

# DANMARKS NATIONALBANK

3. JUNI 2019 — NR. 3

## Overvågning af den finansielle infrastruktur

- Danmark har en moderne og velfungerende betalingsinfrastruktur. Kronos2 og tilslutningen af kroner til den fælleseuropæiske værdipapirplatform, T2S, har i høj grad bidraget til, at infrastrukturen er up to date.
- Nationalbanken er løbende i dialog med ejerne af den finansielle infrastruktur om deres arbejde med cybersikkerhed. Cybersikkerhed har høj prioritet. Der arbejdes systematisk med styring af risici, om end modenheten i arbejdet varierer.
- Der er på Nationalbankens anbefaling etableret et samarbejde og en fælles metode for styring af risici ved gensidige afhængigheder mellem Kronos2, VP-afviklingen og detailbetalingssystemerne. Det er et vigtigt skridt i arbejdet med en robust dansk betalingsinfrastruktur.

### INDHOLD

- 2 CYBERROBUSTHED I FOKUS FOR NATIONALBANKENS OVERVÅGNING
- 6 INTERBANKBETALINGER
- 10 DETAILBETALINGER
- 12 CLEARING OG AFVIKLING AF DETAILBETALINGER
- 14 VÆRDIPAPIR-AFVIKLING
- 18 VALUTAHANDELS-AFVIKLING
- 20 BETALINGER OG VÆRDIPAPIR-AFVIKLING I EURO

**Ikke alle er  
lige langt fremme**

### Cybersikkerhed

har været i fokus i Nationalbankens overvågning i 2018

[Læs mere](#)

**Vigtig  
infrastruktur**

### 536 mia. kr.

afvikles der i gennemsnit betalinger for hver bankdag

[Læs mere](#)

## Cyberrobusthed i fokus for Nationalbankens overvågning

I Danmark gennemføres hver dag millioner af betalinger. Det sker via et netværk af systemer, der gør det muligt for borgere, virksomheder, finansielle institutter og offentlige myndigheder at udveksle betalinger og andre finansielle transaktioner med hinanden. Den danske betalingsinfrastruktur er beskrevet i boks 1.

Danmark har en moderne og velfungerende betalingsinfrastruktur. I august 2018 udskiftede Nationalbanken Kronos med Kronos2, der er et nyere og mere robust system til interbankbetalinger. I oktober blev værdipapirafviklingen i kroner tilsluttet Target2-Securities (T2S), der er den fælles europæiske clearing- og afviklingsplatform for værdipapirer.

Nationalbankens overvågning har fulgt arbejdet med tilslutningen af danske kroner til T2S. Tilslutningen og de problemer, der opstod i migreringsweekenden og tiden efter, er beskrevet i rapportens afsnit om overvågningen af værdipapirafvikling.

De centrale betalings- og afviklingssystemer og vigtigste betalingsløsninger efterlever i vid udstrækning internationale standarder for sikre, stabile og effektive systemer og løsninger. Det viser Nationalbankens overvågning.

Kravene til infrastrukturens systemer og løsninger skærpes imidlertid løbende i takt med ændringer i teknologi og trusselsbillede. Særligt truslen om cyberangreb stiller nye krav til robustheden i betalingsinfrastrukturen. Derfor har Nationalbankens overvågning også i 2018 haft særlig fokus på,

### Nationalbankens overvågning

Nationalbanken overvåger, at betalinger og finansielle transaktioner i Danmark kan gennemføres sikkert og effektivt. Overvågningen omfatter de centrale systemer og løsninger i den danske betalingsinfrastruktur:

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

Nationalbankens overvågning er beskrevet i bankens overvågningspolitik ([link](#)).

I denne rapport præsenteres de væsentligste konklusioner fra overvågningen af den danske betalingsinfrastruktur i 2018.

hvordan cyberrisici imødegås i infrastrukturens systemer og løsninger.

### Arbejdet med cyberrobusthed

I lyset af den stigende cybertrussel offentliggjorde CPMI-IOSCO i 2016 retningslinjer for betalings- og afviklingssystemers håndtering af cyberrisici.<sup>1</sup> Retningslinjerne uddyber de mere generelle CPMI-IOSCO-principper fra 2012.<sup>2</sup> Nationalbanken er i dialog med de ansvarlige for infrastrukturens centrale systemer om arbejdet med at efterleve retningslinjerne.

Arbejdet med cybersikkerhed har høj prioritet på tværs af systemer og løsninger i infrastrukturen. Der er udarbejdet strategier for arbejdet, som er forankret og følges på øverste ledelsesniveau. Der arbejdes systematisk med styring af risici, herunder

1 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures ([link](#)) er offentliggjort af Bank for International Settlement, BIS, og International Organization of Securities Commissions, IOSCO. Committee on Payment and Market Infrastructures, CPMI, er den arbejdskomite i BIS, der har medvirket til at lave retningslinjerne. I komiteen deltager repræsentanter fra en lang række centralbanker, fx ECB, Federal Reserve Bank og Bank of England.

2 Principles for financial market infrastructures ([link](#)) er offentliggjort af BIS/IOSCO. BIS-komiteen, CPMI, hed Committee on Payment and Settlement Systems, CPSS, da principperne blev udarbejdet. De omtales derfor også som CPSS-IOSCO principperne.

## Betalingsinfrastrukturen i Danmark

Boks 1

Hver bankdag<sup>1</sup> afvikles i gennemsnit betalinger for 536 mia. kr. i den danske betalingsinfrastruktur, svarende til næsten en fjerdedel af BNP.

Nationalbankens betalingssystem, Kronos2, har en central rolle i infrastrukturen; både ved afvikling af store, tidskritiske betalinger mellem banker (interbankbetalinger) og i kraft af Nationalbankens rolle som afviklingsbank for de øvrige betalings- og afviklingssystemer. I Kronos2 afvikles dagligt interbankbetalinger for 83 mia. kr.

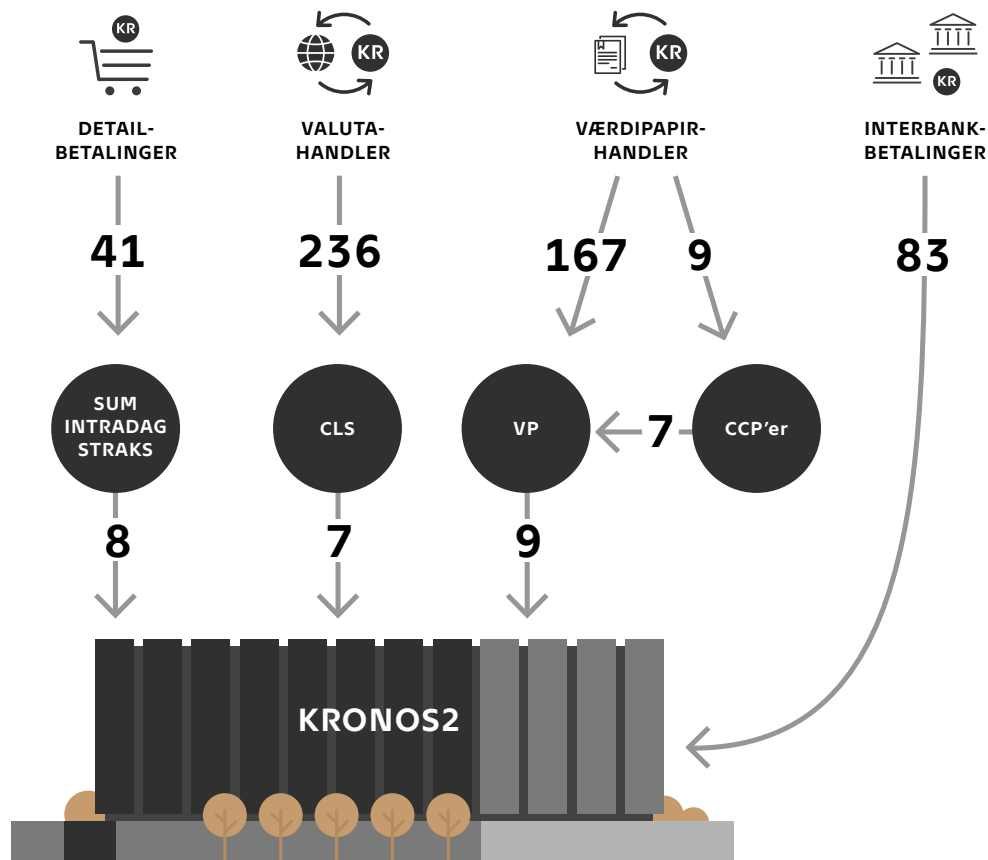
Detailbetalinger er betalinger mellem borgere, virksomheder og offentlige myndigheder, fx ved brug af Dankort eller konto til konto-overførsler. Detailbetalinger cleares og afvikles alt efter type i Sum-, Intradag- eller Straks-clearingen (detailbetalingssystemerne).

Valutahandler i CLS omfatter bl.a. FX spot-, FX forward- og FX swaphandler.

Værdipapirhandler i VP omfatter handler med obligationer, aktier og investeringsbeviser. Nogle værdipapirhandler, fx aktiehandler, cleares gennem en såkaldt central modpart (central counterparty, CCP). Det gælder dog kun en begrænset del af den samlede omsætning.

Betalings- og afviklingssystemerne i infrastrukturen, dvs. CLS, VP og de tre detailbetalingssystemer afvikler deres deltageres nettopositioner i Kronos2. Nettopositionerne beregnes i de respektive systemer ved at modregne deltagernes tilgodehavender og forpligtelser. Denne netting reducerer deltagernes likviditetsbehov til afviklingen betydeligt sammenlignet med en situation, hvor alle betalinger afvikles enkeltvist, fx reducerer netting likviditetsbehovet til afvikling af detailbetalinger fra 41 mia. kr. til 8 mia. kr. dagligt, svarende til en reduktion på 80 pct. I CLS og VP reduceres likviditetsbehovet ved netting med henholdsvis 97 pct. og 95 pct.

### Betalingsflow, mia. kr., gennemsnit pr. bankdag i 2018



<sup>1</sup> 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.

cyberrisici, om end modenheten i arbejdet varierer. Arbejdet med cyberrobusthed er beskrevet nærmere i rapportens afsnit om overvågning af de enkelte betalings- og afviklingssystemer.

En vigtig del af arbejdet med cyberrobusthed sker i samarbejde med andre aktører. Blandt andet i FSOR, Finansielt Sektorforum for Operationel Robusthed, er der siden 2016 arbejdet med forskellige aspekter af cyberrobusthed. Deltagelse i disse sektoraktiviteter understøtter arbejdet med cyberrobusthed hos de enkelte aktører og medvirker til, at CPMI-IOSCO's retningslinjer for cybersikkerhed efterleves.

### Red team-test af cybersikkerheden

De ansvarlige for de centrale systemer og løsninger deltager i TIBER-DK, der er et dansk intelligence-led red team-testprogram, hvor kritiske systemer live-testes mod et simuleret cyberangreb. TIBER-DK er et fælles rammeværk, der skal sikre, at alle deltagere bliver underlagt samme høje minimumsniveau for cybertest.

Red team-test er et vigtigt værktøj til styrkelse af cybersikkerheden og indgår i CPMI-IOSCO's retningslinjer for cybersikkerhed.

### Risici ved gensidige afhængigheder

Efter anbefaling fra Nationalbankens overvågning er der etableret et samarbejde mellem VP, Finans Danmark og Nationalbanken om at identificere og håndtere risici som følge af gensidige afhængigheder mellem Kronos2, VP-afviklingen og detailbetalingsystemerne.

Det tætte samspil mellem systemerne betyder, at der er risiko for, at driftsproblemer i et system påvirker afviklingen i de andre systemer. En anden risiko er, at udefrakommende problemer, som fx et cyberangreb, spredt sig mellem systemerne. Ligeledes kan der være risici som følge af, at systemer-

ne anvender fælles kommunikationsnetværk eller samme kritiske serviceleverandør.

Samarbejdet blev medio 2018 formaliseret i Risikoforum for Gensidige Afhængigheder (RGA) med en fælles metode for risikostyringen. RGA har identificeret og klassificeret en række risici, som der samarbejdes om at imødegå. Derudover drøfter RGA emner vedrørende samspillet mellem systemerne og håndtering af hændelser, som påvirker flere systemer.

RGA rapporterer ind til FSOR, og RGA kan eskalere sager til FSOR, som kræver en bredere sektorinvolvering. Etableringen af RGA og samspillet med FSOR er et vigtigt skridt i arbejdet med en robust dansk betalingsinfrastruktur.

### Dialog med kritiske leverandører

Som et af de første initiativer i arbejdet med de identificerede risici holdt RGA i januar 2019 et fælles møde med kritiske leverandører til infrastrukturen. Formålet var at opnå en fælles forståelse for de gensidige afhængigheder og drøfte mulighederne for videndeling og samarbejde på tværs af leverandører, operatører og systemejere.

Den videre dialog med leverandører til infrastrukturen vil ske i regi af FSOR. Derved breddes fokus ud til at dække alle kritiske dele af infrastrukturen, og erfaringerne fra dialogen kan indgå direkte i FSOR's arbejde med kortlægning og risikoanalyse af infrastrukturen.

### Risikoen for kriminelle transaktioner

På baggrund af bl.a. cyberangrebet mod centralbanken i Bangladesh i 2016 har CPMI offentliggjort en strategi<sup>3</sup>, der skal hjælpe med at styrke endpoint-sikkerhed<sup>4</sup> og derved reducere risikoen for kriminelle transaktioner i centrale betalingsystemer; primært til afvikling af interbankbetalinger.

3 Reducing the risk of wholesale payments fraud related to endpoint security, ([link](#)).

4 Et betalingssystem er forbundet med andre finansielle infrastrukturer, serviceleverandører og deltagere (dvs. banker og andre finansielle institutioner) via netværk til at sende meddelelser. Tilsammen udgør disse parter og tilhørende netværk et komplekst "økosystem" til at afvikle betalinger. Et endpoint er i CPMI's terminologi defineret som et punkt i økosystemet, hvor betalingsinstrukser udveksles mellem parter i økosystemet.

Hovedelementerne i strategien er beskrevet i boks 2. Centralt i strategien er, at ejere af betalingssystemer skal stille passende krav til deltagerne, som fremmer endpoint-sikkerhed. Da ingen aktør alene kan kontrollere alle forhold omkring endpoint-sikkerhed, fremhæver strategien vigtigheden af, at alle relevante aktører inddrages i at implementere sikkerhedstiltag ved de endpoints, de kontrollerer.

Nationalbanken understøtter strategien ved at udmønte den i konkrete anbefalinger til de overvågede systemer og ved at arbejde med problemstillingen i relevante fora som fx FSOR. I 2018 har en FSOR-arbejdsgruppe ledet af Finans Danmark gennemført en analyse af risikoen for kriminelle transaktioner, hvor bl.a. risici for svindel med interbankbetalinger i danske kroner og værdipapirhandler er blevet belyst.

### Strategi for reduktion af risici relateret til endpoint-sikkerhed

Boks 2

CPMI udgav i 2018 rapporten *Reducing the risk of wholesale payments fraud related to endpoint security*. Strategien indeholder syv elementer rettet mod relevante aktører, dvs. operatører af systemer til afvikling af interbankbetalinger, meddelelsesnetværk, serviceleverandører og deltagere i systemerne.

De syv elementer omfatter, at relevante aktører skal identificere og forstå risici for svindel relateret til endpoint-sikkerhed. Desuden skal operatører stille klare krav til deltageres endpoint-sikkerhed som en del af adgangskriterierne for at deltage i et betalingssystem. Operatører og deltagere skal benytte information og værktøjer, som øger mulighederne for at forebygge og opdage forsøg på svindel, og de skal have passende retningslinjer og tilstrækkelige ressourcer til at reagere rettidigt på svindel eller mistanke om svindel. Alle aktører skal løbende støtte uddannelse og awareness om endpoint-sikkerhed og deling af relevant information samt udvikle og opdatere endpoint-sikkerheden og koordinere relevante tiltag indbyrdes.

## Interbankbetalinger

Interbankbetalinger er betalinger mellem finansielle institutter. Betalingerne er typisk karakteriserede ved at være tidskritiske og af høj værdi, og de afvikles derfor i realtidsbruttoafviklingssystemer, RTGS-systemer, som afvikler betalinger enkeltvist og øjeblikkeligt.

I august 2018 udskiftede Nationalbanken det eksisterende RTGS-system for interbankbetalinger i danske kroner, Kronos, med et mere tidssvarende og robust Kronos2 – se boks 3. I Kronos2 afvikles foruden interbankbetalinger også pengepolitiske operationer og nettopositioner fra tilsluttede betalings- og afviklingssystemer.

### Brug

I Kronos2 er der 88 direkte deltagere. Deltagerne er primært danske banker, realkreditinstitutter og filialer af udenlandske banker.

I 2018 blev der dagligt gennemført i gennemsnit ca. 5.400 interbankbetalinger i Kronos2 med en samlet værdi på 83 mia. kr., jf. tabel 1. Det er en stigning i forhold til 2017, hvor værdien var 74 mia. kr.

Der er i 2018 sket et markant fald i overførsler til Sum-, Intradag- og Straksclearingen. Faldet afspejler, at de nye likviditetsstyringsfunktioner i Kronos2 giver deltagerne mulighed for at udnytte deres likviditet mere effektivt, jf. boks 3.

### Driftsstabilitet

I forbindelse med overgangen til Kronos2 har der været flere hændelser end normalt. Det skyldtes bl.a. operationelle fejl ved samspillet med de øvrige systemer i infrastrukturen.

Den 31. august var en fejlindstilling i Kronos2 med til at forsinke udbetalinger af løn. Fejlen skyldtes,

<b>Betalinger i Kronos2</b>		Tabel 1				
Mia. kr., gennemsnit pr. bankdag	2014	2015	2016	2017	2018	
<b>Interbankbetalinger</b>	<b>92,0</b>	<b>99,3</b>	<b>83,0</b>	<b>74,0</b>	<b>83,0</b>	
- Heraf kundebetalinger	11,0	12,8	11,5	11,5	13,6	
<b>Pengepolitiske operationer</b>	<b>25,5</b>	<b>37,5</b>	<b>28,7</b>	<b>39,9</b>	<b>36,9</b>	
- Heraf salg af indskudsbeviser	24,9	37,3	28,6	39,9	36,9	
- Heraf pengepolitiske udlån	0,6	0,2	0,1	0,0	0,0	
<b>Overførsler til afviklingssystemer</b>	<b>320,2</b>	<b>380,0</b>	<b>283,4</b>	<b>316,3</b>	<b>237,4</b>	
- Heraf til Sum-, Intradag- og Straksclearingen	274,6	334,9	242,7	273,8	177,2	
- Heraf til VP-afviklingen	35,2	35,5	31,7	32,5	40,6	
- Heraf til CLS	10,4	9,6	9,0	10,0	19,6	
<b>Afviklede nettopositioner</b>	<b>25,7</b>	<b>27,5</b>	<b>25,1</b>	<b>24,8</b>	<b>24,0</b>	
- Heraf Sum-, Intradag- og Straksclearingen	7,0	7,6	10,6	8,0	8,1	
- Heraf VP-afviklingen	12,2	12,7	10,6	10,1	9,1	
- Heraf CLS	6,5	7,2	6,9	6,7	6,8	

## Kronos2

Boks 3

Kronos2 består af et RTGS-modul til interbankbetalinger og overførsler til afvikling af detailbetalinger, værdipapirer mv., et modul til håndtering af pengepolitiske operationer samt et modul til sikkerhedsstillelse, Calypso. RTGS-modulet, der leveres af Perago, anvendes også af bl.a. Sveriges Riksbank, Norges Bank og Islands centralbank, mens Calypso-systemet anvendes af Banque de France og Banco de España.

Kronos2's centrale placering i den danske finansielle infrastruktur stiller høje krav til sikkerhed og effektivitet.

Kronos2 er specifikt designet til at opfylde høje sikkerhedsmæssige krav vedrørende fortrolighed, integritet og tilgængelighed. Systemet er bygget på en isoleret og dedikeret it-plattform. Det gør det muligt for Nationalbanken at teste hele platformen og løbende foretage egne sikkerhedsmæssige forbedringer. Endvidere er alle vigtige komponenter duplerede, hvilket understøtter målet om en maksimal genetableringstid på to timer efter en større hændelse eller nedbrud.

Funktionalitet i Kronos2 har muliggjort tilslutning af danske kroner til den fælles europæiske værdipapirplatform T2S. Som følge af tilslutningen til T2S, er det pengepolitiske døgn<sup>1</sup> blevet udvidet, så det løber fra kl. 17.30 til 16.45 den efterfølgende dag. Tidligere var det fra kl. 16.30 til kl. 15.30.

Kronos2 er tilgængeligt 24/7, og deltagerne kan derfor udnytte deres likviditet mere effektivt. Fx overfører Kronos2 løbende likviditet på vegne af deltagerne til brug for Straks-clearingen, og der hentes automatisk likviditet til de natlige afviklinger i Sum- og Intradagclearingen. De nye likviditetsstyringsfunktioner har erstattet funktionen "Mest muligt", der overførte hele deltagerens disponible foliolikviditet til nattens afviklinger. Det har ført til en væsentlig reduktion i deltagernes overførsel til detailbetalingssystemerne, jf. tabel 1 og nedenstående figur, der viser likviditetsanvendelsen i detailbetalingssystemerne.

Kronos2 har til forskel fra Kronos ingen køfunktionalitet. Det har ikke ført til problemer, idet deltagerne har rigelig likviditet til at afvikle deres betalinger.

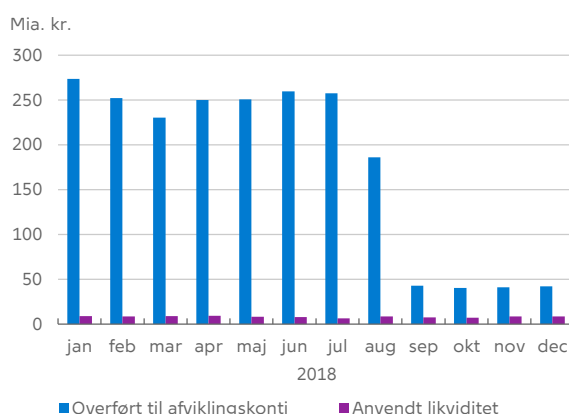
Med Kronos2 er der kommet en ny prismodel<sup>2</sup> for deltagerne, der primært er beregnet på baggrund af en ligelig vægtning af deltagernes andel af det samlede antal og den samlede værdi af alle transaktioner i Kronos2.

## Det pengepolitiske døgn og likviditetsanvendelsen i detailbetalingssystemerne

### Det pengepolitiske døgn



### Likviditetsanvendelsen i detailbetalingssystemerne

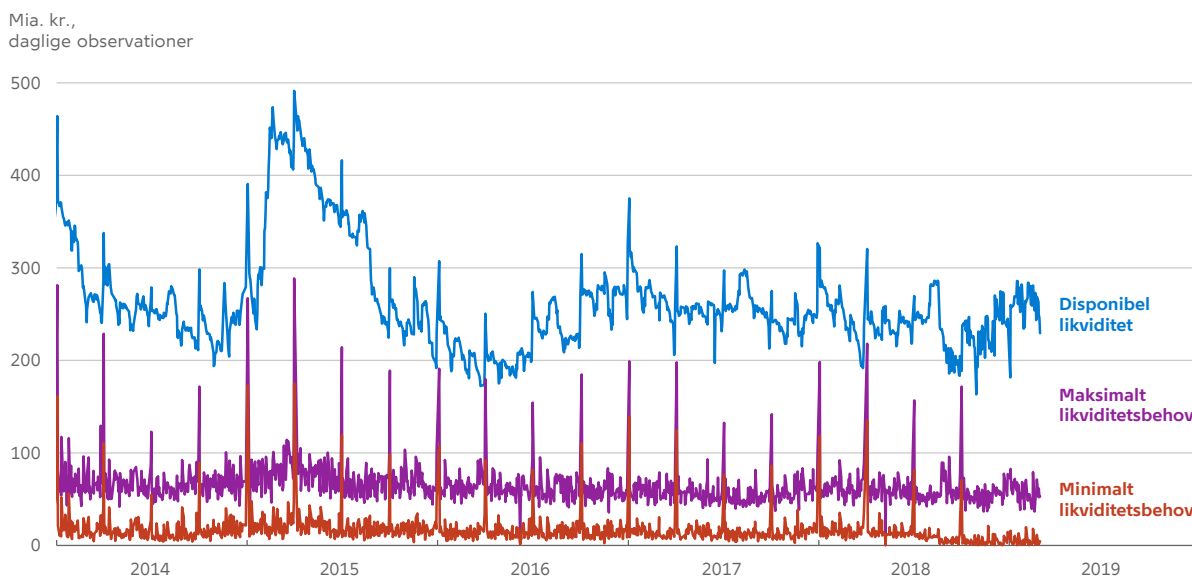


Kilde: Danmarks Nationalbank.

1. Det pengepolitiske døgn er det tidsrum, hvor bankerne kan trække og placere likviditet på deres konto i Nationalbanken, når forskellige betalinger gennemføres.  
 2. Prismodel for Kronos2, ([link](#)).

### Rigelig likviditet blandt deltagerne i Kronos2

Figur 1



Anm.: Disponibel likviditet er deltageres trækingsadgang tillagt saldi på deres foliokonti, når Kronos2 åbner (kl. 7.00). Trækingsadgang via sikkerhedsretten er ikke medtaget. Maksimalt likviditetsbehov svarer til den likviditetsbeholdning, som deltagerne behøver, for at kunne afvikle alle betalinger i løbet af dagen uden forsinkelse. Beløbet afhænger af rækkefølgen af dagens betalinger. Minimalt likviditetsbehov er opgjort som den likviditetsbeholdning, deltagerne behøver for at kunne afvikle dagens betalinger efter maksimal udligning af ind- og udgående betalinger.

Kilde: Danmarks Nationalbank.

at Kronos2's øvre ramme for, hvor højt et beløb der må trækkes på Nationalbankens konto, ved en fejl var sat for lavt. Det betød, at statens betalinger ikke kom videre fra Nationalbanken til bankerne. Indstillingen i Kronos2 blev hurtigt rettet, men som kædereaktion opstod der problemer hos datacentralerne, som skabte yderligere forsinkelser – se afsnit om clearing og afvikling af detailbetalinger.

Det vurderes, at der er blevet fulgt tilfredsstillende op på denne og de øvrige hændelser i relation til Kronos2 i 2018.

#### Likviditet

Deltagerne har som helhed haft rigelig likviditet til at gennemføre deres betalinger i Kronos/Kronos2. Figur 1 viser deltageres likviditetsmæssige overdækning.

Tidligere var likviditetsbehovet særligt stort på dage, hvor handler i forbindelse med auktioner over realkreditinstitutternes rentetilpasningsobligationer afvikles, hvilket ses ved de periodiske stigninger i likviditetsbehovet, jf. figur 1. Efter tilslutning af kroner til T2S i oktober 2018 kan indfrielse af udløbne og finansiering af nye obligationer ske i samme proces, så likviditetsbehovet reduceres gennem netting.

Den rigelige likviditet blandt deltagerne i Kronos2 medvirker til, at afviklingen af betalinger foregår uden problemer.

#### Internationale standarder

Ved seneste vurdering af Kronos efter CP-MI-IOSCO's principper blev der identificeret fire forbedringspotentialer<sup>5</sup>. Som opfølgning blev der i 2017 gennemført en analyse af risici ved indirekte

5 Vurdering af Kronos, 2016 ([link](#))



deltagere.<sup>6</sup> Ved implementeringen af Kronos2 er målet for den maksimale genetableringstid blevet nedbragt fra fire til to timer. Der arbejdes fortsat på de to sidste forbedringspotentialer, herunder at styrke styringen af risici ved gensidige afhængigheder i infrastrukturen, jf. det indledende afsnit. Det udestår at forankre de risici, der identificeres i samarbejdet med VP og Finans Danmark, i risikostyringen for Kronos2.

Som led i den løbende overvågning er risikostyringen af Kronos2 blevet gennemgået efter CP-MI-IOSCO's principper. Konklusionerne fra gennemgangen indgår i Nationalbankens videre arbejde med at styre risici.

### **Cyberrobusthed**

I 2018 er Nationalbankens Risiko- og Sikkerhedspolitik blevet revideret. Det har ført til en styrkelse af rammerne for risikostyringen, herunder styringen af cyberrisici. Bl.a. er målsætninger og krav vedr. risikostyring og sikkerhedsniveau gjort tydeligere, og der er etableret en mere klar rolle- og ansvarsfordeling.

Overgangen fra Kronos til Kronos2 har ført til en væsentlig styrkelse af cyberrobustheden. Kronos2 er designet med høje krav til sikkerheden og er bygget på en isoleret it-plattform, der gør det muligt at foretage løbende justeringer for at imødekomme relevante sikkerhedsmæssige krav.

Nationalbanken har i løbet af 2018 arbejdet på at forbedre kortlægningen af risici i relation til Kronos2. Der er blevet lavet en teknisk risikovurdering af Kronos2's centrale komponenter og en forretningsmæssig risikovurdering af de centrale processer i Kronos2.

I 2018 er der endvidere blevet arbejdet på at opfylde kravene i SWIFT Customer Security Programme (CSP) og ECB's Connectivity Guide. Kravene har til formål at styrke sikkerheden i hele netværket af betalinger, dvs. både sikkerheden i betalings- og afviklingssystemer, kommunikationsnetværk og hos deltagerne. Kronos2 efterlever både SWIFT CSP og ECB's Connectivity Guide.

### **Systemændringer**

Med implementeringen af Kronos2, er en stor milepæl nået. Nationalbanken fortsætter arbejdet med at modernisere sine kernesystemer; bl.a. etableres en styrket Extreme Contingency-løsning, der skal bruges til afvikling af betalinger, i tilfælde af at Kronos2 rammes af en større hændelse eller nedbrud.

---

<sup>6</sup> Analyse af risici ved indirekte deltagere, ([link](#))

## Detailbetalinger

Betalinger mellem borgere og virksomheder kan ske med sedler og mønter eller ved brug af forskellige elektroniske betalingsløsninger. Hovedparten af betalingerne sker elektronisk. Fx konto til konto-overførsel via netbank eller MobilePay, Dankort til betaling af indkøb i supermarkedet eller Betalingsservice til huslejen. I 2018 blev der i gennemsnit gennemført elektroniske detailbetalinger for 27,9 mia. kr. pr. dag.<sup>7</sup>

Nationalbanken overvåger de betalingsløsninger, der har størst betydning i Danmark, nemlig Dankort, Betalingsservice og konto til konto-overførsler, jf. boks 4.

### Driftsstabilitet

Driftsstabiliteten i Nets' systemer vedrørende Dankort og Betalingsservice var tilfredsstillende i 2018. For Dankort var der dog enkelte tilfælde, hvor visse kortholdere havde problemer med at godkende betalinger på nettet med SMS-kode. Det er Nationalbankens vurdering, at Nets' opfølgning på hændelserne har været tilfredsstillende.

I januar 2018 igangsatte Nets desuden en præventiv udskiftning af 36.000 co-brandede Dankort (Visa/Dankort). Baggrunden var en mistanke om, at kortoplysningerne via en kompromitteret udenlandsk hjemmeside var havnet i forkerte hænder. Alle de Visa/Dankort, der var blevet anvendt på pågældende hjemmeside, blev udskiftet.

Betalingservice har ikke været ramt af hændelser med konsekvenser for systemets virkemåde i 2018.

### Misbruget af Dankort er faldende

I 2018 lå misbruget af Dankort ifølge Nets på 57,5 mio. kr., svarende til 0,14 promille af det samlede forbrug.<sup>8</sup> Det er det laveste niveau i fire år, jf. figur 2.

<sup>7</sup> 27,9 mia. kr. pr. kalenderdag svarer til 41,1 mia. pr. bankdag, jf. tabel 2 i afsnittet "Clearing og afvikling af detailbetalinger".

<sup>8</sup> Nets' statistik for misbrug af Dankort: ([link](#)) Nets' misbrugstal er ikke direkte sammenlignelige med Nationalbankens statistik over misbrug med betalingskort, der viser det samlede misbrug med Dankort og internationale kort i Danmark.

### Nationalbankens overvågning af betalingsløsninger

Boks 4

Nationalbanken overvåger Dankort, Betalingsservice og konto til konto-overførsler.

Overvågningen af Dankort og Betalingsservice er rettet mod Nets, som er ejer af disse løsninger. Overvågningen af Dankort omfatter både de rene Dankort og Dankort-siden af de co-brandede Dankort (primært Visa/Dankort).

Overvågningen af konto til konto-overførsler indgår som en del af overvågningen af detailbetalingssystemerne (Sum-, Intradag- og Straksclearingen), jf. afsnittet "Clearing og afvikling af detailbetalinger".

Udviklingen i de forskellige betalingsløsninger i det danske marked følges løbende for at vurdere, om der er behov for målrettet overvågning af dem.

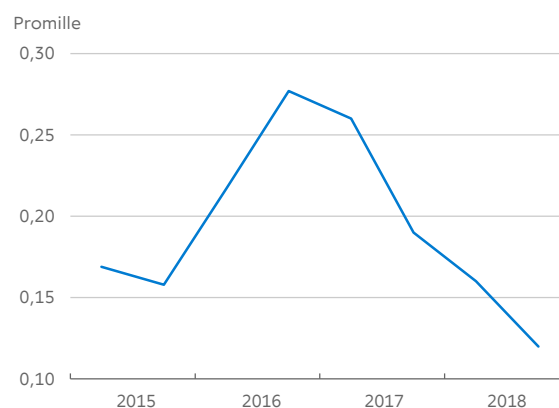
MobilePay vinder stadig større udbredelse til bl.a. handel i butikker, køb på internettet, betaling af faste regninger og overførsler mellem brugerne. Den gennemsnitlige daglige omsætning for MobilePay var på 0,2 mia. kr. i 2018.<sup>1</sup> Til sammenligning lå Dankort i 2018 på 1,1 mia. kr. pr. dag.<sup>2</sup>

De nye betalingsløsninger på det danske marked, Apple Pay og Google Pay, har endnu kun en ganske begrænset markedsandel.

1. Pressemeddelelse fra MobilePay, den 27. december 2018 ([link](#))
2. Nets' statistik for misbrug af Dankort: ([link](#))

### Misbrug som del af det samlede forbrug med Dankort

Figur 2



Kilde: Nets.

Misbruget af stjålne eller tabte Dankort til at handle i butikker eller tage kontanter ud i hæveautomater er blevet mere end halveret siden 2. halvår af 2017 til 0,065 promille i 2. halvår af 2018.<sup>9</sup>

Nets har oplyst, at der i samarbejde med politiet er gennemført en målrettet indsats i 2018 for at forhindre misbrug med stjålne kort. Nets og politiet har i fællesskab identificeret de steder i landet, hvor der oftest sker afluring af folks PIN-kode. Indsatsen har ført til, at kriminelle grupperinger er blevet anholdt.

Ifølge Nets har brugen af kontaktløse betalinger også medvirket til at reducere misbruget: Når PIN-koden ikke bruges ved kontaktløse betalinger, kan den heller ikke aflures. Det mindsker risikoen for den type misbrug, hvor kendskab til PIN-koden og besiddelse af kortet anvendes til at hæve kontanter eller foretage større køb i en butik. Beløbsgrænsen for kontaktløse betalinger med Dankort er blevet hævet fra 200 kr. til 350 kr. fra 1. februar 2018. Det betyder ifølge Nets, at cirka 85 % af betalingerne ved handel i butikker ligger under den nye beløbsgrænse.<sup>10</sup> Af sikkerhedsmæssige årsager vil man dog lejlighedsvis blive bedt om at indtaste sin PIN-kode ved køb under beløbsgrænsen.

Der er også sket et fald i misbruget af Dankort på danske hjemmesider. Misbrug på nettet sker typisk ved tyveri af kortnummer og tilhørende CVV/CVC-kode. Fra 2017 til 2018 faldt denne type misbrug fra 0,5 til 0,38 promille.<sup>11</sup>

Nets gennemførte i begyndelsen af 2017 to tiltag for at styrke sikkerheden af Dankort: Dankort Secured by Nets er en løsning, der bygger på stærk autentifikation, hvor brugeren ved handel på internettet foruden oplysningerne på Dankortet også afkræves en kode, som Nets sender på SMS, før køb over 450 kr. kan færdiggøres; og Fraud Prevention er et system, der ved hjælp af mønstergenkendelse kan afvise transaktioner, der er så usædvanlige, at de må antages at være foretaget af en anden end kortets ejer.

### Internationale standarder

Som led i Nationalbankens overvågning af Dankort og Betalingsservice følges løbende op på Nets' risikostyring. Det vurderes, at Nets har en moden risikostyring, som bygger på anerkendte standarder og anvendes bredt i organisationen. Nets har funktioner i både 1. og 2. organisatoriske forsvarslinje, der følger op på arbejdet med risici og tilhørende kontrolforanstaltninger.

Nets har i 2018 efterlevet de to sidste anbefalinger i Nationalbankens vurdering fra 2017 af Dankort efter ECB's standarder for kortsystemer.<sup>12</sup> Nets har udarbejdet en plan for kommunikation til relevante interessenter ved større driftsforstyrrelser og ændringer vedrørende Dankort. Endvidere har Nets styrket de overordnede beslutningsprocesser for Dankort via en opdateret formel ramme for samarbejdet med bankerne.

Nationalbanken er ved at færdiggøre en vurdering af Betalingsservice efter ECB's standarder for direkte debiteringssystemer.

### Regulering

EU's nye betalingstjenestedirektiv "PSD2" sigter bl.a. på at gøre elektroniske betalinger mere sikre og skabe større konkurrence på betalings-markedet i EU. Den nye Lov om betalinger gennemførte PSD2 i dansk ret og indførte samtidig en række nationale regler den 1. januar 2018.

Mange af de vigtigste bestemmelser for de nye og gamle aktører i markedet vil dog først finde anvendelse i sin endelige udformning den 14. september 2019. Fra denne dato skal bankerne bl.a. være klar med tekniske løsninger, der skal gøre det muligt for deres kunder at foretage betalinger ved hjælp af en udbyder af betalingsløsninger i markedet, uden der er indgået aftale mellem banken og pågældende udbyder.

9 Nets' statistik for misbrug af Dankort: ([link](#))

10 Se nyhed fra Dankort, 13. december 2017: ([link](#))

11 Nets' statistik for misbrug af Dankort: ([link](#))

12 Jf. Danmarks Nationalbank, Vurdering af Dankort, *Danmarks Nationalbank Rapport*, nr. 4, maj 2017 ([link](#)).

## Clearing og afvikling af detailbetalinger

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

I Sumclearingen cleares alle kortbetalinger, Betalingservice samt Nets' øvrige betalingsprodukter én gang i døgnet på bankdage. I Intradagclearingen cleares konto til konto-overførsler som fx netbank-overførsler, lønudbetalinger og offentlige udbetalinger. På faste tidspunkter opgør systemerne deltageres nettopositioner svarende til summen af betalinger til og fra bankernes kunder. Nettopositionerne sendes til Kronos2, der udveksler beløbene mellem bankerne.

Straksclearingen er et reeltidsafviklingssystem, hvor konto til konto-overførsler bogføres på kundernes konti, i takt med at de foretages. Det kan lade sig gøre, fordi bankerne på forhånd reserverer likviditet i Kronos2 til overførslerne. Selve udvekslingen af likviditet mellem bankerne sker seks gange om dagen på bankdage. Straksclearingen anvendes primært til netbank-overførsler og til betalinger via MobilePay.

### Brug

Der er 54 direkte deltagere i detailbetalingssystemerne og 29 indirekte deltagere, som afvikler gennem en direkte deltager. Værdien af transaktionerne i detailbetalingssystemerne udgjorde i gennemsnit 41,1 mia. kr. pr. bankdag i 2018, jf. tabel 2.

Antallet af transaktioner i Straksclearingen er fortsat stigende, jf. figur 3. Stigningen skyldes bl.a., at MobilePay siden 2017 løbende er overgået til i højere grad at anvende konto til konto-overførsler i Straksclearingen frem for dankorttransaktioner i Sumclearingen.<sup>13</sup>

Selv om der har været en stigning i antallet af straksoverførsler, udgør straksbetalinger kun en lille andel af de samlede detailbetalinger målt på værdi, jf. tabel 2.

Værdi af transaktioner i Sum-, Intradag- og Straksclearingen

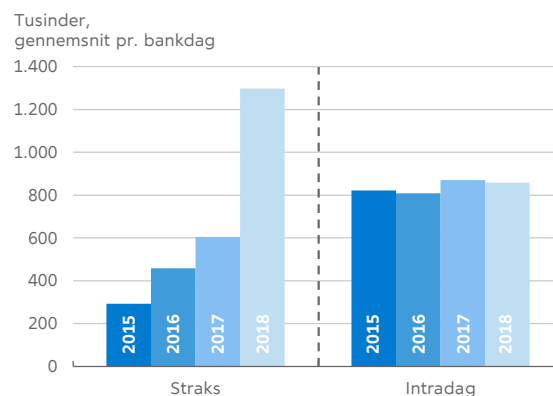
Tabel 2

Mia. kr., gennemsnit pr. bankdag	2014	2015	2016	2017	2018
Sumclearingen	17,9	16,7	17,2	17,8	19,8
Intradagclearingen	17,0	17,8	18,4	19,7	20,1
Straksclearingen	0,5	0,6	0,8	0,9	1,2
I alt	35,4	35,0	36,4	38,4	41,1

Kilde: Nets.

Antal transaktioner i Intradag- og Straksclearingen, 2015-2018

Figur 3



Kilde: Nets.

### Driftsstabilitet

Driften af detailbetalingssystemerne er i 2018 overordnet set forløbet tilfredsstillende. Den 31. august opstod dog betydelige forsinkelser i udbetalingen af løn, pension mv. En fejlindstilling i Kronos2 betød, at der ikke var likviditet nok til nattens afviklinger, som derfor først blev gennemført om morgenen. I kølvandet på hændelsen opstod der følgeføj og pres på kapaciteten hos datacentralerne på grund af ophobningen af transaktioner, der

<sup>13</sup> Antal og værdi af transaktioner i Straksclearingen er ikke udtryk for omfanget af betalinger. Fx kan en betaling i MobilePay medføre, at der foretages to transaktioner i detailbetalingssystemerne.

skulle være bogført om natten, og hvis antal var større end normalt, fordi det var en ultimo-dag. Det forsinkede bogføringen på kundernes konti.

På baggrund af hændelsen 31. august er det besluttet at justere de natlige afviklinger, så afviklingerne kl. 03.00 og 06.00 – i tilfælde af en hændelse – kan afvikles manuelt og dermed tidligere. Det vil give datacentralerne bedre tid til at afslutte bogføringen inden dagens start. Det vurderes, at der er blevet fulgt tilfredsstillende op på hændelsen.

### Likviditet

Deltagerne reserverer likviditet på konti i Nationalbanken til afvikling af deres nettopositioner i Sum-, Intradag- og Straxclearingen. Hvis en deltager ikke reserverer tilstrækkelig likviditet, kan det skabe en dominoeffekt af forsinkede betalinger. Ud over hændelsen 31. august har der i 2018 kun været to tilfælde, hvor deltagere ikke har reserveret tilstrækkelig likviditet.

### Internationale standarder

Nationalbanken offentliggjorde i 2018 en vurdering af detailbetalingssystemerne efter CPMI-IOSCO's principper<sup>14</sup>. Systemerne efterlever i høj grad princippernes krav til sikkerhed og effektivitet. På en række områder er der dog plads til forbedringer. Nationalbanken har bl.a. anbefalet, at governance og risikostyring styrkes yderligere, at der gennemføres test på udvalgte områder, og at arbejdet med cybersikkerhed intensiveres.

Finans Danmark har efterlevet en række af anbefalingerne ved bl.a. at udarbejde en cyberstrategi for detailbetalingssystemerne, teste konkursprocedurer og nødberedskab for systemerne samt ved at offentliggøre en beskrivelse af detailbetalingssystemerne efter internationale standarder. Derudover har Finans Danmark styrket kontrollen af, at opgaverne i relation til detailbetalingssystemerne, herunder risikostyringen, udføres effektivt og i overensstemmelse med gældende politikker og procedurer.

Finans Danmark har lagt en plan for, hvordan de resterende anbefalinger imødekommes.

I 2018 har Finans Danmark sammen med VP og Nationalbanken fastlagt en fælles metode for styring af risici ved gensidige afhængigheder, og Finans Danmark har indarbejdet de identificerede risici i sin egen risikostyring. Dette lukker en tidligere anbefaling fra Nationalbanken.

Nationalbanken har igangsat en vurdering af detailbetalingssystemerne efter CPMI-IOSCO's retningslinjer for cybersikkerhed.

### Systemændringer

Den finansielle sektor har etableret et nyt netværk til brug for kommunikationen mellem datacentralerne, Nets og Kronos2 ifm. clearing og afvikling af detailbetalinger, kaldet e-connect. Det nye netværk lever op til høje standarder for sikkerhed, redundans og driftsstabilitet. Netværket forvaltes af e-nettet, der er ansvarlig for governance og leverandørstyring på vegne af hele sektoren. Migreringen af netværkstrafikken til e-connect forventes afsluttet medio 2019.

Som følge af danske kroners tilslutning til T2S er åbningstiden i Kronos2 blevet forlænget. I den forbindelse er det blevet drøftet, om de sidste afviklingstidspunkter i Intradag- og Straxclearingen bør rykkes til senere på dagen for at få en større andel af dagens transaktioner afviklet samme dag, som de er foretaget. Drøftelserne indgår i et projekt, der skal se på afviklingstidspunkterne for både detailbetalingssystemerne og værdipapirafviklingen for at opnå et mere robust afviklingsdøgn.

En gruppe af større svenske, danske og finske banker<sup>15</sup> arbejder på at etablere et fælles nordisk detailbetalingssystem kaldet P27. Ifølge bankerne er der stordriftsfordele ved at deles om én platform, ligesom et fælles system vil muliggøre fælles produkter på tværs af Norden. Visionen er effektive grænseoverskridende betalinger.

14 Vurdering af de danske detailbetalingssystemer, 2018 ([link](#))

15 Bankerne bag initiativet er Danske Bank, Nordea, Handelsbanken, SEB, Swedbank og OP Financial Group. DNB var en del af initiativet, men trak sig fra projektet marts 2019.

## Værdipapirafvikling

VP-afviklingen er det danske system for afvikling af handler med værdipapirer. VP Securities A/S, VP, står også for registrering af ejerskab af værdipapirer og håndtering af periodiske betalinger, emissioner, indfrielse mv.

Den 29. oktober 2018 flyttede en del af den kro-  
ne-denominerede værdipapirafvikling fra VP's  
egen platform til den fælleseuropæiske værdipa-  
pirplatform Target2Securities (T2S). Fremadrettet  
gennemføres værdipapirafviklingen enten på T2S  
eller VP's egen platform afhængigt af de parter, der  
gennemfører handlen (se boks 5).

### Brug

VP-afviklingen har 126 deltagere, hvoraf 62 er uden-  
landske markedsdeltagere. Tre deltagere har direkte  
adgang til T2S. De øvrige deltagere har indirekte  
adgang til T2S via VP.

Der blev afviklet værdipapirer for 174,5 mia. kr. i  
gennemsnit pr. bankdag i 2018, jf. tabel 3. Det er en  
stigning på 7,3 pct. i forhold til 2017. Der er vækst i  
afviklingen af både aktier, obligationer og invester-  
ingsbeviser. Dermed er de sidste års fald i aktier  
og obligationer vendt.

I løbet af 2018 lukkede VP sit datterselskab i Luxem-  
bourg – VP Lux. Selskabet havde bl.a. til formål at  
bistå danske udstedere med euro-denominerede  
udstedelser, der var belånbare i Eurosystemet.  
Siden 2014 har udstedelser uden for Eurozonen  
også været belånbare, hvorfor behovet for VP Lux

### Danske kroner på T2S – todelt afviklingssystem

Boks 5

Den fælleseuropæiske værdipapirafviklingsplatform, T2S, blev idriftsat 2015 med det formål at gøre grænseover-  
skridende værdipapirafvikling ligeså billigt og effektivt  
som national værdipapirafvikling. Det skulle bl.a. ske ved  
at give nationale værdipapircentraler mulighed for at  
afvikle værdipapirhandel på T2S-platformen. Historisk  
har den grænseoverskridende værdipapirafvikling været  
håndteret af et netværk af internationale depotbanker  
med depoter i forskellige værdipapircentraler eller via  
deltagelse i en international værdipapircentral.

Fortsættes

### Danske kroner på T2S – todelt afviklingssystem

Boks 5

Fortsat

I 2016 fik danske deltagere adgang til at afvikle værdipa-  
pirhandel i euro på T2S, og 29. oktober 2018 migrerede  
danske kroner til T2S. Herefter gennemføres afviklingen  
af deltagernes indbyrdes værdipapirhandel på T2S,  
mens investorenes værdipapirhandel fortsat afvikles i  
VP's egne systemer via deres respektive banker.

Værdipapirafviklingen bliver således fremadrettet  
håndteret i to systemer. Professionelle aktører vil via T2S  
få lettere adgang til afvikling af grænseoverskridende  
handler med danske værdipapirer. De mange private  
investorer med mindre handelsvolumen vil fortsat få  
deres handel afviklet på VP's platform og deres depoter  
administreret i VP.

T2S-platformen drives af euro-systemet og er forbundet  
med centralbankernes RTGS-systemer. Indtil nu har det  
alene været Euroområdet Target2-system, men nu er Na-  
tionalbankens Kronos2-system også forbundet med T2S.

Danske kroner er dermed den første valuta ud over  
Euro, som afvikles på T2S. Den bedre integration med  
den Europæiske infrastruktur bør på længere sigt styrke  
omsætteligheden af danske værdipapirer og understøtte  
visionen om et samlet europæisk finansielt marked.

For den del af værdipapirafviklingen, som sker over T2S,  
er der sket ændringer i likviditetsstyringen. Deltagerne har  
en særlig T2S-afviklingskonto, som holder kronelikviditet  
til værdipapirhandel på T2S. De deltagere, som afvikler  
på VP's platform, vil fortsat skulle reservere likviditet på  
konti i Nationalbanken til VP's nettoafviklingsblokke.

For begge platforme gælder, at hvis en deltager ikke har  
reserveret nok likviditet, vil indrapporterede køb blive  
udskudt til afvikling på et senere tidspunkt, hvor likvidite-  
ten er stillet til rådighed. Der er ikke etableret et bødesy-  
stem på T2S ved manglende likviditetsstillelse, men ifølge  
Central Securities Depository Regulation (CSDR<sup>1</sup>) skal der  
etableres et sanktionssystem, hvor deltagere, som enten  
ikke stiller med tilstrækkelig likviditet eller værdipapirer  
til en handel, skal kompensere deres modpart. Dette sy-  
stem er fortsat under udvikling og vil ifølge planen skulle  
idriftnes i 2020.

I de kommende år vil deltagere skulle tilpasse sig de  
nye muligheder, som infrastrukturen giver, og man vil  
inden for Eurosystemet fortsat arbejde for en harmoni-  
sering af regler for udbytte og beskatning – to områder,  
hvor der i dag er forskelle mellem de enkelte lande, som  
vanskeliggør grænseoverskridende værdipapirhandel og  
-afvikling.

1. Reguleringen af værdipapircentraler i EU sker via CSDR.

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

Tabel 3

År, Gennemsnit pr. dag	I alt		Obligationer		Aktier		Investerings- foreningsbeviser	
	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.
2014	61,1	178,2	3,1	144,4	32,3	28,2	25,6	5,6
2015	67,1	206,2	3,4	158,5	33,4	41,4	30,2	6,3
2016	63,6	175,9	2,8	131,8	30,9	37,6	29,9	6,6
2017	66,9	162,7	2,7	118,4	32,4	36,6	31,8	7,7
2018	71,4	174,5	2,8	125,1	34,2	40,6	34,3	8,9

Anm.: Værdien er opgjort på baggrund af værdipapirbenet i en handel, dvs. markedsværdien af de papirer sælger overdrager til køber.  
 Kilde: VP.

er mindsket. I forbindelse med flytningen skulle alle pantsatte papirer flyttes fra VP Lux til VP, og adgangen til T2S skulle lukkes. Ingen af delene er prøvet før, men både flytning og nedlukning foregik planmæssigt.

### Driftsstabilitet

Driftsstabiliteten i VP-afviklingen har i 2018 været påvirket af flere hændelser i forbindelse med migrationen af danske kroner til T2S. Hændelserne medførte længere forsinkelser af værdipapirafviklingen og i to specifikke tilfælde en udskydelse af handler til næste pengepolitiske døgn.

I den første uge efter igangsættelsen var driften i VP ustabil, bl.a. grundet problemer med eksternt og intern netværkskommunikation. VP gennemførte en række tilpasninger i systemer og processer, og omkring 2 uger efter igangsættelsen var driften stabil, og afviklingsblokke blev afviklet til tiden.

VP har fulgt op på alle hændelser og har håndteret de relaterede problemer. De omfattende systemændringer og relaterede hændelser har betydet, at VP har måttet styrke sine processer og kontroller i forbindelse med systemændringer.

### Ikke-matched handler

Efter migrationen til T2S opstod unormalt mange ikke-matched handelsinstruktioner. Disse kunne pri-

mært henføres til fejl ved deltageres instruktioner. Både implementeringen af nye udvekslingsformater og skift af landekode for en enkelt stor deltager medførte mange fejlinstruktioner. Endvidere var nogle deltageres kontoforhold på T2S først endeligt på plads efter migrationen.

VP og deltagerne samarbejdede om at identificere problemerne og fik frem mod årsskiftet nedbragt antallet af ikke-matched handelsinstruktioner betragteligt.

Forløbet med de mange ikke-matched handler viser vigtigheden af forberedelse og effektiv systemunderstøttelse hos deltagerne, der skal tilpasse, teste og implementere ændringer i egne systemer. Der er fortsat opfølgingsarbejde hos nogle af deltagerne efter tilslutningen af kroner til T2S.

### Afviklingsprocent

Ifølge den fælleseuropæiske regulering af værdipapircentraler, CSDR, artikel 5, skal værdipapirhandler afvikles to dage efter, at handlerne er indgået. Afviklingsprocenten måler andelen af handler, der afvikles rettidigt.

I 2018 har hændelserne i forbindelse med migrationen til T2S resulteret i en faldende afviklingsprocent, jf. figur 4. Afviklingsprocenten er stabiliseret i første kvartal 2019, bl.a. i takt med at problemerne med de ikke-matched handelsinstruktioner er blevet løst.

Afviklingsprocenten har ligget stabilt højt frem til 2017, hvor en enkelt markant hændelse i oktober påvirkede afviklingsprocenten negativt.

### Likviditet

Når en deltager ikke har tilstrækkelig likviditet på sin værdipapirafviklingskonto, kan en eller flere handler ikke gennemføres. Det kan give problemer for deltagerens modparter, der måske ikke kan møde deres forpligtelser grundet de ikke-gennemførte handler. Et sanktionsystem kan medvirke til at disciplinere deltagerne til at stille tilstrækkelig likviditet til afviklingen.

I 2018 var der i alt 116 tilfælde, hvor en deltager ikke havde stillet nok likviditet til værdipapirafviklingen på VP's egen platform. Dette benævnes også "overtræk". Heraf blev der i 43 tilfælde tildelt bøder.

Antallet af tilfælde, hvor der ikke blev stillet tilstrækkelig likviditet/givet bøder, var højere end i 2017, men på niveau med tidligere år, jf. figur 5.

Der gives i dag ikke bøder ved manglende likviditet på T2S-plattformen, hvor der i stedet udvikles et fælleseuropæisk sanktionsystem baseret på kompensation mellem modparter. Det fælles sanktionsystem har planlagt idriftsættelse i 2020. Systemet vil blive gennemgående for både T2S og VP og afløser dermed det nuværende sanktionsystem på VP's platform.

### Internationale standarder

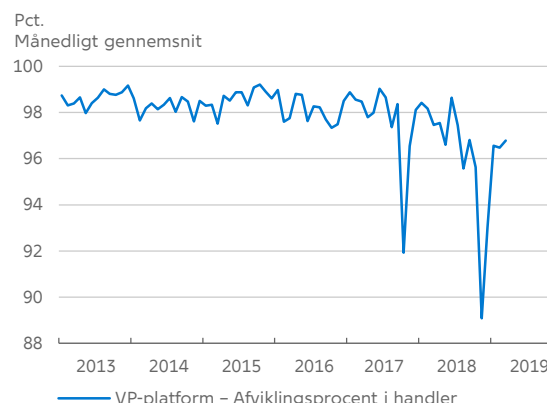
Som led i den løbende overvågning gennemgik Nationalbanken VP's risikostyring i foråret 2018. Konklusionen på gennemgangen er, at VP har en moden risikostyring, som bygger på anerkendte standarder og anvendes bredt i organisationen.

Ved Nationalbankens vurdering i 2016 af VP-afviklingen efter CPMI-IOSCO's principper fik VP fire anbefalinger. De to blev efterlevet i 2017. I 2018 har VP sammen med Finans Danmark og Nationalbanken fastlagt en fælles metode for styring af risici ved gensidige afhængigheder, og VP har indarbejdet de identificerede risici i sin egen risikostyring. Dermed efterlever VP den tredje anbefaling.

Ifølge den sidste anbefaling skal VP tilpasse sin genopretningsplan, så der tydeligere tages stilling til de kritiske scenarier, som er beskrevet i de tekniske standarder under CSDR. VP er i proces med at revidere genopretningsplanen.

**Afviklingsprocenten i VP var lavere i 2018 pga. migreringen af kroner til T2S**

Figur 4

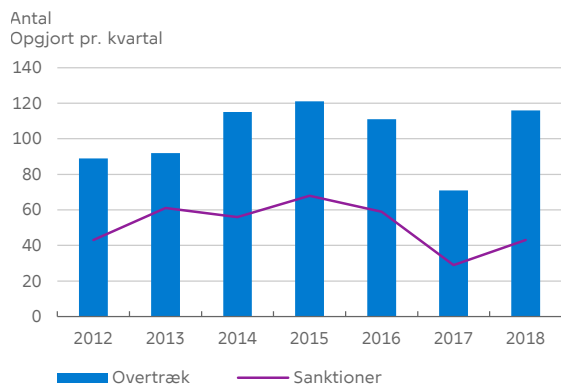


Anm.: I figuren er afviklingsprocenten opgjort for antal transaktioner. Totalen er et vægtet gennemsnit af afviklingsprocenten for VP-plattform og T2S-plattform.

Kilde: VP.

**Overtræk og sanktioner i VP-afviklingen på niveau med tidligere år**

Figur 5



Anm.: Tallene vedrører alene sanktioner og utilstrækkelig likviditetsstillelse for VP-plattformen.

Kilde: VP.

VP har løbende arbejdet på at styrke sin cyberrobusthed. Konkret har VP styrket sin databeskyttelse, adgangskontroller, sikkerhed i systemer og netværk samt gennemført træning og kampagner for medarbejdere.

Nationalbanken har i 2018 igangsat en vurdering af VP's efterlevelse af CPMI-IOSCO's retningslinjer for cybersikkerhed.



### Systemændringer

I forbindelse med migrationen af danske kroner til T2S blev lukningen af det pengepolitiske døgn flyttet til 16.45, hvilket har givet plads til en ny VP-afviklingsblok 80, der køres kl. 15.00.

Tilpasningen af det pengepolitiske døgn skete for at være bedre afstemt med den afviklingscyklus, som T2S-platformen følger. T2S starter sin natlige afvikling kl. 20.00. Kl. 05.00 om morgenen tager T2S-dagsafvikling over, og der kører delivery-versus-payment, DvP-afvikling, frem til kl. 16.00.

Med baggrund i erfaringerne efter migrationen drøfter VP, Finans Danmark og Nationalbanken, om der er behov for yderligere justeringer af tidspunkterne for clearing- og afviklingsblokke hen over det pengepolitiske døgn.

### CCP-clearing

I Danmark gennemføres handel med aktier og repo'er gennem en central modpart, også kaldet central counterparty, CCP, jf. boks 6.

De tre CCP'er, EuroCCP, LCH Clearnet og Six X-clear, clearer aktiehandler, mens Nasdaq Clearing clearer repoforretninger. Efter CCP-clearingen afvikles handlerne i T2S, som EuroCCP har direkte adgang til.

Det løbende tilsyn med, at CCP'erne lever op til kravene i lovgivningen, foretages af de nationale tilsynsmyndigheder i samarbejde med såkaldte tilsynskollegier bestående af tilsynsmyndigheder og centralbanker fra de lande, som CCP'en primært opererer i. Nationalbanken følger udviklingen bl.a. via deltagelse i tilsynskollegiet for EuroCCP.

### Hvad er en CCP?

Boks 6

En CCP stiller sig mellem parterne i en handel og påtager sig risikoen for både køber og sælger, i tidsrummet fra handlen er indgået, og til den er endeligt afviklet. Hvis én af parterne i handlen går konkurs inden for det tidsrum, er CCP'en således stadig forpligtet over for den anden part. Det medfører imidlertid også, at risici koncentrerer sig i CCP'en, der derfor er underlagt en række lovkrav<sup>1</sup> for at sikre gennemførelsen af handlen.

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

## Valutahandelsafvikling

CLS Bank International (CLS) er et afviklingssystem for valutahandler. CLS ejes af store internationale banker og afvikler handler i 18 tilsluttede valutaer, herunder danske kroner.

Traditionelt er de to betalinger i en valutahandel blevet afviklet uafhængigt af hinanden, fx via korrespondentbanker i de pågældende valutaer. Hvis de to betalinger ikke gennemføres samtidig, påføres parterne en afviklingsrisiko, dvs. en risiko for, at modparten ikke betaler sin del af handlen. Med CLS reduceres afviklingsrisikoen, da begge sider af handlen afvikles samtidigt (payment-versus-payment, PVP).

Nationalbanken deltager i den fælles overvågning af CLS, jf. boks 7.

### Brug

Over 80 pct. af valutahandler i danske kroner gennemføres via CLS.<sup>16</sup> Både finansielle institutter og erhvervsvirksomheder deltager i CLS-afviklingen i danske kroner.

Én dansk bank deltager direkte i CLS-afviklingen. Hvis man ikke selv er direkte deltager, kan man afvikle valutahandler i CLS via en af de ni deltagere, der tilbyder indirekte deltagelse til det danske marked. I alt fire deltagere har en CLS-afviklingskonto i Nationalbanken og tilbyder håndtering af ind- og udbetalinger til CLS-afviklingen på vegne af de øvrige deltagere.

Værdien af handler i CLS i danske kroner fortsatte i 2018 den stabile udvikling jf. figur 6. Den gennemsnitlige daglige værdi af handler i danske kroner var 236 mia. kr. i 2018. Antal og værdi af afviklede handler er især stor i dagene omkring udenlandske helligdage og ved kvartalsskifter.

### Brexit

CLS er underlagt engelsk lov og udpeget af Bank of England som et system beskyttet af direktivet om endelig afregning i betalingssystemer og værdipa-

### Overvågning af CLS

Boks 7

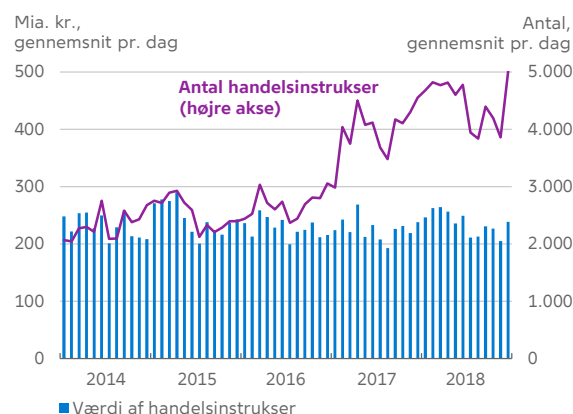
Overvågningen af CLS tager udgangspunkt i CP-MI-IOSCO's principper. CLS offentliggør hvert andet år en opdateret beskrivelse af systemets efterlevelse af principperne.<sup>1</sup>

Overvågningen af CLS foregår i den fælles overvågningskomite, CLS Oversight Committee, der er et forum for samarbejde mellem de tilsluttede valutaers centralbanker<sup>2</sup>, som derigennem kan varetage deres nationale overvågningsforpligtelse. Nationalbanken deltager i samarbejdet, der ledes af den amerikanske centralbank, Federal Reserve, FED, som også er tilsynsmyndighed for CLS. Nationalbankens overvågning har fokus på forhold, der har betydning for afviklingen af handler i danske kroner.

1. CLS, Principles for Financial Market Infrastructures Disclosure, 2016 ([link](#)).
2. Federal Reserve System, Protocol for the Cooperative Oversight Arrangement of CLS ([link](#)).

### Værdi af handelsinstruktioner i CLS følger stabil udvikling

Figur 6



Anm.: Gennemsnit pr. dag beregnet på månedsbasis. CLS har den 23. januar 2017 ændret beløbsgrænsen for, hvornår en handel splittes op i flere instrukser. Dette har øget antallet af instrukser pr. dag.

Kilde: CLS Bank.

<sup>16</sup> Anslået på baggrund af BIS, Triennial Central Bank Survey, Foreign exchange turnover in April 2016, Bank for International Settlements, September 2106 ([link](#)) og data fra CLS Bank.

pirafvikling – også kaldet Settlement Finality Directive. Det betyder, at betalinger i CLS er endelige og ikke kan tilbagekaldes ved fx en deltagers konkurs.

Med Storbritanniens udtræden af EU mister CLS beskyttelsen under direktivet. For at deltagerne i EU fortsat kan afvikle deres valutahandler gennem CLS, kræver det, at landene i national lovgivning har præciseret, at direktivets bestemmelser vedr. endelig afregning også gælder for systemer uden for EØS. I Danmark har vi disse bestemmelser i Kapitalmarkedsloven. I henhold hertil, har Finanstilsynet godkendt CLS som et tredjelandets betalingsystem, og de danske deltagere kan derfor fortsætte i CLS-afviklingen efter Brexit.

### Driftsstabilitet og likviditet

Indbetalingerne til CLS sker via de nationale RTGS-systemer; for danske kroner via Kronos2. Driftsstabiliteten i CLS er derfor afhængig af stabiliteten i de tilsluttede RTGS-systemer. I 2018 var der en enkelt hændelse i Kronos2, hvor netværksproblemer forsinkede deltagernes indbetalinger til CLS-afviklingen. Der blev igangsat nødprocedurer, for at sikre at CLS-afviklingen kunne gennemføres inden for de fastsatte tidsfrister. Det vurderes, at der er blevet fulgt tilfredsstillende op på hændelsen.

De danske deltagere reserverer tilstrækkelig likviditet til CLS-afviklingen.

### Systemændringer

I 2018 blev CLSNet lanceret. CLSNet er en standardiseret, automatisk bilateral netting-service<sup>17</sup>, beregnet til valutahandler, som afvikles uden for CLS. I CLSNet kan deltagerne indsende handler i omkring 120 forskellige valutaer. Servicen er bygget på en platform baseret på distributed ledger-teknologi (DLT) og kan tilgås via SWIFT-netværket.

CLS lancerede i 2018 også CLSClearedFX. En service, som kan afvikle betalinger, der kommer fra CCP-clearede produkter. LCH Clearnet deltager i CLSClearedFX, og det forventes, at Eurex Clearing kommer på i 2019.

Der arbejdes fortsat på udviklingen af CLSNow<sup>18</sup>, som er underlagt lovgivningsmæssig godkendelse. CLSNow vil gøre det muligt at afvikle handler enkeltvist inden for samme dag ved PvP. Servicen vil potentielt blive udvidet til alle CLS-valutaer<sup>19</sup>.

17 CLS, CLSNet (*link*).

18 CLS, CLSNow (*link*).

19 Ved go-live vil dog kun CAD, CHF, EUR, GBP og USD være inkluderet.

## Betalinger og værdipapirafvikling i euro

Danmark er tilsluttet Target2 og Target2-Securities (T2S). Target2 er det fælleseuropæiske RTGS-system til afvikling af interbankbetalinger i euro. I Target2 laves der også overførsler til brug for afvikling i andre eurobetalingssystemer, fx T2S. I T2S afvikles værdipapirhandler i euro og nu også danske kroner – se boks 5.

### Brug

Der er 28 danske deltagere i Target2. I 2018 gennemførte de danske deltagere interbankbetalinger for i gennemsnit 8,8 mia. euro om dagen. Der udveksles flest euro med deltagere i Tyskland, Finland, Frankrig og Holland.

De danske deltagere bruger hovedsageligt Target2 til at gennemføre koncerninterne betalinger og betalinger til udenlandske deltagere. Der er, jf. figur 7, sket et fald i koncerninterne betalinger i løbet af andet halvår af 2017. Det skyldes en ændring i markedsdeltagernes praksis inden for likviditetsstyring.

I T2S er der i alt 21 værdipapircentraler fra 20 europæiske lande, herunder VP. I alt har 13 danske banker en T2S-euro-afviklingskonto i Nationalbanken. Heraf har tre banker via deres filial etableret en eurokonto ved en centralbank i euroområdet for at kunne låne euro intradag. De øvrige banker har indgået aftale med en korrespondentbank.

### Driftsstabilitet

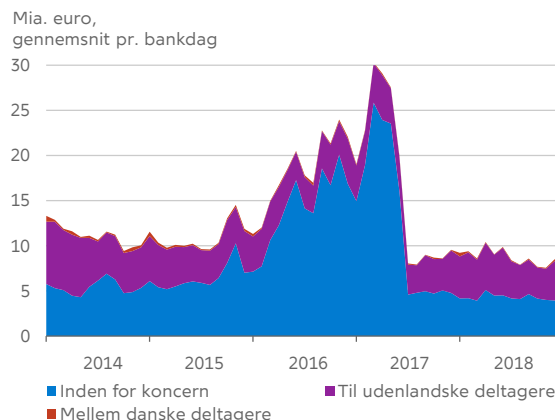
Driftsstabiliteten i de lokale komponenter af Target2, som Nationalbanken har ansvaret for, har i 2018 været tilfredsstillende. Der har i 2018 kun været mindre hændelser, der ikke har påvirket gennemførelsen af betalinger i euro.

### Internationale standarder

Overvågningen af Target2 og T2S sker i samarbejde med centralbankerne i EU i arbejdsgrupperne Payment and Securities Oversight Working Group, PSOWG, og Market Infrastructure and Payments Committee, MIPC, hvor Nationalbanken deltager.

Interbankbetalinger i Target2

Figur 7



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

Kilde: Danmarks Nationalbank.

Nationalbanken og Finanstilsynet deltager sammen med andre europæiske centralbanker og tilsyn i et såkaldt Cooperative Arrangement, som definerer fælles rammer og koordinerer tilsynet med T2S.

### Systemændringer

I 2018 lancerede ECB, TIPS, Target Instant Payment Settlement, som en tjeneste under Target2 – se boks 8.

ECB fortsætter moderniseringen af den europæiske betalingsinfrastruktur, og arbejder på at udskifte Target2 med et mere tidsvarende RTGS-system, der skal være på samme platform som T2S<sup>20</sup>. Det vil øge sikkerheden og reducere driftsomkostninger. Den konsoliderede platform forventes at blive sat i drift i november 2021. Platformen vil tilbyde nye RTGS-services, herunder forbedrede procedurer for likviditetsstyring og en multicurrency-service.

<sup>20</sup> Den it-platform, som understøtter det europæiske afviklingssystem for værdipapirhandler, Target2-Securities, T2S.

### TIPS er gået live

Boks 8

Den Europæiske Centralbank, ECB, har de seneste år arbejdet på at modernisere den europæiske betalingsinfrastruktur. ECB's system til straksbetalinger, kaldet TIPS, gik live november 2018. Systemet giver banker mulighed for at klare og afvikle straksbetalinger i euro. Samtidig understøtter TIPS multicurrency, det vil sige, at systemet kan anvendes til at håndtere straksbetalinger i andre valutaer end euro.

Formålet med TIPS er at tilbyde en løsning, der sikrer, at straksbetalinger mellem alle kontoindehavere i Europa kan ramme hinanden. Det er ECB's ambition, at sådan en service kan minimere risikoen for en fragmenteret europæisk detailbetalingsinfrastruktur og behovet for nationale straksbetalingssystemer.

## OM RAPPORT



Rapporter er tilbagevendende beretninger om Nationalbankens virke.

Rapporter omfatter bl.a. Nationalbankens årsrapport og den halvårslige rapport om monetære og finansielle tendenser.

DANMARKS NATIONALBANK  
HAVNEGADE 5  
1093 KØBENHAVN K  
WWW.NATIONALBANKEN.DK

Redaktionen er afsluttet  
26. april 2019



DANMARKS  
NATIONALBANK