DANMARKS NATIONALBANK

RAPPORT | Overvågning af den finansielle infrastruktur
4. maj 2026 | Nr. 3

Overvågning af den finansielle infrastruktur 2025

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 2025.

Skrevet af

Lone Natorp
Chef for Overvågningen
ln@nationalbanken.dk
+45 3363 6161

Anne Hye Hedemann
Overvåger af interbankbetalinger og valutahandelsafvikling
anhk@nationalbanken.dk
+45 3363 6262

Jonas Moltke-Aaen
Overvåger af betalingsløsninger og værdipapircentraler
jmaa@nationalbanken.dk
+45 3363 6137

Line Bolding Holmegaard
Overvåger af detailbetalingssystemer
lbh@nationalbanken.dk
+45 3363 6087

Mathilde Bak Møller
Overvåger af detailbetalingssystemer
mbm@nationalbanken.dk
+45 3363 6109

37 Sider

Betalingsinfrastrukturen er sikker, effektiv og stabil

De centrale systemer og løsninger i infrastrukturen lever i høj grad op til de krav, som internationale standarder stiller til bl.a. organisering, risikostyring og beredskab. Det medvirker til, at borgere og virksomheder i Danmark normalt kan udveksle betalinger uden forsinkelser og forstyrrelser.

Truslerne mod infrastrukturen er fortsat alvorlige og udvikler sig løbende

Systemejerne har generelt en høj grad af modenhed i arbejdet med cyberrobusthed, men truslen fra cyberkriminelle er fortsat høj og udvikler sig løbende. Desuden er flere forhold, herunder brugen af hybride virkemidler, med til at gøre trusselsbilledet mere komplekst. Derfor skal robustheden i infrastrukturen fortsat styrkes for at være på forkant med udviklingen.

Der er fortsat behov for fokus på robuste beredskaber

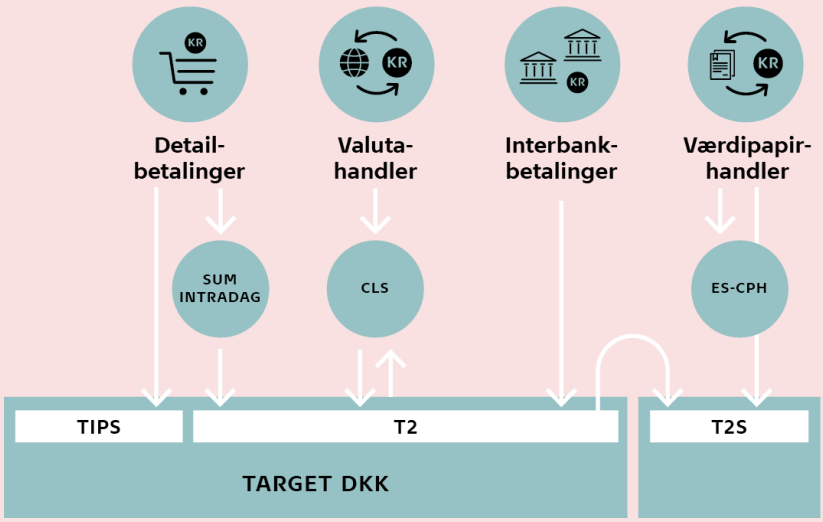
Det er ikke muligt at beskytte sig fuldt ud mod cyberangreb og andre operationelle hændelser. Derfor skal systemejerne have beredskaber på plads til at genoprette driften hurtigt og sikkert efter et angreb eller andre former for nedbrud. Nationalbanken anbefaler, at systemejerne også forbereder sig på at kunne håndtere ekstreme situationer såsom nedbrud på flere datacentre eller korrumpering af kritisk data.

Hvorfor er det vigtigt?

I 2025 blev der på en gennemsnitlig bankdag sendt betalinger for 838 mia. kr. – svarende til en fjerdedel af BNP – 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

1
Introduktion

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. Det er afgørende for den finansielle stabilitet og samfundsøkonomien, at disse systemer og løsninger fungerer uden forstyrrelser og nedbrud, så det er nemt og effektivt at betale for varer og tjenester. I 2025 blev der gennem betalingsinfrastrukturen hver dag udvekslet betalinger for 838 mia. kr.

Fordi betalingsinfrastrukturen spiller en så kritisk rolle i samfundsøkonomien, overvåger Nationalbanken, at de centrale systemer i infrastrukturen er velfungerende, sikre og effektive. Overvågningen omfatter også de vigtigste betalingsløsninger. Som del af overvågningen vurderer Nationalbanken, om de overvågede systemer og løsninger lever op til internationale standarders høje krav til sikkerhed og effektivitet, herunder krav til cyberrobusthed. Nationalbanken anbefaler ændringer til systemerne og løsningerne, hvis de ikke lever op til kravene. Nationalbankens overvågning er beskrevet nærmere i boks 1.

BOKS 1

Nationalbankens overvågning i 2025

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

- TARGET DKK (afvikling i danske kroner via T2 og TIPS på TARGET Services samt Nationalbankens system for de pengepolitiske instrumenter og sikkerhedsstillelse, SPI)
- Sumclearingen og Intradaglearingen (detailbetalinger)
- Euronext Securities Copenhagens afviklingssystem (værdipapirafvikling)
- Dankort, Betalingsservice og konto-til-konto-overførsler (de vigtigste betalingsløsninger)

Internationale systemer, som Nationalbanken deltager i overvågningen af:

- TARGET Services, der består af
  - T2 (interbankbetalinger)
  - T2S, TARGET2-Securities (værdipapirafvikling)
  - TIPS, TARGET Instant Payment Settlement (straksbetalinger)
- CLS (valutahandler).

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.

Fortsættes ...

... fortsat

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 Danmarks Nationalbank, *Overvågningspolitik 2025*, september 2025 (*link*).

Den danske betalingsinfrastruktur er beskrevet nærmere i boks 2.

BOKS 2

Betalingsinfrastrukturen i Danmark

På bankdage[1] i 2025 blev der i gennemsnit sendt betalinger for 838 mia. kr. gennem den danske betalingsinfrastruktur. Det svarer til omkring en fjerdedel af det danske BNP.

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

TARGET Services er en fælleseuropæisk teknisk platform, som stilles til rådighed for deltagende centralbanker af den Europæiske Centralbank, ECB, og Eurosystemet. Danske kroner benytter de 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 betalingsinfrastrukturen, 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. Afvikling i danske kroner i TARGET Services er anmeldt som et særskilt betalingssystem i henhold til kapitalmarkedsloven. Den danske betalingsinfrastruktur, som den så ud fra påsken 2025, er vist i boksens Figur A.

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, og efterfølgende afviklet i Kronos2. Efter påsken 2025 afvikles nettopositioner fra Sum- og Intradagclearingen i TARGET DKK. Straksbetalinger afvikles efter påsken 2025 gennem TIPS DKK, hvor betalingerne bliver afviklet enkeltvist og i realtid. Nationalbanken er systemejer for TIPS DKK, der har erstattet Straksclearingen, som nu er lukket. Sum- og Intradagclearingen ejes af Finans Danmark.

Fortsættes ...

... fortsat

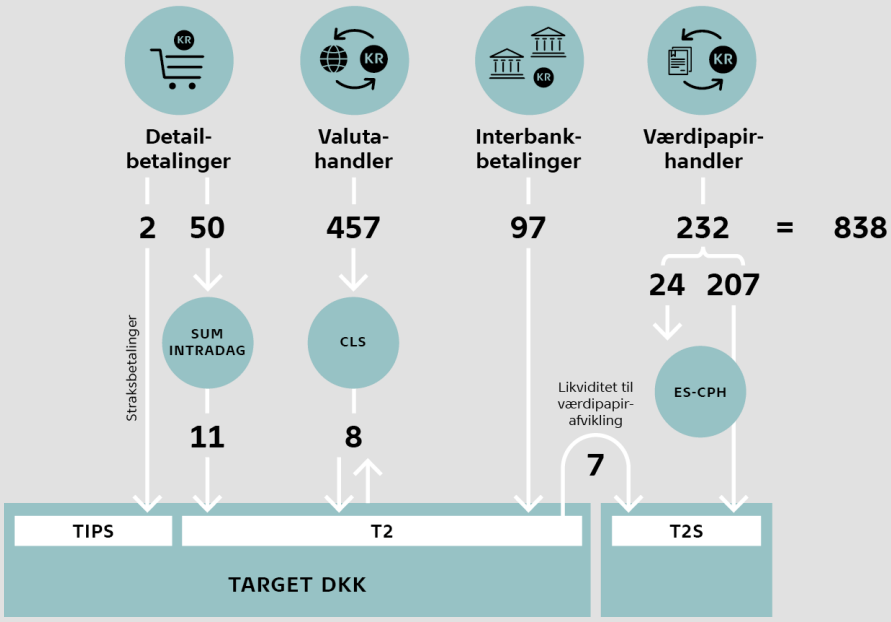
Værdipapirhandler kan indgås på forskellige måder: På børsen, gennem en multilateral handelsplatform eller bilaterale handler via en bank eller fondsmægler (også kaldet "over the counter"). Afviklingen af handler med dansk udstedte værdipapirer håndteres af værdipapircentralen Euronext Securities Copenhagen, 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.

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 i TARGET DKK via T2. Før påsken 2025 reserverede deltagerne likviditet til afviklingen af valutahandler i CLS på konti i Kronos2. CLS ejes af en række store internationale banker.

Netting har stor betydning for afviklingen af betalinger
Sum- og Intradagclearingen afvikler som nævnt ovenfor deres deltageres nettopositioner på deltagernes konti i TARGET DKK. 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 50 mia. kr. til 11 mia. kr. dagligt, svarende til en reduktion på 78 pct. På T2S sker afviklingen også ved brug af netting. Likviditeten til afviklingen på T2S overføres fra deltagernes pengekonti i TARGET DKK. Nettingen reducerer deltagernes behov for at reservere likviditet fra 207 mia. kr. til 7 mia. kr., hvilket svarer til en reduktion på ca. 97 pct.

FIGUR A

Betalingsflow, mia. kr., gennemsnit pr. bankdag i 2025



[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 lever i høj grad op til 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. Samtidig udvikler trusselsbilledet sig hele tiden, så der er behov for løbende at styrke robustheden, se nedenfor.

Driftsstabiliteten i infrastrukturen var i 2025 generelt høj, og der er sjældent forstyrrelser i udveksling af betalinger og afvikling af værdipapirhandler i Danmark. I 2025 var der enkelte forstyrrelser i infrastrukturen bl.a. i forbindelse med tre større hændelser i TARGET Services samt en større hændelse i kortbetalingsinfrastrukturen. Nationalbankens overvågning har fulgt op over for ejerne af systemerne for at sikre, at opfølgningen på hændelserne er tilfredsstillende. Hændelserne og den efterfølgende opfølgning er nærmere beskrevet nedenfor i afsnittene om de respektive systemer.

Den operationelle robusthed er høj, men skal løbende udvikles

Trusselsbilledet for den finansielle sektor udvikler sig løbende. Cybertruslen mod den finansielle sektor er fortsat høj, og betalingsinfrastrukturen kan blive udsat for alvorlige cyberangreb eller andre operationelle hændelser, der kan føre til forstyrrelser og nedbrud i den finansielle sektor. Flere forhold er med til også at gøre trusselsbilledet mod Danmark mere komplekst, bl.a. udbredelsen af hybride trusler.[1]

I august 2025 blev telekommunikationsudbyderen Colt Technology Services ramt af et ransomware-angreb, der bl.a. påvirkede virksomhedens administrative systemer. Colt Technology Services' netværk anvendes bl.a. til at tilgå TARGET Services. Angrebet medførte ikke forstyrrelser eller kompromittering af tjenester relateret til TARGET Services.[2]

Ejerne af systemerne i den finansielle infrastruktur har gennem de seneste år lagt en stor indsats i arbejdet med at øge infrastrukturens robusthed overfor cyberangreb og andre trusler, og har generelt en høj modenhed på området. Den vedvarende udvikling i trusselsbilledet betyder dog, at robustheden overfor cyberangreb og andre trusler fortsat skal styrkes.

I de senere år har ejerne af systemerne særligt haft stort fokus på arbejdet med beredskaber i tilfælde af, at cyberkriminelle skulle få succes med at trænge ind i systemerne, og Nationalbankens overvågning har givet en række af systemerne anbefalinger til at styrke arbejdet på området. Det gælder bl.a. anbefalinger om at sikre stærke rammer for arbejdet med at håndtere ekstreme, men plausible scenarier såsom datakorrumpering og nedbrud på flere datacentre. Nationalbanken har i 2025 bl.a. fulgt op på, hvordan systemejerne udvælger konkrete og relevante scenarier og inkluderer dem i deres beredskabsarbejde. Systemejernes arbejde med de disse anbefalinger i 2025 er beskrevet i kapitel 2, 3, 4 og 5 nedenfor.

Nationalbanken har i 2025 analyseret, hvordan det kan sikres, at borgere og virksomheder fortsat kan gennemføre betalinger og overføre penge, selv hvis

[1] For en nærmere beskrivelse af trusselsbilledet mod den finansielle sektor, se Danmarks Nationalbank, *Usikre tider kræver fokus på robusthed og beredskab, Danmarks Nationalbank Analyse (Finansiel stabilitet), nr. 28,* november 2025 *(link)*.
[2] Bleeping Computer, *Colt Telecom attack claimed by WarLock ransomware, data up for sale,* 15. august 2025 *(link)*.

centrale systemer eller data ikke er tilgængelige. Nationalbanken har på baggrund af analysen givet finansielle virksomheder en række anbefalinger til at styrke de operationelle beredskaber.[3] Disse anbefalinger er også relevante for systemejernes efterlevelse af de internationale standarder, og Nationalbankens overvågning vil i 2026 følge systemejernes arbejde med disse anbefalinger.
Det er helt centralt, at systemerne i infrastrukturen er godt rustet til at håndtere nedbrud og andre hændelser, også hvis de skulle have en ekstrem karakter. Samtidig kræver arbejdet med cyberrobusthed en holistisk tilgang. Det er derfor vigtigt, at systemejerne fortsætter arbejdet med at styrke alle dele af sikkerheden, herunder også beskyttelse mod indtrængning i systemerne samt evnen til hurtigt at opdage cyberhændelser tidligt i forløbet. Kravene til systemejernes arbejde med cyberrobusthed er nærmere beskrevet i 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 og ECB's *Cyber resilience oversight expectation for financial market infrastructures*, CROE.

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, for at styrke cyberrobustheden.

De fem indsatsområder og de tre tværgående elementer under CROE er illustreret i Figur B.

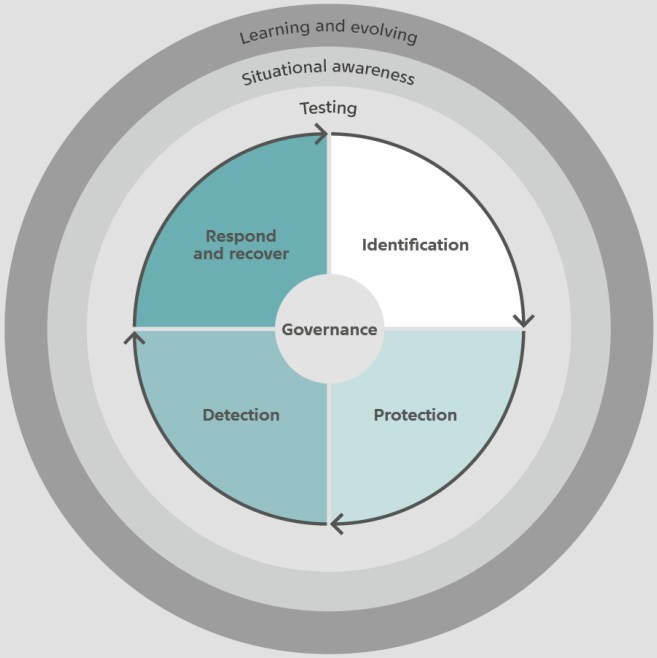
Fortsættes ...

[3] Danmarks Nationalbank, *Beredskab for samfundskritiske aktiviteter i den finansielle sektor i ekstreme scenarier*, *Danmarks Nationalbank Analyse,* nr. 29, december 2025 (*link*).

... fortsat

FIGUR B

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.

Sektorsamarbejder bidrager til at styrke operationel robusthed

Systemerne i den finansielle infrastruktur er tæt forbundne, og koordination og videndeling i arbejdet med operationel robusthed, herunder særligt cyberrobusthed, er afgørende. De internationale standarder stiller derfor en række krav til deltagelse i sektorsamarbejder, der skal øge sektorens operationelle robusthed som helhed, herunder robustheden over for cyberangreb. Desuden styrker denne form for samarbejder også de enkelte virksomheders eget arbejde med operationel robusthed. Nationalbankens overvågning følger løbende systemejernes deltagelse i de danske sektorsamarbejder.

De internationale standarder stiller krav til, at systemejerne løbende identificerer, overvåger og håndterer risici, der er relateret til deltagerne i systemet og til andre systemer. Det indebærer særligt et fokus på, at risici fra gensidige afhængigheder mellem systemerne håndteres. Håndtering af disse risici kræver tæt samarbejde mellem alle dele af økosystemet. Dette samarbejde sker i Danmark bl.a. gennem *Finansielt Sektorforum for Operationel Robusthed*, FSOR,[4] der er et offentlig-privat samarbejdsforum ledet af Nationalbanken.

[4] 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 2025 (*link*).

Medlemmerne i FSOR drøfter risici, deler viden og beslutter fælles mitigerende initiativer. FSOR har desuden etableret et fælles kriseberedskab, der skal koordinere indsatsen på tværs af den finansielle sektor i tilfælde af en krise, som kan true den finansielle stabilitet.[5] FSOR udarbejder løbende et fælles risikobillede, hvor cybertruslen fortsat udgør den primære risiko. I 2025 har FSOR også haft særligt fokus på bl.a. kvantesikker kryptering, netværksforbindelser og kriseberedskab og -kommunikation. Nationalbankens overvågning har drøftet arbejdet med disse emner med ejerne af de overvågende systemer og løsninger.

Ejerne af de centrale systemer i infrastrukturen samarbejder desuden i *Risikoforum for Gensidige Afhængigheder*, RGA[6], om at håndtere konkrete risici fra gensidige afhængigheder. RGA har tidligere arbejdet med kontrolleret nedlukning og genåbning i en række scenarier. I 2025 har Nationalbanken fulgt op på systemejernes eget arbejde med de planer.

Samararbejdet om cyberrobusthed er også understøttet af TIBER-DK-programmet. I en TIBER-test skal virksomhederne identificere, forhindre og reagere på avancerede cyberangreb simuleret i de faktiske produktionsmiljøer. Testen giver på den måde konkrete input til, hvordan virksomheden beskytter sine samfundskritiske aktiviteter mod cyberangreb og undgår, at cyberangreb forårsager skade. Deltagerne i TIBER-DK deler efterfølgende læring fra disse tests med hinanden for at styrke cyberrobustheden.[7]

Endelig stiller de internationale standarder også krav til tværgående deling af information om cybertrusler og cyberangreb. De centrale systemer og løsninger i infrastrukturen deltager alle i *Nordic Financial CERT*, NFCERT[8], der er et fællesnordisk sektorsamarbejde om indsamling og deling af information om cybertrusler og cyberangreb.

Konsolidering og internationalisering af infrastrukturen fortsætter

Den danske betalingsinfrastruktur er gennem en årrække blevet tættere integreret i den europæiske infrastruktur, og flere systemer og løsninger indgår i internationale koncerner. Det er en udvikling, der er fortsat i 2025.

I 2025 har Finans Danmark, som er systemejer for Sum- og Intradagclearingen for detailbetalinger, sat gang i forberedelserne til at benytte EBA CLEARING som ny leverandør af clearinginfrastruktur. EBA CLEARING er et non-profitselskab, der er ejet af 48 europæiske banker. EBA CLEARING foretager i dag clearing af detailbetalinger i euro og skal nu udvikle en clearingløsning i danske kroner, som skal afløse den eksisterende Intradagclearing.

ES-CPH har i 2025 arbejdet videre med Euronext-koncernens såkaldte *convergence programme*, der indebærer, at alle fem CSD'er i koncernen skal køre på samme tekniske platform[9]. ES-CPH vil efter planen i 2028 have gennemført programmet, hvorefter alle de vigtigste tjenester vil køre på Euronext-koncernen fælles tekniske systemer.

[5] FSOR's kriseberedskab supplerer medlemmernes egne kriseplaner og det nationale kriseberedskab, NOST. Nationalbanken varetager formandskabet for FSOR's kriseberedskab og er ansvarlig for sekretariatsbetjeningen.
[6] Risikoforum for Gensidige Afhængigheder er et samarbejdsforum mellem de organisationer, der er ansvarlige for de centrale betalings- og afviklingssystemer i infrastrukturen, dvs. Nationalbanken (interbank- og straksbetalinger), ES-CPH (værdipapirhandler), Finans Danmark (detailbetalinger) og e-nettet (kommunikationsnetværk). Arbejdet i RGA koordineres med FSOR.
[7] Se Nationalbanken, TIBER-DK/TLPT – trusselsbaserede red team-test, 2026 (*link*).
[8] 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.
[9] Euronext, *Euronext Securities CSD Convergence Programme*, 2026 (*link*).

Nets, der driver Dankort, og MPS, der driver Betalingsservice, er ligeledes en del af internationale koncerner, hvor forretningsfunktioner og systemer deles på tværs af koncernen.

Nationalbankens overvågning følger løbende udviklingen med henblik på at sikre, at systemejerne fortsat efterlever de internationale standarder.

2
Interbankbetalinger og den centrale afvikling af betalinger i danske kroner

En interbankbetaling er en betaling mellem finansielle institutioner. Disse betalinger er typisk kendetegnet ved at være både tidskritiske og af høj værdi. De afvikles i et såkaldt RTGS-system, der står for *Real Time Gross Settlement System,* hvilket betyder at betalingerne afvikles enkeltvis og øjeblikkeligt.

Interbankbetalinger i danske kroner blev afviklet i Nationalbankens Kronos2 frem til påsken 2025, hvor afviklingen blev flyttet til TARGET DKK. TARGET DKK er en samlet betegnelse for afviklingen af betalinger i danske kroner på TARGET Services og Nationalbankens system for det pengepolitiske instrumentarium og sikkerhedsstillelse, SPI.

TARGET DKK fungerer som et centralt knudepunkt i den danske betalingsinfrastruktur. Udover interbankbetalinger afvikles også pengepolitiske operationer og nettopositioner fra bl.a. detailbetalingssystemerne, og der bliver overført likviditet til afvikling af værdipapir- og valutahandler, som foregår i andre systemer.

Med flytningen er danske kroner den første valuta, udover euroen, til at afvikle RTGS-betalinger på den fælleseuropæiske platform, TARGET Services.

Brug

De fleste danske banker og realkreditinstitutter deltager i TARGET DKK og har konto i Nationalbanken, på samme måde som privatpersoner har konto i en privat bank. Derudover deltager også filialer af udenlandske banker.

Ved udgangen af 2025 var der 71 deltagere i betalingsafviklingen i TARGET DKK, hvoraf 29 af dem var under co-management. Co-management er en ny deltagelsestype i Danmark, som kommer fra TARGET Services. Co-management er målrettet de mindre pengeinstitutter, der i denne sammenhæng kaldes for co-managees. En co-managee er kontohaver i Nationalbanken, men har kun en konto til opbevaring af likviditet. Co-managees indgår aftale med en direkte deltager, typisk et større pengeinstitut, der bliver co-manager. Co-manageren administrerer co-managees konto og udfører betalingsinstruktioner på vegne af co-managee. Co-managees har ikke selv forbindelse til TARGET Services. Direkte forbindelse til TARGET Services kræver både efterlevelse af en række sikkerhedskrav, herunder fra deltagerens valgte netværksleverandør SWIFT eller Nexi. Formålet med sikkerhedskravene er at sikre deltagernes modstandsdygtighed overfor potentielle cyberangreb. Det er en omfattende opgave at sikre og attestere efterlevelse af kravene til direkte forbindelse til TARGET Services, og bl.a. derfor vælger mindre pengeinstitutter typisk co-management.

I 2025 blev der gennemført interbankbetalinger i TARGET DKK[10] for 97,4 mia. kr. i gennemsnit pr. bankdag. Det er et fald på 3,5 pct. fra 2024, se tabel 1.

[10] Inkl. Kronos2 indtil flytningen af afviklingen af betalinger i danske kroner i påsken 2025.

Drift

I 2025 var driftsstabiliteten i afviklingen af interbankbetalinger i danske kroner overordnet tilfredsstillende.

I henholdsvis februar og maj 2025 var der to større hændelser i TARGET Services, som medførte, at deltagerne i Kronos2/TARGET DKK ikke kunne gennemføre betalinger eller værdipapirhandler i flere timer. Se nærmere beskrivelse af hændelserne i kapitel 6, Betalinger og værdipapirafvikling i euro.

I marts var der en hændelse i T2S på TARGET Services, der førte til en forsinkelse i lukningen af det danske pengepolitiske døgn samt i åbningen af det nye døgn i Kronos2.

I slutningen af maj var der en hændelse i Nationalbankens SPI. Hændelsen betød, at deltagernes mulighed for selv at indlægge og udtage sikkerheder var begrænset i perioden fra 26.-29. maj.

Hændelserne er efterfølgende blevet fulgt op med tiltag, og der er draget læring ud af hændelsesforløbene, som tilsammen bidrager til at forebygge tilsvarende hændelser fremadrettet og styrker reaktionsevnen, hvis de alligevel skulle indtræffe.

TABEL 1

Betalinger i TARGET DKK mia. kr. pr. bankdag

	Mia. kr., gennemsnit pr. bankdag				
	2021	2022	2023	2024	2025
Interbankbetalinger	88,7	101,5	95,8	100,9	97,4
- Heraf kundebetalinger	16,6	20,7	19,8	21,5	20,3

	Antal, gennemsnit pr. bankdag				
	2021	2022	2023	2024	2025
Interbankbetalinger	8.544	10.344	10.639	10.665	10.228
- Heraf kundebetalinger	3.076	4.294	4.670	4.482	5.380

Anm.: Data for interbankbetalinger var før migreringen til TARGET DKK i påsken 2025, fra Kronos2.
Kilde: Danmarks Nationalbank.

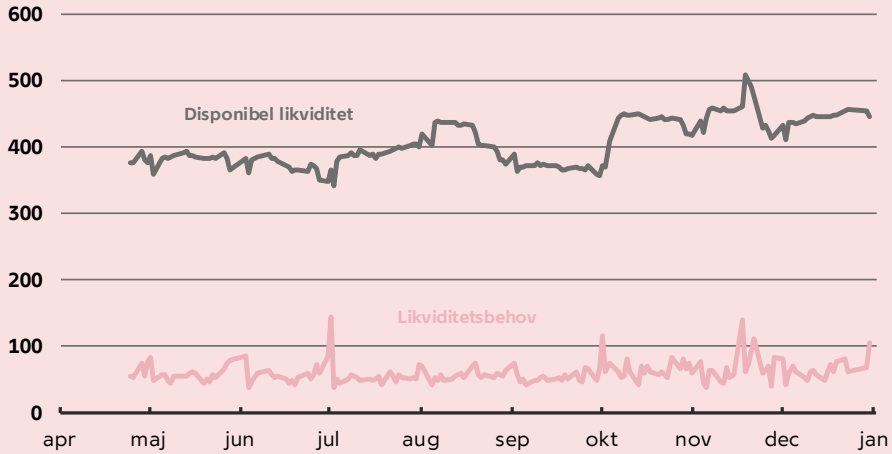
Likviditet

I 2025 har deltagerne fortsat haft rigelig likviditet til at gennemføre betalinger i Kronos2/TARGET DKK. Det dækker både interbankbetalinger, handel med værdipapirer i T2S, straksbetalinger i TIPS DKK og de betalinger, der følger af afviklingsinstruktioner fra de tilsluttede betalings- og afviklingssystemer (detailclearingerne og CLS), se figur 1.

FIGUR 1

Disponibel likviditet i forhold til likviditetsbehov for deltagerne i TARGET DKK i 2025

Mia. kr., daglige observationer



Anm.: Deltagernes disponible likviditet består af indestående på deres konti i TARGET DKK tillige med deres mulighed for at låne inden for dagen mod sikkerhed. Likviditetsbehovet opgøres ved at finde det tidspunkt på dagen, hvor deltagerne har brugt mest likviditet til at gennemføre deres betalinger. Der summeres herefter på tværs af deltagerne for at finde det maksimale samlede likviditetsbehov.
Kilde: Danmarks Nationalbank.

I den første tid efter flytningen af afviklingen af kronebetalinger til TARGET DKK var der hændelser, hvor deltagerne ikke havde reserveret nok likviditet til afviklingen af detailbetalinger. Hændelserne skyldtes ikke mangel på likviditet, men at deltagerne skulle tilpasse deres likviditetsstyring til ny funktionalitet. Læs nærmere om hændelserne i kapitel 3 om clearing og afvikling af detailbetalinger.

Til forskel fra det tidligere RTGS-system Kronos2, er der en kø-funktion i TARGET DKK, hvor betalinger lægges i kø, hvis en deltager ikke har tilstrækkelig likviditet til at afvikle betalingerne straks. Betalingerne bliver automatisk afviklet, når deltageren har dækning på kontoen. Kø-funktionen understøttes herudover af prioriteringsoptioner, hvor betalingerne kan tildeles prioriteterne normal, høj og hastende. TARGET DKK vil forsøge at afvikle de betalinger med den højeste prioritet først, dvs. at deltagernes likviditet prioriteres til de vigtigste betalinger. Kø-funktionaliteten bidrager til at reducere likviditetsrisiko ved at modvirke gridlock og sikre, at midlertidig likviditetsmangel ikke afbryder betalingsafviklingen.

Nationalbanken gennemfører jævnlige stresstest af likviditeten i overensstemmelse med krav i CPMI-IOSCO's principper for finansielle markedsinfrastrukturer, PFMI. Stresstesten omfatter som minimum scenarier, hvor de største deltagere ikke kan gennemføre deres betalinger, samt et stød til deltagernes mulighed for at trække på Nationalbankens facilitet til lån mod sikkerhed inden for dagen. Den første likviditetsstresstest med betalingsdata fra TARGET DKK forventes gennemført i første halvår af 2026.

Cyberrobusthed

Nationalbanken arbejder løbende med at styrke cyberrobustheden i sine systemer og forretningsprocesser. I juni 2025 godkendte Nationalbankens

ledelse en ny strategi for cyberrobusthed. Strategien opstiller målsætninger, der skal sætte retningen for, hvordan bankens cyberrobusthed skal styrkes frem mod 2028. Et af fokusområderne er at styrke bankens beredskab til håndtering af cyberhændelser yderligere, herunder håndtering af ekstreme, men plausible scenarier.

Purple team test er efter de første erfaringer i 2024 blevet et fast testværktøj, der bidrager til at styrke bankens evne til at opdage, reagere på og forhindre cyberangreb. I en purple team test deltager eksterne angrebsspecialister, red team, og bankens egne medarbejdere med ansvar for driften af de kritiske systemer, blue team. Under testene arbejder de to teams tæt sammen, hvilket bl.a. giver blue team indsigt i, hvordan et faktisk angreb på systemerne kan se ud. Identificerede forbedringspotentialer udbedres og gentestes så vidt muligt inden for testperioden. Purple team test er et supplement til Nationalbankens deltagelse i TIBER-DK testprogrammet.

Nationalbanken efterlever både SWIFT's Customer Security Controls Framework, CSCF, og SIAnet's Security Guidelines, som stiller krav om implementering af sikkerhedskontroller, der har til formål at styrke cyberrobustheden i tilfælde af cyberangreb. Det er et krav fra ECB, at centralbanker og kritiske deltagere har to uafhængige netværksforbindelser til TARGET Services via henholdsvis SWIFT og Nexi. Formålet med kravet er at sikre driftsstabilitet og robusthed, hvis den primære netværksforbindelse fejler.

Internationale standarder

I 2024 færdiggjorde Nationalbankens overvågning en vurdering af Calypsos efterlevelse af CPMI-IOSCO's Cyber Guidance. Calypso understøtter SPI og er et vigtigt system i forbindelse med afviklingen i danske kroner, idet systemet anvendes af deltagerne til at stille sikkerheder for til gengæld at kunne få kredit, som kan anvendes til betalingsafviklingen. I 2025 har Nationalbanken arbejdet med de forbedringspotentialer, der blev identificeret i vurderingen. Blandt andet er der oprettet en enhed på forretningsområdet, der skal styrke risikostyringen yderligere, herunder det proaktive arbejde med efterlevelse af de internationale standarder.

Der er tidligere foretaget en vurdering af Nationalbankens efterlevelse af CPMI's strategi for at reducere risikoen for kriminelle transaktioner i centrale betalingssystemer relateret til endpoint-sikkerhed. Som opfølgning på vurderingen er der blevet arbejdet med at styrke responsplaner og opdatere retningslinjer for, hvordan der hurtigt og effektivt skal reageres i tilfælde af mistanke om kriminelle transaktioner i TARGET DKK. Planerne testes med deltagerne i første halvår 2026. Derudover er risici ved endpoints og eksisterende kontrolforanstaltninger hos deltagerne ved at blive kortlagt. Kortlægningen skal være med til at øge forståelsen af, hvilke risici der er i økosystemet omkring TARGET DKK, og hvordan de adresseres. Arbejdet skal desuden være med til at danne ramme om en awareness-uddannelse, som Nationalbanken afholder med deltagerne i 2026.

3
Clearing og afvikling af detailbetalinger

Detailbetalinger i danske kroner cleares og afvikles i henholdsvis Sum- og Intradagclearingen og i systemet for straksbetalinger, TIPS DKK. Detailbetalinger er de betalinger, som borgere, virksomheder og offentlige myndigheder foretager mellem hinanden.

I Sumclearingen afvikles betalinger foretaget med bl.a. kort, indbetalingskort og Betalingsservice én gang i døgnet på bankdage. I Intradagclearingen afvikles konto-til-konto-overførsler, fx netbankoverførsler, 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, TARGET DKK, hvor beløbene udveksles mellem bankerne. Derefter bogføres betalingerne på kundernes konti i bankerne. Sum- og Intradagclearingen kaldes også batchclearingerne, idet betalingerne afvikles i batches, hvor betalingsdata behandles samlet i grupper.

I TIPS DKK afvikles straksbetalinger, dvs. konto-til-konto overførsler, på få sekunder døgnet rundt alle ugens dage. Det kan fx være netbankoverførsler og betalinger via MobilePay. TIPS står for *TARGET Instant Payment Settlement* og er en del af TARGET Services. I påsken 2025 blev afviklingen af straksbetalinger i danske kroner flyttet til TIPS DKK, som erstattede det tidligere system for straksbetalinger, Straksclearingen, der var ejet af Finans Danmark.

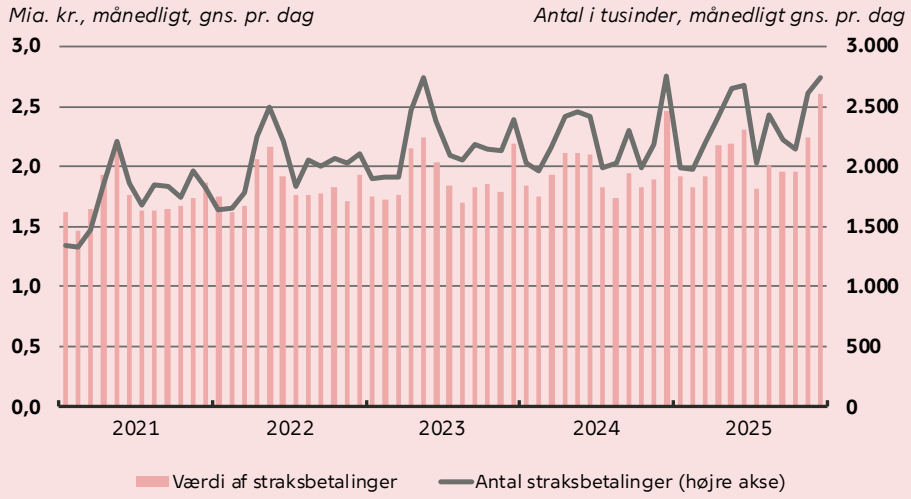
Som det fremgår af figur 2, har overgangen til TIPS DKK ikke ændret på udviklingen i brugen af straksbetalinger. Der ses fortsat en mindre stigning i både den gennemsnitlige værdi og antal fra 2024 til 2025, hvilket er i tråd med den generelt stigende tendens i perioden 2021-2025, hvor antallet er steget med 33,6 pct. Dette kan blandt andet relateres til øget anvendelse af MobilePay i internethandel og betalinger mellem private.[11]

[11] Se Danmarks Nationalbank, *Markedet for digitale detailbetalinger er under forandring*, *Danmarks Nationalbank Analyse*, nr. 2, februar 2025 (*link*).

FIGUR 2

Straksbetalinger i Danmark

Værdi og antal af straksbetalinger i perioden 2021-2025



Anm.: Data består frem til påsken 2025 af transaktioner gennemført i Strakscleringen og efter påsken 2025 af transaktioner gennemført i TIPS DKK.
Kilde: Mastercard Payment Services A/S, MPS, og Danmarks Nationalbank.

Værdien af transaktionerne i detailbetalingssystemerne udgjorde i gennemsnit 51,8 mia. kr. pr. bankdag i 2025, jf. tabel 2. Det er en stigning på 6,6 pct. sammenlignet med 2024.

TABEL 2

Værdi af transaktioner i detailbetalingssystemerne, 2021-2025, gennemsnit pr. bankdag

Mia. kr., gennemsnit pr. bankdag

	2021	2022	2023	2024	2025
Sumclearingen	20,5	21,3	21,2	21,8	22,6
Intradagclearingen	23,9	25	24	24,9	27,1
TIPS DKK*	1,7	1,8	1,9	1,9	2,1
I alt	46,1	48,1	47,1	48,6	51,8

Anm.:* Data består frem til påsken 2025 af transaktioner gennemført i Strakscleringen og efter påsken 2025 af transaktioner gennemført i TIPS DKK.
Kilde: Mastercard Payment Services A/S, MPS, og Danmarks Nationalbank

Batchclearingerne

Batchclearingerne ejes af Finans Danmark, forvaltes af e-nettet, og leveres af Mastercard Payment Services Danmark A/S, MPS.

Brug

Der er to deltagertyper i batchclearingerne, henholdsvis direkte- og indirekte deltagere.

Direkte deltagelse kræver bl.a., at deltageren har en hovedkonto og en afviklingskonto i Nationalbanken. Har deltageren ikke selv en konto, kan den være indirekte deltager. I så fald sker afviklingen af den indirekte deltagers betalinger via en direkte deltagers afviklingskonto. Ved udgangen af 2025 var der 33 direkte deltagere i batchclearingerne og 29 indirekte deltagere.

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 det medfører ændrede nettopositioner for øvrige deltagere, som derved risikerer ikke at modtage den forventede likviditet.

I 2025 har der været flere henlæggelser som følge af manglende reserveret likviditet på deltagernes konti. Størstedelen af henlæggelserne forekom i perioden umiddelbart efter overgangen fra Kronos2 til TARGET DKK, hvor deltagerne i forbindelse med migreringen skulle tilpasse deres likviditetsstyring, herunder med øget fokus på løbende, aktiv disponering af likviditet gennem dagen. Tidligere kunne deltagerne i højere grad benytte automatiserede værktøjer til styring af likviditet.

Finans Danmark har forud for migreringen haft fokus på at uddanne sektoren i likviditetsstyring på TARGET DKK og har som opfølgning på henlæggelserne været i dialog med de berørte deltagere.

Drift

I 2025 har driftsstabiliteten for Sum- og Intradagclearingen været tilfredsstillende.

Der har været en enkelt større hændelse i Sumclearingen i forbindelse med, at en gruppe banker overgik fra at være direkte til indirekte deltagere. Denne overgang medførte en fejlkonfiguration i produktionsmiljøet, som betød, at nogle betalinger blev forsinket med to dage.

Overvågningen vurderer, at Finans Danmarks opfølgning på hændelsen og henlæggelserne har været tilfredsstillende.

Internationale standarder og cyberrobusthed

Finans Danmark arbejder løbende på at styrke cyberrobustheden i batchclearingerne og har i 2025 fortsat arbejdet med at efterleve den sidste åbne anbefaling fra Nationalbankens vurdering efter CPMI-IOSCO's Cyber Guidance fra 2022. Finans Danmarks primære fokus har været en fortsat indsats for at videreudvikle og styrke evnen til at kunne genoprette og/eller opretholde driften inden for fastsatte tidsrammer efter cyberrelaterede hændelser – herunder også i ekstreme, men plausible scenarier. Som led i dette arbejde blev der i 2. halvår 2025 udarbejdet et scenariekatalog, der systematisk kobler hændelsesbeskrivelser, aktiver, trusler, foranstaltninger og nødplaner. Den første praktiske test baseret på scenariekataloget blev gennemført i 3. kvartal 2025 i samarbejde med MPS.

Et yderligere element i Finans Danmarks arbejde med cyberrobusthed er Cybersikkerhedshåndbogen for batchclearingerne, som fastsætter it-sikkerhedskrav til datacentralerne og de deltagende banker. Håndbogen dækker de otte indsatsområder i CPMI-IOSCO's Cyber Guidance, jf. boks 3.

Finans Danmark følger årligt op på deltagernes efterlevelse af cybersikkerhedshåndbogen[12] og anvender resultaterne som grundlag for løbende dialog og videre arbejde. Finans Danmarks opfølgning sker både i tværgående fora og bilateralt med de enkelte banker og datacentraler.

Nationalbankens overvågning drøfter årligt risikostyring og beredskab med systemejerne. I 2025 har overvågningen og Finans Danmark blandt andet været i dialog om vigtigheden af, at Finans Danmark fortsat prioriterer og sikrer en tilstrækkelig bemanding i sin beredskabsplanlægning, så både egne interne beredskaber og FSOR's kriseberedskab kan håndteres effektivt ved en samtidig aktivering.

Overvågningen har i 2025 også drøftet arbejdet med at sikre tilstrækkelig redundans i netværksforbindelser og forberedelser til at kunne indføre kvantesikker kryptering med Finans Danmark.

Ændringer i ejerskabsmodellen for batchclearingerne

Finans Danmark har i 2025 igangsat arbejde med etablering af et datterselskab, Clearing Services P/S, der skal overtage ejerskabet af Sum- og Intradagclearingen. Clearing Services bliver som ejer af clearingerne ansvarlig for den daglige drift og vedligeholdelse samt for, at de internationale standarder for finansielle markedsinfrastrukturer efterleves.

Finans Danmark finder det nødvendigt at adskille sine opgaver som henholdsvis clearinghus og interesseorganisation som følge af en ændring i Finality-direktivet[13], der muliggør, at betalingsinstitutter og e-pengeinstitutter kan få adgang til detailclearingsystemerne. Formålet med den nye ejerskabsmodel er at skabe en klarere adskillelse mellem medlemmer af interesseorganisationen og deltagere i clearingerne.

Nationalbankens overvågning vil forud for overgangen til den nye ejerskabsmodel gennemgå Clearing Services' efterlevelse af udvalgte dele af CPMI-IOSCO's Principles for Financial Market Infrastructures, PFMI, herunder princip 2 om governance og princip 15 om forretningsrisiko.

Systemændringer i clearinginfrastrukturen i 2025

Finans Danmark har i regi af Sektorprogrammet for Fremtidens Betalingsinfrastruktur udarbejdet en langsigtet, strategisk plan for modernisering af den danske clearinginfrastruktur, jf. boks 4. Som led heri har Finans Danmark indgået en aftale med EBA CLEARING om at etablere en ny STEP2 DKK-clearingløsning, der skal erstatte den eksisterende Intradagclearing. Med etableringen af STEP2 DKK løftes en del af batchclearinginfrastrukturen til en standardplatform, der er NPC-kompatibel (se boks 4). Finans Danmark forventer, at der er øget resiliens i den nye clearing. Der er på nuværende tidspunkt ikke taget stilling til modernisering af Sumclearingen. Nationalbankens overvågning har peget på vigtigheden af, at der også udarbejdes en plan for denne.

[12] I 2024 blev elementer af Cybersikkerhedshåndbogen opdateret med nye krav om, at datacentralerne og de deltagende banker skal arbejde mere systematisk med robusthed, nødplaner og genoprettelsesmuligheder, herunder beredskabsplaner og nødprocedurer. Formålet er at sikre vedvarende sektor-fokus på disse områder. Implementeringsperioden løb til udgangen af 2025, og kravene er nu fuldt gældende.

[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 uden at skulle gå igennem en bank. Dog har betalingsinstitutterne udelukkende adgang til afviklingskonti i Nationalbanken og får ikke adgang til at anvende de pengepolitiske instrumenter.

Finans Danmark forventer, at test og udviklingsaktiviteter vil være afsluttet for den tekniske del af STEP2 DKK-løsningen i november 2026, og at STEP2 DKK-clearingen tages i brug første halvår 2027. Nationalbankens overvågning følger STEP2 DKK-projektet tæt, og har særligt fokus på governance, risikostyring og beredskab samt Clearing Services' parathed til at varetage den nye STEP2 DKK-clearing.

Fokus på at nedbringe digital svindel

Som led i Sektorprogrammet for Fremtidens Betalingsinfrastruktur igangsatte Finans Danmark i 2024 arbejdet med at vælge en leverandør til en Verification of Payee-tjeneste, VoP, til den danske sektor. Initiativet blev sat i værk som følge af ny EU-lovgivning, der blandt andet stiller krav om, at en betalers betalingstjenesteudbyder skal tilbyde en service, som verificerer identiteten af den modtager, som betaleren ønsker at sende en standard- eller straksbetaling[14]. I april 2025 indgik Finans Danmark en aftale med SurePay om at varetage rollen som national udbyder af VoP-tjenesten[15]. VoP-tjenesten har været operationel for eurobetalinger siden oktober 2025 og forventes at være operationel for betalinger i danske kroner i første halvår 2027. VoP-tjenesten er et centralt redskab i indsatsen mod digital svindel og misbrug.

Finans Danmark arbejder også med etableringen af en fælles fastfrysningsordning, der skal gøre det muligt at stoppe svindeltransaktioner, før de når at blive flyttet videre fra svindleres konti[16]. I 2025 igangsatte Finans Danmark en analyse af mulighederne for en fælles løsning for den finansielle sektor. Arbejdet pågår fortsat, idet realiseringen blandt andet forudsætter en lovændring.

BOKS 4

Sektorprogram for Fremtidens Betalingsinfrastruktur

Der er i regi af Finans Danmark udarbejdet en samlet sektorplan, hvis mål er at sikre en fortsat modernisering og modstandsdygtighed af den danske detailbetalingsinfrastruktur. Arbejdet med sektorplanen er forankret i et sektorprogram under Finans Danmarks bestyrelse med en bredt sammensat styregruppe, drevet af e-nettet i samarbejde med Finans Danmark.

Som led i sektorprogrammet har Finans Danmark udarbejdet en langsigtet, strategisk plan for den danske clearinginfrastruktur, herunder etableringen af STEP2 DKK, som skal erstatte Intradagclearingen. Initiativet udspringer bl.a. af en sektorbeslutning om at anvende Nordic Payments Councils, NPC[1], betalingsstandarder. 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.

[1] 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 til konteksten i lokale betalingslandskaber i Norden.

[14] Se ECB vedrørende EU-lovgivningen for standardkredit og straksoverførsler, Instant Payment Regulation, IPR, marts 2024 (*link*).
[15] SecurePay, Denmark becomes the first non-Euro country to implement a nationwide VOP solution, april 2025 (*link*).
[16] Se Finans Danmark, *Her er 18 anbefalinger, der kan bremse it-svindlen i Danmark*, november 2024 (*link*).

TIPS DKK

Nationalbanken er systemejer af TIPS DKK. TIPS DKK overvåges som en del af TARGET DKK.

Brug

Der er i alt 53 deltagere i TIPS DKK. Heraf deltager 25 indirekte og afvikler derfor deres betalinger via en direkte deltagers TIPS-konto i TARGET DKK.

Likviditet

Gennemførelse af straksbetalinger forudsætter, at deltageren har stillet den nødvendige likviditet til rådighed i TIPS DKK. Deltagerne overfører likviditet fra deres hovedkonto i TARGET DKK til en afviklingskonto dedikeret til straksbetalinger.

Afviklingen af straksbetalinger sker 24/7/365, men overførsel af likviditet til og fra en deltagers TIPS afviklingskonto kan kun ske i TARGET DKK's åbningstid, som er klokken 19.30-17.00 på bankdage. Deltagerne skal derfor sørge for at have overført tilstrækkelig likviditet til deres TIPS konto forud for weekender og helligdage, hvor øvrige services er lukkede, og likviditetsjustering derfor ikke er muligt.

Drift

I december var der en hændelse hos et datacenter, der medførte, at mange borgere ikke kunne gennemføre straksbetalinger i flere timer. Nationalbanken aktiverede beredskabet for TIPS, og der blev afholdt møder i beredskabet, indtil hændelsen var afsluttet. TARGET DKK, herunder TIPS, var ikke berørt af hændelsen, hvilket betød, at afviklingen af betalinger forløb normalt under hændelsen. Hændelsen skyldtes kapacitetsmangel hos datacentret, der medførte, at straksbetalingerne ikke kunne behandles. Der er efterfølgende gjort udbedrende tiltag ved datacentret, der skal sikre mod lignende hændelser fremover.

Udvikling af et straksbetalingssystem på tværs af valutaer

Siden 2024 har Nationalbanken i samarbejde med ECB og Sveriges Riksbank arbejdet på etableringen af TIPS Cross-Currency, som skal muliggøre grænseoverskridende straksbetalinger i euro, danske kroner og svenske kroner via TIPS. Formålet er at give borgere og virksomheder adgang til hurtige, billige og sikre straksbetalinger på tværs af valutaer. Den første version af den tekniske løsning blev stillet til rådighed i november 2025, og arbejdet videreføres i 2026.

4
Detailbetalinger

Når borgere og virksomheder i Danmark køber varer og betaler regninger, bruger de for det meste digitale betalingsløsninger. De mest anvendte betalingsløsninger i Danmark er Dankort, internationale betalingskort fra Visa og Mastercard, MobilePay, Betalingsservice og konto-til-konto-overførsel via netbank eller mobilbank. I 2025 blev der foretaget betalinger for ca. 52 mia. kr. i gennemsnit pr. dag med digitale betalingsløsninger[17].

Nationalbanken overvåger Dankort og Betalingsservice. Overvågningen af disse betalingsløsninger er baseret på PISA-standarderne, se boks 1. Konto-til-kontooverførsler overvåges også. Det sker som en del af Nationalbankens overvågning af Detailclearingerne, se kapitel 3 *Clearing og afvikling af detailbetalinger*. Visa og Mastercard overvåges af Eurosystemet.

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.

Dankort

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

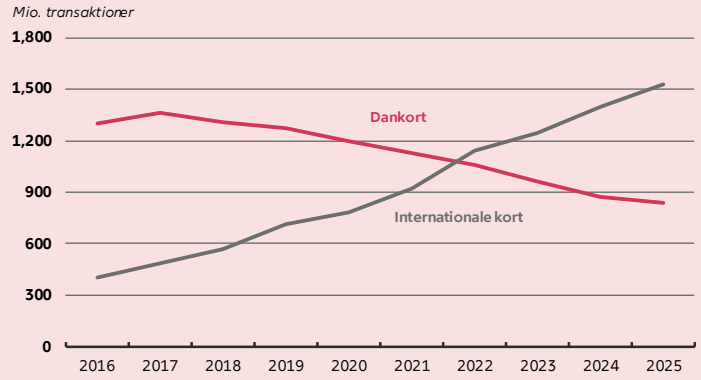
Siden 2017 er der sket et væsentligt fald i anvendelsen af Dankort. Denne udvikling er vendt i 2025. Der er fortsat et fald for året som helhed, men faldet er lavere end de tidligere år, og i fjerde kvartal af 2025 er brugen af Dankort steget. Faldet i brugen af Dankort skyldes især øget anvendelse af Visa og Mastercard, se figur 3 og 4. Dankort spiller dog fortsat en central rolle for danske detailbetalinger.

[17] Dette omfatter alle betalinger, der gået gennem de danske detailclearinger, herunder kortbetalinger, MobilePay, kontooverførsler, regningsbetalinger gennem Betalingsservice, Leverandørservice og FI-kort samt løn- og pensionsudbetalinger mv. gennem Overførselsservice. Opgørelsesmetoden er en anden end for tidligere års rapporter, hvorfor tallene ikke kan sammenlignes direkte.

FIGUR 3

Brugen af Dankort og internationale kort i Danmark (antal)

Samlet antal transaktioner foretaget med betalingskort i Danmark

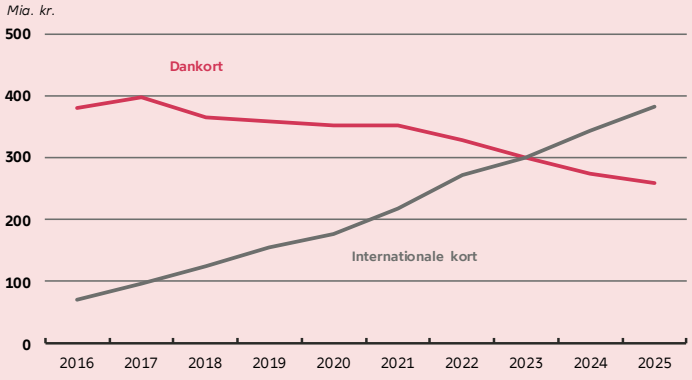


Anm.: Opgørelsen dækker kortbetalinger i fysisk handel, på internettet og selvbetjeningsmiljøer i Danmark.
Kilde: Nets og Danmarks Nationalbank.

FIGUR 4

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.

Det er særligt brugen af internationale kort til at gennemføre mobilbetalinger via Wallet-løsningerne Apple Pay og Google Pay, der driver udviklingen på kortbetalingsområdet.[18] Fra starten af 2025 har Nets stillet krav om, at kortudstedere/banker, der gør det muligt at anvende et kort co-badged med Dankort i en Wallet-løsning, skal sikre, at Dankortsiden også kan anvendes. Udsteder en bank et Visa/Dankort, hvor Visa-siden kan anvendes i en Wallet, skal banken altså sørge for, at Dankort-siden kan anvendes i samme. Alle danske banker lever nu op til disse krav for så vidt angår ApplePay[19].

Folketinget vedtog i juni 2025 et lovforslag, der præciserer, at betalingssystemer skal give udbydere af betalingstjenester adgang til deres betalingssystemer på objektive, ikke-diskriminerende og proportionale vilkår[20]. Det indebærer blandt andet, at Nets skal give andre indløsere adgang til at indløse Dankort-betalinger. Forligskredsen bag Dankortet (dvs. Regeringen, SF, Konservative, Radikale Venstre og Dansk Folkeparti) indgik i juni 2025 desuden en aftale om styrkelse af Dankortet, der skal sikre udstedelse af markant flere Dankort. Det skal bl.a. ske gennem udvikling af Dankort med saldokontrol og et erhvervskort samt mulighed for finansiering af andre tiltag, der sikrer en fremtidig videreudvikling af Dankort. Aftalen skal i den forbindelse danne grundlag for, at Nets kan få dækket de omkostninger, der er forbundet med at udvikle de nye funktioner og tiltagene til at give nye indløsere adgang til at indløse Dankort-betalinger[21]. Nationalbankens overvågning har i 2025 drøftet konsekvenserne af disse ændringer med Nets. Drøftelserne fortsætter i 2026 med fokus på efterlevelse af PISA-standarderne, herunder at Nets etablerer en passende styring af risici forbundet med, at andre virksomheder end Nets indløser Dankort-transaktioner.

[18] Se Danmarks Nationalbank, *Markedet for digitale betalinger forandrer sig, Danmarks Nationalbank Nyt*, februar 2025 *(link)*.
[19] Google Pay understøtter på nuværende tidspunkt ikke betaling med co-badged betalingskort såsom Visa/Dankort. Bankernes arbejde med at efterleve Nets' krav for Google Pay er derfor ikke påbegyndt endnu.
[20] LOV nr. 711 af 20/06/2025 *(link)*.
[21] Erhvervsministeriet, *Ny aftale skal styrke Dankortet,* juni 2025 *(link)*.

Drift

Driftsstabiliteten i Dankort-systemet har i 2025 været tilfredsstillende med fuld oppetid på nær én større hændelse.

19. juli 2025 var der en større hændelse i Nets' kortbetalingssystemer, herunder også Dankort-systemet. Hændelsen skyldtes en overbelastning af en database i Nets' kortplatform og førte til en nedetid på ca. 3,5 time og lange svartider i Nets' systemer, hvor kun en begrænset del af korttransaktionerne blev gennemført. Herudover medførte hændelsen, at nogle betalinger blev bogført/reserveret flere gange, og nogle betalinger blev bogført på forkerte konti. Endelig var kommunikationskanalerne på Nets' hjemmeside nede, da den blev overbelastet af den store trafik, og Nets var ikke i stand til at håndtere de mange henvendelser. Nets' nødløsning i form af offlinekortbetalinger fungerede som forventet under nedbruddet, men mange betalingsmodtagere var ikke klar over, hvordan de skulle anvende løsningen.

Nationalbanken har fulgt op på håndteringen af hændelsen sammen med Nets. Drøftelserne har bl.a. fokuseret på identifikation af årsagen til hændelsen, herunder hvordan der kunne ske forkert bogføring af betalinger, Nets' leverandørstyring samt krisehåndtering og -kommunikation. Nationalbanken har i den forbindelse også deltaget som observatør i den IT-inspektion, som Finanstilsynet afholdt hos Nets i december 2025. Inspektionen havde blandt andet til formål at følge op på Nets' håndtering af hændelsen. Inspektionen er endnu ikke afsluttet.

Nationalbanken har i forbindelse med opfølgningen på hændelsen også drøftet overgangen til en ny driftsplatform for kortbetalinger med Nets. Nets forventer, at Dankortbetalinger vil kunne behandles på den nye platform i 2027, og det er Nets' forventning, at platformen vil medføre en øget robusthed i Dankortsystemet.

Endelig har Nationalbankens overvågning fulgt Nets' arbejde med yderligere at udbrede muligheden for at gennemføre offlinekortbetalinger, herunder også for kortbetalinger med mobiltelefonen gennem fx ApplePay eller GooglePay. Dette er en central del af arbejdet med det nationale betalingsberedskab[22], der skal sikre, at borgere kan betale for et basalt forbrug af fødevarer og medicin i mindst en uge, hvis de digitale betalingsløsninger ikke fungerer som normalt. Nationalbanken har i den forbindelse også haft fokus på, hvordan erfaringerne fra hændelsen i juli 2025 indgår i Nets' videre arbejde med at styrke offlineberedskabet både hos Nets selv og hos Nets' kunder, dvs. butikker og andre betalingsmodtagerne.

Misbrug

Misbruget af Dankort er fortsat lavt. Det udgjorde i alt ca. 28 mio. kr. i 2025, svarende til ca. 0,1 promille af de samlede Dankort-betalinger. Udviklingen fra 2024 til 2025 har overordnet været stabil, og det samlede misbrug for året er stort set uændret.

Misbrug relateret til tyveri eller tab af kort udgør fortsat størstedelen af misbruget. Denne type misbrug beløb sig til ca. 21 mio. kr. i 2025, mens misbruget ved handel på internettet var på ca. 7 mio. kr.

Internationale standarder og cyberrobusthed

Nationalbanken vurderede i 2024 Dankort efter PISA's krav til risikostyring og beredskab og gav i den anledning anbefalinger til Nets' arbejde med disse

[22] Dette arbejde ledes af Nationalbanken gennem sin varetagelse af formandskabet for Betalingsrådet. Læs mere om Betalingsrådet på Nationalbankens hjemmeside (*link*).

områder. Nationalbanken har bl.a. anbefalet, at Nets styrker sine procedurer for arbejdet med at håndtere ekstreme, men plausible scenarier. Det skal medvirke til, at Nets har stærke rammer for at udvikle og vedligeholde sit cyberberedskab. Nets har i 2025 arbejdet med anbefalingerne, og Nationalbanken og Nets drøfter nu resultaterne af dette arbejde. Nationalbanken vil på den baggrund vurdere, om Nets har efterlevet anbefalingerne. Nationalbanken vil i den forbindelse inddrage konklusioner fra Finanstilsynets IT-inspektion i vurderingen.

Nationalbanken har i 2025 også drøftet arbejdet med at sikre tilstrækkelig redundans i netværksforbindelser og forberedelser til at kunne indføre kvantesikker kryptering med Nets.

Betalingsservice og PBS-clearingen

Nationalbankens overvågning af Betalingsservice og PBS-clearingen er rettet mod Mastercard Payment Services Denmark A/S, MPS, der er systemejer for Betalingsservice og PBS-clearingen. PBS-clearingen er en delclearing, der anvendes til at samle transaktioner fra MPS' egne produkter, herunder Betalingsservice[23], samt korttransaktioner fra Nets, før de indgår i Sumclearingen, se kapitel 3 *Clearing og afvikling af detailbetalinger*.

Drift og misbrug

Driftsstabiliteten var høj i Betalingsservice og PBS-clearingen i 2025. Der var ingen driftsforstyrrelser i Betalingsservice. Der har ligeledes været fuld oppetid i PBS-clearingen og kun en enkelt mindre forsinkelse i juni måned pga. manglende rettidig leverance af afviklingsfiler for kortbetalinger fra Nets. Beredskabsproceduren i PBS-clearingen fungerede i den forbindelse som forventet.

Der var ikke misbrug af Betalingsservice i 2025.

Internationale standarder og cyberrobusthed

Nationalbanken har i 2025 fulgt MPS' arbejde med efterlevelse af PISA-standarderne. Det er Nationalbankens indtryk, at MPS har arbejdet målrettet med at sikre Betalingsservices efterlevelse af PISA-standarderne. Nationalbanken har særligt fulgt MPS' arbejde med beredskaber og evnen til at håndtere ekstreme, men plausible cyberscenarier. Disse drøftelser fortsætter i 2026.

MPS har i 2025 styrket sin interne organisering for at sikre løbende efterlevelse af PISA-standarderne.

Nationalbanken og MPS har i 2025 også drøftet MPS' arbejde med at sikre tilstrækkelig redundans i netværksforbindelser og med at undersøge mulighederne for at kunne indføre kvantesikker kryptering.

[23] Udover Betalingsservice indgår Leverandørservice og Overførselsservice i PBS-clearingen.

5
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[24], 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 finder den endelige afvikling af værdipapirhandlerne først 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. Handler mellem bankerne og deres egne kunder afvikles fortsat i ES-CPH's eget afviklingssystem[25]. ES-CPH har i de seneste år gradvist indskrænket brugen af ES-CPH-afviklingen og vil helt udfase denne, jf. afsnittet nedenfor om systemændringer.[26]

ES-CPH står også for håndtering af periodiske betalinger, emissioner, indfrielser mv.[27] ES-CPH er den eneste virksomhed i Danmark med tilladelse fra Finanstilsynet til at drive værdipapircentral.

Brug

ES-CPH har 88 deltagere, hvoraf 35 er udenlandske markedsdeltagere, herunder fire centrale modparter (Central Counterparties, CCP'er)[28]. 45 af deltagerne i ES-CPH har også en konto i TARGET DKK, så de kan overføre likviditet til deres afviklingskonto på T2S. Det er også muligt at overføre likviditet til afviklingskonti på T2S via en co-manager i TARGET DKK uden selv at være deltager i TARGET DKK, se kapitel 2, *Interbankbetalinger og den centrale afvikling af betalinger i danske kroner*[29].

I 2025 blev der i gennemsnit afviklet ca. 102.000 handler om dagen i danske kroner gennem ES-CPH, hvilket er stigning på 9,1 pct. i forhold til 2024, se tabel 3. Det skyldes en stigning i antallet af handler med aktier og investeringsforeningsbeviser. Værdien af de afviklede handler var i gennemsnit ca. 232 mia. kr. pr. bankdag, hvilket er stigning på 4,4 pct. i forhold til 2024, se

[24] 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.
[25] Opdelingen af afviklingen på henholdsvis T2S og ES-CPH-afviklingen kaldes også den lagdelte afviklingsmodel. Afvikling af værdipapirhandler via den lokale ES-CPH-afvikling sker for danske kroner og euro kun som såkaldte free-of-payment-handler, FoP. Afvikling af handler i svenske kroner sker fortsat med udveksling af penge mellem deltagerne.
[26] Se også nærmere om denne udvikling i afsnittet *Systemændringer* nedenfor.
[27] Også kaldet corporate actions.
[28] 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.
[29] Før påsken 2025 skete denne overførsel af likviditet på samme vis blot fra konti i Kronos2 i stedet for TARGET DKK. Se kapitel 2, *Interbankbetalinger*.

tabel 3. Det skyldes særligt en stigning i værdien af handler med obligationer og investeringsforeningsbeviser. Stigningen i antallet af handler kan i følge ES-CPH bl.a. henføres til den øgede aktivitet i markedet som følge af de skiftende amerikanske toldudmeldinger.

TABEL 3

Antal og værdi af værdipapirhandler

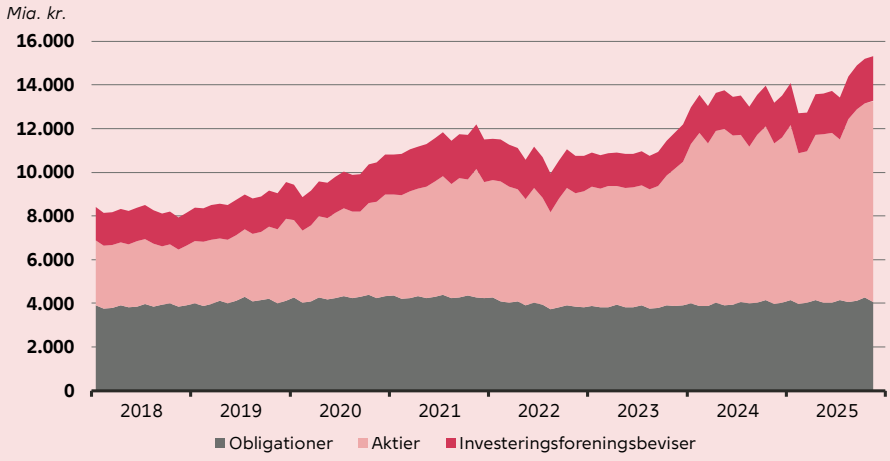
	I alt		Obligationer		Aktier		Investerings-foreningsbeviser	
År, Gennemsnit pr. dag	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.
2018	65,5	168,5	2,6	119,0	29,4	40,8	33,5	8,8
2019	67,0	223,1	4,2	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
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
2025	102,1	231,7	3,8	159,6	46,4	62,3	51,9	9,8

Kilde: ES-CPH.

Markedsværdien af værdipapirer opbevaret i ES-CPH steg i 2025 med 16 pct., se figur 5. Stigningen skyldes særligt stigninger i værdien af aktier og investeringsforeningsbeviser.

FIGUR 5

Markedsværdi af værdipapirer opbevaret i ES-CPH



Kilde: ES-CPH.

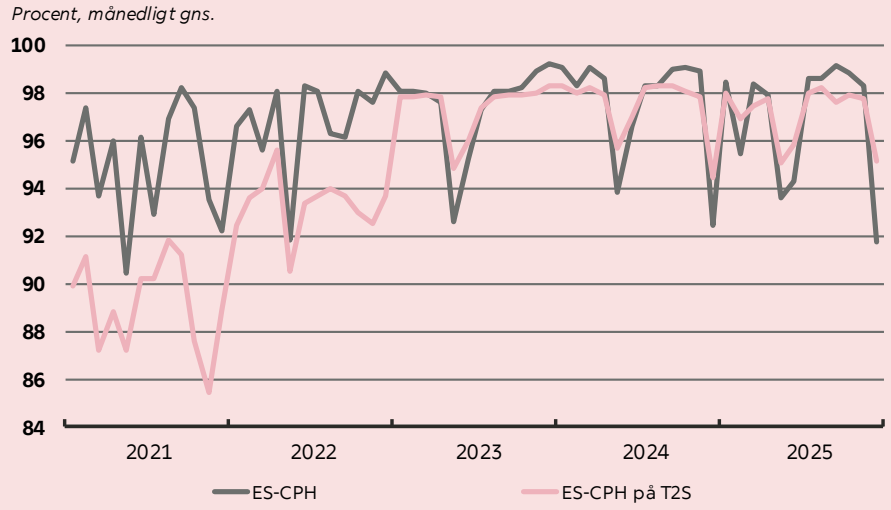
Afviklingsprocent

Afviklingsprocenten måler andelen af handelsomsætningen, der afvikles rettidigt, det vil sige senest to dage efter handlerne er indgået.[30]

Figur 6 viser afviklingsprocenten for henholdsvis ES-CPH's afvikling på T2S og for ES-CPH's eget system. Det er tilfredsstillende, at afviklingsprocenten i 2025 generelt er fastholdt på et højt niveau. Dette er med undtagelse af februar måned, hvor der var et fald i afviklingsprocenten grundet hændelsen i TARGET Services 27. februar, jf. nedenfor. Udsvingene i maj, juni og december måned skyldes, at T2S har åbent på danske banklukkedage, og afspejler ikke et fald i afviklingsdisciplinen hos deltagerne.[31]

FIGUR 6

Afviklingsprocent



Kilde: ES-CPH.

Drift

Driftsstabiliteten i afviklingen af danske værdipapirhandler i ES-CPH-afviklingen har i 2025 overordnet været tilfredsstillende. Tre større hændelser i TARGET Services medførte en væsentlig påvirkning af driften hos ES-CPH. Hændelserne fandt sted 27. februar, 13.-14. marts og 5. maj 2025, og alle tre hændelser skyldtes problemer med kommunikationen mellem T2S og de tilknyttede værdipapircentraler og deltagere. Hændelserne gjorde det nødvendigt for ES-CPH at spærre afviklingen af handler med en række værdipapirer og medførte forsinkelser af lukningen af afviklingsdøgnet og afviklingen af værdipapirhandler. Håndteringen af hændelserne indebar et større arbejde hos ES-CPH for at kunne gennemføre korrekt afstemning af deltagernes værdipapirkonti.

[30] Ifølge CSDR, artikel 5, skal værdipapirhandler afvikles senest to dage efter handelsdagen. Fra 11. oktober 2027 forkortes afviklingstiden, så handler skal afvikles senest dagen efter handelsdagen.
[31] På danske banklukkedage, hvor T2S samtidig har åbent, sker der et fald i afviklingseffektiviteten pga. den manglende aktivitet hos de danske deltagere. Faldet i maj måned skyldes 30. maj, dagen efter Kristi himmelfartsdag. Faldet i juni måned skyldes Grundlovsdag. Faldet i december skyldes 24. og 31. december. På disse dage har T2S åbent. I år, hvor de særlige danske banklukkedage falder på en weekend, skaber det ikke udsving i afviklingsprocenten.

Nationalbankens overvågning har fulgt op på håndteringen af hændelserne med ES-CPH og vurderer, at opfølgningen på hændelserne har været tilfredsstillende.

Se nærmere beskrivelse af hændelserne i T2S 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.

Overvågningen af ES-CPH koordineres tæt med Finanstilsynet, da overvågningen berører mange af de samme elementer, som Finanstilsynets tilsyn med ES-CPH's efterlevelse af kravene i den fælleseuropæiske lovgivning om værdipapircentraler, CSDR[32]. Nationalbanken bidrager i den forbindelse til Finanstilsynets løbende evalueringer af, om ES-CPH lever op til kravene i CSDR (også kaldet review and evaluation). Nationalbanken har i dette arbejde særligt fokus på ES-CPH's styring af operationelle risici og arbejdet med beredskaber, særligt til at håndtere ekstreme, men plausible scenarier.

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*.

Nationalbanken foretog i 2020 en vurdering af ES-CPH efter CPMI-IOSCO's Cyber Guidance.[33] Vurderingen viste, at ES-CPH efterlevede Cyber Guidance på de fleste områder. På få, men centrale, områder gav Nationalbanken anbefalinger til ES-CPH om, hvordan arbejdet med cyberrobustheden burde styrkes. Det gælder bl.a. ES-CPH's procedurer for arbejdet med at håndtere ekstreme, men plausible cyberscenarier. Det skal medvirke til, at ES-CPH har stærke rammer for at udvikle og vedligeholde sit cyberberedskab. Nationalbanken har vurderet, at ES-CPH i 2025 har efterlevet yderligere to af anbefalingerne. En enkelt af de oprindeligt 16 anbefalinger er fortsat åben.

Nationalbanken følger løbende ES-CPH's arbejde med at forbedre cyberrobustheden i systemerne. Nationalbanken og ES-CPH har i 2025 drøftet vigtigheden af, at ES-CPH i sin beredskabsplanlægning sikrer en tilstrækkelig bemanding til at kunne håndtere en samtidig aktivering af både sine egne interne beredskaber og FSOR's kriseberedskab. Nationalbanken og ES-CPH har også drøftet behovet for at sikre en bedre integration af eskalation til FSOR's kriseberedskab i sine egne interne beredskabsplaner.

Nationalbanken og ES-CPH har i 2025 også drøftet ES-CPH's arbejde med at sikre tilstrækkelig redundans i netværksforbindelser og ES-CPH's forberedelser til at kunne indføre kvantesikker kryptering.

Systemændringer

I 2024 begyndte ES-CPH at anvende Euronext-koncernens corporate actions-platform, CA4U, til håndtering af corporate actions for obligationer. ES-CPH besluttede i 2025 at udsætte den planlagte anvendelse af CA4U for andre typer værdipapirer fra ultimo 2025 til september 2026.

[32] 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 (CS'er), som driver afviklingsinfrastrukturen.
[33] Nationalbankens vurdering af ES-CPH efter Cyber Guidance er ikke offentliggjort.

Europa-Parlamentet og Ministerrådet vedtog i oktober 2025 Europa-Kommissionens forslag om at forkorte afviklingstiden for værdipapirhandler til dagen efter handelsdagen (også kaldet T+1)[34]. Dette vil kræve en række ændringer i den nuværende markedspraksis og i IT-systemer i den finansielle sektor. Forud for overgangen til T+1-afvikling 11. oktober 2027 vil ES-CPH foretage tilpasninger af den lokale afviklingsplatform, så den vil kunne understøtte den forkortede afviklingstid. ES-CPH har tidligere planlagt, at den lagdelte afviklingsmodel skulle udfases i løbet af 2027. ES-CPH blev i 2025 enig med afviklingsdeltagerne om at udskyde udfasningen af den lokale afviklingsplatform til august 2028. Herefter skal alle værdipapirhandler afvikles på T2S. Efter august 2028 vil ES-CPH efter planen have fuldført sin del af Euronext-koncernens såkaldte *convergence programme*, der indebærer, at alle fem CSD'er skal køre på samme tekniske platform.[35]

[34] Europa-Parlamentets og Rådets forordning (EU) 2025/2075 af 8. oktober 2025 om ændring af forordning (EU) nr. 909/2014 for så vidt angår en kortere afviklingscyklus i Unionen (*link*).
[35] Udover ES-CPH indgår CSD'erne i Grækenland, Italien, Norge og Portugal i Euronext-koncernen.

6
Betalinger og værdipapirafvikling i euro

Afvikling af betalinger og værdipapirhandler i euro sker gennem TARGET Services. TARGET Services består af tre services, henholdsvis T2, T2S og TIPS. T2 er det fælleseuropæiske RTGS-system til afvikling af store og tidskritiske betalinger samt til overførsel af likviditet til afvikling i andre systemer, herunder T2S og TIPS. T2S, TARGET2-Securities, er det fælleseuropæiske system til afvikling af værdipapirhandler. TIPS er afviklingssystemet for straksbetalinger.

TARGET Services kan håndtere flere valutaer, herunder danske kroner. 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

I alt er der omkring 1.000 banker, der anvender T2 til at gennemføre betalinger i euro, herunder 18 danske banker og filialer af udenlandske banker i Danmark. I 2025 gennemførte de danske deltagere interbankbetalinger for i gennemsnit 5,4 mia. euro om dagen. De danske deltagere bruger hovedsageligt T2 til at gennemføre koncerninterne betalinger og betalinger til udenlandske deltagere. Der udveksles flest euro med deltagere i Tyskland, Frankrig, Finland og Belgien.

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. Der er 11 danske deltagere, som har en T2S-afviklingskonto i TARGET Services via Nationalbanken, og benytter denne til betaling eller modtagelse af euro i forbindelse med T2S-afviklingen.

Der er lige nu ingen danske deltagere, der tilbyder straksbetalinger i euro via TIPS, men det vil ændre sig fra 2027, hvor deltagere, som tilbyder kreditoverførsler i euro også skal tilbyde straksbetalinger i euro, jf. forordningen om straksbetalinger. Forordningen om straksbetalinger, IPR, blev vedtaget af Europa-Parlamentet og Rådet 13. marts 2024 og har til formål at fremskynde udrulningen af straksbetalinger i Europa. Forordningen omfatter kreditoverførsler i euro inden for EU.

Drift

Driftsstabiliteten i TARGET Services har ikke været helt tilfredsstillende i 2025. Der har været flere større hændelser, som både har påvirket afviklingen af betalinger og værdipapirhandler i euro og afviklingen i andre systemer jf. kapitlerne om

interbankbetalinger i danske kroner, værdipapirafvikling og afvikling af valutahandel.

I slutningen af februar var der en større hændelse i TARGET Services, der medførte, at der i omkring otte timer midt på dagen ikke kunne gennemføres betalinger og værdipapirafvikling i T2 og T2S. Som følge af hændelsen blev lukningen af det europæiske pengepolitiske døgn udskudt i seks timer. Under hændelsen blev nødløsningen i TARGET Services, ECONS II, aktiveret for at håndtere de mest tidskritiske betalinger.

Den 13. og 14. marts var der problemer med at sende bekræftelser til deltagerne i T2S på, at værdipapirafviklingen var gennemført. Hændelsen betød, at værdipapircentraler ikke kunne afstemme deltagernes beholdninger og som følge heraf måtte spærre for afviklingen af handler med visse værdipapirer. Hændelsen medførte forsinkelser i lukningen af det pengepolitiske døgn, herunder også DKK-døgnet samt væsentlige forsinkelser i afviklingen af værdipapirhandler.

Mandag den 5. maj var der udfordringer med at tilgå TARGET Services. Det blev besluttet af ECB, at driften skulle flyttes til et andet datacenter, en øvelse, som tager halvanden time, hvor imens TARGET Services ikke var tilgængelig. Konsekvensen var, at der ikke kunne gennemføres betalinger og værdipapirhandler i dette tidsrum.

I slutningen af november var der henholdsvis to hændelser i TARGET Services, hvor driftsfejl forsinkede afviklingen af værdipapirer og forsinkede afviklingsdøgnet i euro og danske kroner.

De ansvarlige for driften af TARGET Services har fulgt op på hændelserne, og der er igangsat tiltag, som skal forebygge lignende hændelser i fremtiden. Nationalbankens overvågning deltager i regi af den fælles overvågning i opfølgningen på hændelser. Vurderinger af TARGET Services opfølgning på hændelser og efterlevelse af de internationale standarder kommunikeres af ECB's overvågningsfunktion. Derudover følger Nationalbankens overvågning op på de tilknyttede systemers håndtering af konsekvenserne af disse hændelser, se kapitel 2 *Interbankbetalinger*, kapitel 5 *Værdipapirafvikling* og kapitel 7 *Valutahandelsafvikling*.

Internationale standarder

ECB og den fælles overvågning er ved at færdiggøre to vurderinger; en såkaldt comprehensive assessment af T2 og TIPS efter SIPS-forordningen, Regulation on oversight requirements for systemically important payment systems[36], samt en vurdering af T2S efter CPMI-IOSCO's principper for finansielle markedsinfrastrukturer, PFMI.

ECB's overvågning afsluttede i 2022 en vurdering af T2S efterlevelse af Cyber Resilience Oversight Expectations, CROE. Nationalbankens overvågning deltager i opfølgningen på den handlingsplan, ECB har udarbejdet for at adressere identificerede forbedringspotentialer i regi af den fælles overvågning af TARGET Services.

[36] European Union, Den Europæiske Centralbanks forordning (EU) nr. 795/2014 af 3. juli 2014 om overvågningskrav for systemisk vigtige betalingssystemer, juli 2014 (*link*).

Systemændringer

I juni 2025 blev eurosystemets sikkerhedsstillelsessystem, ECMS (Eurosystem Collateral Management System), idriftsat.[37] ECMS håndterer kun sikkerhedsstillelse i euro og ikke danske kroner.

[37] European Central Bank, *Eurosystem launches single collateral management system,* juni 2025 (*link*).

7
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 sælge valuta. Valutahandler, hvor danske kroner købes eller sælges mod en anden valuta, kan enten afvikles via korrespondentbanker eller gennem det internationale valutahandelsafviklingssystem, CLS.

Når en valutahandel afvikles via korrespondentbanker, sker afviklingen af de to betalinger ikke nødvendigvis samtidigt. Ofte afvikles valutahandler på tværs af tidszoner, og betalingerne kan være mange timer undervejs. Det sker fx, hvis en dansk bank sælger danske kroner og køber dollars fra en amerikansk bank. Den danske bank sender måske kronebetalingen om morgenen centraleuropæisk tid. På dette tidspunkt er det nat i USA, og den amerikanske bank sender muligvis først dollars via det amerikanske betalingssystem i dets sædvanlige åbningstid, hvilket kan være mange timer senere. I den mellemliggende periode har den danske bank derfor betalt uden at have modtaget den købte valuta. Det kan resultere i betydelige tab, hvis den anden part i valutahandlen går konkurs, inden modbetalingen er gennemført, og kan potentielt føre til systemiske konsekvenser.

Ved afvikling gennem valutahandelsafviklingssystemet, CLS, reduceres afviklingsrisikoen betydeligt, fordi begge sider af valutahandlen afvikles samtidigt (payment-versus-payment, PvP). Udover PvP afvikling er CLS-afviklingen et multilateralt nettingssystem, der udregner en samlet opgørelse for deltagernes betalinger på tværs af valutaer og modparter, hvilket reducerer deltagernes likviditetsbehov med over 96 pct[38].

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 bankdag afvikles der samlet set i gennemsnit valutahandler for over 8.000 mia. US dollar i CLS.

CLS har derudover en bilateral nettingberegningsservice i 120 valutaer, CLSNet[39], som giver deltagerne en samlet oversigt over deres nettobetalingsforpligtelser. Netting reducerer afviklingsrisikoen ved valutahandler, da netting reducerer de beløb, som skal udveksles mellem parterne i valutahandler. CLSNet bidrager derfor til at reducere afviklingsrisikoen for valutahandler, der ikke kan afvikles i CLS-afviklingen.

CLS ejes af de store internationale banker, der deltager i CLS-afviklingen, heriblandt Danske Bank og Nordea.

Nationalbanken samarbejder med centralbankerne for de øvrige tilsluttede valutaer om overvågning af CLS, se boks 5.

[38] CLS Bank, *CLSSettlement,* marts 2026 (*link*).
[39] CLS Bank, CLSNet, marts 2026 (*link*).

BOKS 5

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

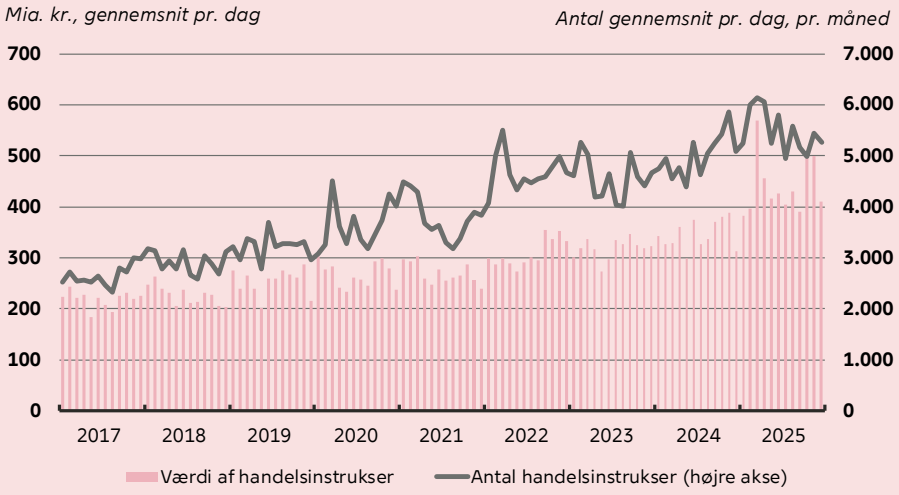
Brug

Danske kroner er den 21.-mest omsatte valuta i verden.[40] Den gennemsnitlige værdi af handler i danske kroner i CLS var på 457 mia. kr. pr. bankdag i 2025. Det er en stor stigning på 26,6 pct. i forhold til 2024, se figur 7. Udviklingen følger en generel global tendens, hvor øget uro på de internationale finansielle markeder, fx i forbindelse med de gentagne amerikanske toldtrusler, har medvirket til en øget aktivitet på de globale valutamarkeder.

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.

FIGUR 7

Handelsinstruktioner i CLS



Kilde: CLS Bank.

[40] Se Danmarks Nationalbank, Handlen med kroner er steget – især i Danmark, *Danmarks Nationalbank Statistiknyhed*, december 2025 (*link*).

Drift og likviditet

De danske deltagere reserverede i 2025 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 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 skete fx i februar 2025, hvor CLS-afviklingen blev påvirket af en større hændelse i TARGET Services, se kapitel 6, Betalinger og værdipapirafvikling i euro. Hændelsen forsinkede udbetalingerne i flere valutaer, herunder USD, CAD, CHF, GBP og SEK, fordi CLS afventede indbetalinger i euro. I CLS-afviklingen er afviklings- og finansieringsprocesserne tæt forbundne, så udbetalinger i valutaer kan først gennemføres, når de nødvendige indbetalinger i andre valutaer er modtaget.

Publikationer

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.

STAFF PAPER

Staff Papers giver indblik i det analysearbejde, som Nationalbankens ansatte er i gang med. Staff Papers indeholder fx baggrundsanalyser og metodebeskrivelser. De henvender sig primært til dig, der i forvejen har kendskab til økonomiske og finansielle analyser. De konklusioner, der udtrykkes i Staff Papers, er forfatternes egne og skal ikke opfattes som Nationalbankens holdning.

WORKING PAPER

Working Papers præsenterer forskningsarbejde fra både ansatte i Nationalbanken og vores samarbejdspartnere. Working papers 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. De konklusioner, der udtrykkes i Working Papers, er forfatternes egne og skal ikke opfattes som Nationalbankens holdning.

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.

STATISTIKNYHED

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.

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 2026

DANMARKS NATIONALBANK