext-koncernen. Anvendelsen af den nye platform skal samtidig medvirke til, at ES-CPH kan efterleve de såkaldte SCoRE-standarder[42], der bl.a, stiller krav til håndteringen af corporate actions. Efterlevelsen af SCoRE-standarderne er en forudsætning for, at værdipapirer i euro udstedt af ES-CPH kan anvendes i Eurosystemets nye sikkerhedsstillelsessystem, ECMS, der efter planen skal anvendes fra juni 2025. I første omgang vil CA4U kun håndtere corporate actions for obligationer, og fra ultimo 2025 vil øvrige typer værdipapirer også blive håndteret heri. Indtil da vil CA4U derfor fungere i samspil med ES-CPH's eksisterende corporate actions-system.

I 2024 begyndte ES-CPH også at anvende Euronext-koncernens Message Hub til udveksling af beskeder mellem ES-CPH og deltagerne om clearing og afvikling af handler og betalinger.

ES-CPH har i 2024 fortsat arbejdet med at udfase brugen af den lokale afviklingsplatform, ES-CPH-afviklingen. I november 2024 blev handelsafvikling i danske kroner indskrænket yderligere og endeligt udfaset i marts 2025. Det samme skete for handler i euro i 2022. Derfor vil al afvikling i de to valutaer, hvor

[39] 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.
[40] Nationalbankens vurdering af ES-CPH efter Cyber Guidance er ikke offentliggjort.
[41] Ud over ES-CPH indgår CSD'erne i Italien, Norge og Portugal i Euronext-koncernen.
[42] Se ECB's standarder for sikkerhedsstillelse, *Single Collateral Management Rulebook for Europe, SCoRE* (*link*).

der udveksles penge mellem deltagerne, nu ske på T2S. Afvikling af værdipapirhandler via den lokale ES-CPH-afvikling vil derefter kun finde sted i svenske kroner eller som såkaldte free-of-payment-handler, FoP.[43] ES-CPH har besluttet, at den lokale afviklingsplatform udfases helt i 2027. Dette sker bl.a. som led i forberedelserne til at kunne afvikle alle værdipapirhandler dagen efter handelsdagen, også kaldet T+1, se boks 5 nedenfor. Derefter vil alle handler blive afviklet på T2S.

I november 2024 blev den såkaldte Sikkerhedsret, der anvendes til sikkerhedsstillelse for intradagkredit i Kronos2, også udfaset. Dette hænger sammen med, at afviklingen af betalinger i danske kroner fra påsken 2025 foregår i TARGET DKK, se kapitel 2, *Interbankbetalinger*.

BOKS 5

Forkortelse af afviklingstiden til T+1

I løbet af 2024 overgik flere markeder, herunder det amerikanske, til at afvikle værdipapirhandler dagen efter handelsdagen (også kaldet T+1). Indtil da har den generelle standard globalt været to dage efter handelsdagen (T+2), som det fortsat er i EU. Der har også i EU i længere tid været drøftelser om en forkortelse af afviklingstiden for værdipapirhandler. Det samme er tilfældet i Storbritannien og Schweiz, der er tæt forbundet med de europæiske markeder.

Europa-Kommissionen fremsatte 12. februar et forslag om en ændring af CSDR, der gør det lovpligtigt at afvikle værdipapirhandler senest T+1. Europa-Kommissionen foreslår, at ændringen skal finde anvendelse fra 11. oktober 2027[1], og det europæiske marked er nu gået i gang med at forberede sig på at kunne afvikle handler T+1.

Hos ES-CPH består forberedelserne bl.a. i at udfase den lagdelte afviklingsmodel, der bruges i dag. Med udgangen af 2027 vil ES-CPH derfor helt udfase brugen af den lokale ES-CPH-afvikling. Herefter skal alle værdipapirhandler afvikles på T2S. Dermed forenkles afviklingen, og det danske marked får bedre vilkår for at kunne håndtere en kortere afviklingsperiode.

Der er nedsat en arbejdsgruppe, der skal koordinere arbejdet med at forberede overgangen til T+1 for de danske markedsdeltagere. Gruppen er nedsat under den danske National Stakeholder Group (DK-NSG) for T2S og har repræsentanter fra ES-CPH, danske banker og andre relevante interessenter, herunder Nationalbanken.

[1] Se Europa-Kommissionens forslag om ændring af CSDR (*link*).

[43] Ved free-of-payment-handler udveksles kun værdipapiret mellem sælger og køber, og der er ikke penge involveret i afviklingen af handlen. Allerede i dag udveksles der sjældent penge mellem parterne i disse handler, da der er tale om handler mellem en bank og bankens egen kunde. Betalingen afregnes i det tilfælde internt i banken mellem kunden og banken selv.

06
Betalinger og værdipapirafvikling i euro

De danske banker bruger TARGET Services til at afvikle betalinger og værdipapirhandler i euro. TARGET Services kan håndtere flere valutaer, og i påsken 2025 blev al afvikling af danske kroner samlet på TARGET Services, se boks 2. Afviklingen af betalinger sker i T2, der er det fælleseuropæiske RTGS-system. I T2 kan deltagere derudover overføre likviditet til brug for afvikling i andre eurosystemer, herunder T2S, TARGET2Securities. T2S er det fælleseuropæiske system til afvikling af værdipapirhandler. I dette kapitel fokuseres på afviklingen af betalinger i euro.

TARGET Services ejes af Den Europæiske Centralbank, ECB, og de nationale centralbanker i euroområdet og drives af 4CB (de fire centralbanker i Tyskland, Frankrig, Italien og Spanien) med ECB som koordinator.

Overvågningen af TARGET Services sker i samarbejde mellem ECB's overvågningsfunktion 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 i alt omkring 1.000 banker, der anvender T2 til at gennemføre betalinger i euro, herunder 17 danske banker og filialer af udenlandske banker i Danmark. I 2024 gennemførte de danske deltagere interbankbetalinger for i gennemsnit 11,1 mia. euro om dagen. De danske deltagere bruger hovedsageligt T2 til at gennemføre koncerninterne betalinger og betalinger til udenlandske deltagere.

Der er i alt 24 værdipapircentraler med aktiviteter i 23 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.

En T2S-afviklingskonto oprettes via en af centralbankerne i EU, herunder Nationalbanken. 11 danske deltagere har en T2S-afviklingskonto i TARGET Services via Nationalbanken til betaling eller modtagelse af euro i forbindelse med T2S-afviklingen.[44]

Driftsstabilitet

Driftsstabiliteten i de lokale komponenter af T2, som Nationalbanken har ansvaret for, har været tilfredsstillende i 2024.

ECB har i 2024 arbejdet videre med de sidste udestående tiltag i den handlingsplan[45], der blev lavet for at følge op på de fem alvorlige it-relaterede

[44] Andre danske deltagere kan have oprettet en T2S-afviklingskonto via andre EU-centralbanker.
[45] Handlingsplanen har haft et bredt sigte og dækker tiltag inden for change and release management, business continuity management, failover and recovery tests, communication protocols, governance og data centre and IT operations.

hændelser (ikke cyberhændelser), der i 2020 påvirkede afviklingen af betalinger og værdipapirhandler i T2 og T2S. Nationalbanken deltager i ECB's opfølgning på handlingsplanen i regi af den fælles overvågning af TARGET Services.

27. februar 2025 medførte en større hændelse i TARGET Services, at der i omkring otte timer midt på dagen ikke kunne gennemføres betalinger i T2 og T2S, og lukningen af det pengepolitiske døgn i T2 og T2S blev udskudt i seks timer. I håndteringen af hændelsen blev nødløsningen i TARGET Services, ECONSII, aktiveret for at kunne foretage de mest tidskritiske betalinger. Hændelsen havde også konsekvenser for Kronos2, ES-CPH og CLS, se kapitel 2, *Interbankbetalinger og den centrale afvikling af betalinger i danske kroner,* kapitel 5, *Værdipapirafvikling,* og kapitel 7, *Valutahandelsafvikling.* Nationalbankens overvågning deltager i opfølgningen på hændelsen i regi af ECB's overvågning af TARGET Services.

Internationale standarder

ECB igangsatte i oktober 2023 en såkaldt comprehensive assessment af T2 og TIPS efter SIPS-forordningen, Regulation on oversight requirements for systemically important payment systems,[46] samt en vurdering af T2S efter CPMI-IOSCO's principper for finansielle markedsinfrastrukturer, PFMI. Arbejdet med vurderingerne er fortsat i 2024.

ECB har i 2024 fortsat arbejdet med anbefalingerne fra vurderingen af T2S efter Cyber resilience oversight expectations, CROE, som blev afsluttet i 2022. Nationalbankens overvågning deltager i ECB's opfølgning på handlingsplanen i regi af den fælles overvågning af TARGET Services.

Systemændringer

Idriftsættelsen af Eurosystemets nye sikkerhedsstillelsessystem, ECMS, er blevet forsinket og er nu planlagt til juni 2025.

Hidtil har hovedsageligt banker kunnet deltage i afviklingen af betalinger i T2 og TIPS. Som følge af ændringer i EU-lovgivning har betalingsinstitutter og e-pengeinstitutter siden april 2025 kunnet ansøge om at deltage i de centrale betalingssystemer, herunder T2 og TIPS.[47]

[46] SIPS implementerer PFMI i en ECB-forordning, der gælder for systemisk vigtige betalingssystemer i eurozonen.
[47] I april 2025 trådte ændringer i det såkaldte finality-direktiv i kraft. Ændringerne gør det muligt for betalingsinstitutter (udbydere af betalingstjenester, der ikke er banker) og e-pengeinstitutter at deltage direkte i afviklingen af betalinger i de centrale betalingssystemer, herunder T2 og TIPS, uden at skulle gå igennem en bank. Dog vil betalingsinstitutterne udelukkende have adgang til afviklingskonti i Eurosystemet og vil ikke få adgang til at anvende de pengepolitiske instrumenter.

07
Valutahandelsafvikling

Valutamarkedet er globalt set det største af alle finansielle markeder målt på omsætning. Det er både centralbanker, finansielle institutioner, virksomheder og privatpersoner, som har behov for at købe eller veksle valuta, fx for at kunne købe varer i udlandet. Valutahandler, hvor danske kroner købes eller sælges mod en anden valuta, kan enten afvikles via korrespondentbanker eller gennem det internationale valutahandelsafviklingssystem, CLS.

Ved afvikling gennem korrespondentbanker afvikles de to betalinger i en valutahandel ikke samtidig, hvilket udsætter parterne i handlen for afviklingsrisiko. Hvis betalingerne i forskellige valutaer skal udveksles på tværs af tidszoner, kan betalingerne være mange timer eller dage undervejs, hvilket medfører en betydelig afviklingsrisiko. Afviklingsrisikoen i en valutahandel er risikoen for, at én part betaler som aftalt, men ikke modtager den købte valuta, hvilket kan resultere i betydelige tab og potentielt føre til systemiske konsekvenser.

Afviklingsrisikoen kan reduceres ved at afvikle begge sider af en valutahandel samtidig[48] (payment-versus-payment, PvP), hvilket bl.a. er muligt i CLS. CLS-afviklingen blev lanceret i 2002 og har lige siden reduceret afviklingsrisikoen væsentligt ved handler på tværs af mange af verdens mest handlede valutaer. 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 7.000 mia. 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.

CLS ejes af de store internationale banker, der deltager i CLS-afviklingen, heriblandt Danske Bank og Nordea. Kun medejere kan deltage direkte i CLS-afviklingen.

Nationalbanken samarbejder med centralbankerne for de øvrige tilsluttede valutaer om overvågning af CLS, se boks 6.

[48] Se Bank for International Settlements, FX settlement risk: an unsettled issue, *BIS Quarterly Review*, december 2022 (*link*).

BOKS 6

Overvågning af CLS

Overvågningen af CLS foregår i en fælles overvågningskomite, CLS Oversight Committee[1], 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 særligt 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 betalingssystemer (Principles for financial market infrastructures, PFMI). CLS offentliggjorde senest i august 2024 en beskrivelse af, hvordan systemet efterlever CPMI-IOSCO's principper.[2]

[1] Se Fed, Federal Reserve System, *Protocol for the Cooperative Oversight Arrangement of CLS* (*link*).
[2] Se CLS, *Principles for financial market infrastructures (PFMI) disclosure*, 2024 (*link*).

Brug

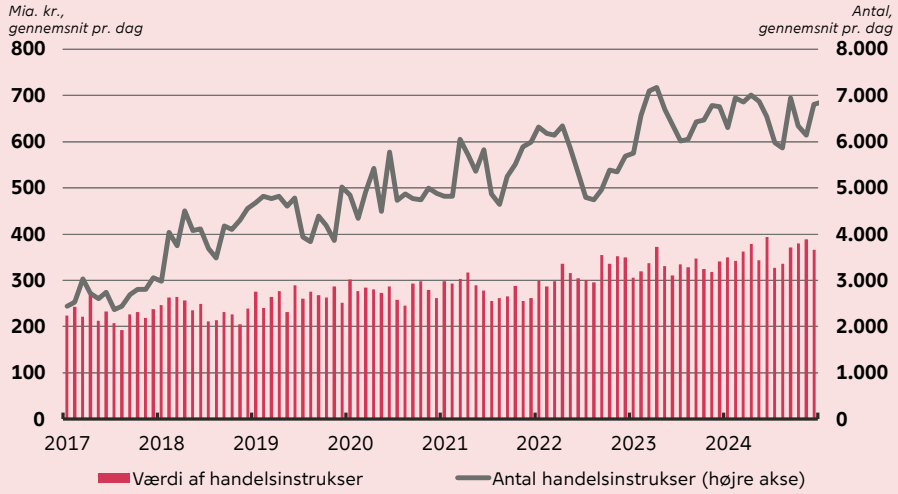
Danske kroner er den 20.-mest omsatte valuta i verden.[49] For danske kroner gælder det, at ca. 90 pct. af alle valutahandler med danske kroner som det ene ben i valutahandlen afvikles i CLS.[50] Den gennemsnitlige daglige værdi af handler i danske kroner i CLS var på 361 mia. kr. i 2024. Det er en stigning på 9,4 pct. i forhold til 2023, se figur 9.

Både danske banker og erhvervsvirksomheder kan afvikle valutahandler via CLS. Der er fire direkte deltagere i CLS, der gennemfører indbetalinger i danske kroner til CLS-afviklingen. Derudover er der en række danske banker og virksomheder, der deltager indirekte i CLS-afviklingen via en af de fire direkte deltagere.

[49] Se Danmarks Nationalbank, Stor fremgang i kronehandel og større dansk valutamarked, *Danmarks Nationalbank Statistiknyhed*, december 2022 (*link*).
[50] Anslået på baggrund af Bank for International Settlements, *Triennial Central Bank Survey, OTC foreign exchange turnover in April 2022*, oktober 2022 (*link*), og data fra CLS Bank.

FIGUR 9

Handelsinstruktioner i CLS



Kilde: CLS Bank.

Driftsstabilitet og likviditet

De danske deltagere reserverede i 2024 tilstrækkelig likviditet til CLS-afviklingen.

CLS-afviklingen foregår i et relativt kort tidsrum på døgnet, hvor de tilsluttede centralbankers RTGS-systemer – på tværs af tidszoner – er åbne samtidig. Ind- og udbetalinger til CLS sker via de tilsluttede centralbankers RTGS-systemer, dvs. for danske kroner via Kronos2 i 2024 og siden påsken 2025 via TARGET DKK. Stabiliteten i CLS-afviklingen 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. Det var fx tilfældet i februar 2025, hvor CLS-afviklingen blev påvirket af en større hændelse i TARGET Services, se kapitel 6, *Betalinger og værdipapirafvikling i euro*. Flere deltageres indbetalinger i euro til CLS-afviklingen blev som følge af problemerne i TARGET Services forsinkede, hvilket førte til, at CLS-udbetalinger i flere valutaer blev udskudt til først på aftenen i stedet for midt på dagen.

Der var ingen hændelser i Kronos2 i 2024, der førte til forsinkelser i CLS-afviklingen.

Må vi sende dig *nyheder* fra Nationalbanken?

Få besked om vores nyeste udgivelser direkte i din indbakke.

Læs mere om vores nyhedsservice
og tilmeld dig på *nationalbanken.dk/da/nyhedsservice,*
eller *scan QR-koden.*

Du kan også få vores nyheder som RSS-feeds.
Læs mere på nationalbanken.dk/da/rss-feeds.

Publikationer

NYT

Nyt er en appetitvækker, der giver et hurtigt indblik i en af Nationalbankens længere publikationer. Nyt er for dig, der har brug for et let overblik og godt kan lide en tydelig vinkling.

STATISTIK NYHED

Statistiknyheder sætter fokus på de nyeste tal og tendenser i Nationalbankens statistikker. Statistiknyheder henvender sig til dig, der vil have hurtig indsigt i aktuelle finansielle data.

RAPPORT

Rapporter er en tilbagevendende beretning om Nationalbankens arbejdsområder og virksomhed. Her finder du bl.a. Nationalbankens årsrapport. Rapporter er for dig, der har brug for en status og opdatering på den forgangne periode

ANALYSE

Analyser fokuserer på aktuelle emner, som er særligt relevante for Nationalbankens formål. Analyser kan også indeholde Nationalbankens anbefalinger. Her finder du bl.a. vores prognose for dansk økonomi og vores vurdering af den finansielle stabilitet. Analyser henvender sig til dig, der har en bred interesse for økonomiske og finansielle forhold.

ECONOMIC MEMO

Economic Memo giver indblik i det analysearbejde, som Nationalbankens ansatte er i gang med. Economic Memo indeholder fx baggrundsanalyser og metodebeskrivelser. Economic Memo henvender sig primært til dig, der i forvejen har kendskab til økonomiske og finansielle analyser.

WORKING PAPER

Working Paper præsenterer forskningsarbejde fra både ansatte i Nationalbanken og vores samarbejdspartnere. Working Paper henvender sig primært til dig, som er fagperson, og til dig med interesse for forskning inden for centralbankvirksomhed samt økonomi og finans i bredere forstand.

Analysen 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
+45 3363 6363

Redaktionen er afsluttet 31. marts 2025

DANMARKS NATIONALBANK