

# DANMARKS NATIONALBANK

30. APRIL 2018 — NR. 4

## Overvågning af den finansielle infrastruktur

- Danmark har en moderne og velfungerende betalingsinfrastruktur. De centrale systemer og løsninger efterlever i høj grad internationale standarder for sikkerhed og effektivitet. Kravene til infrastrukturen skærpes løbende.
- Nationalbanken følger de centrale aktørers arbejde med at efterleve internationale retningslinjer for cybersikkerhed. Ikke alle er lige langt fremme i dette arbejde. En del af arbejdet med cyberrobusthed sker på sektorniveau.
- Der er på Nationalbankens anbefaling etableret et samarbejde om at identificere og håndtere risici som følge af gensidige afhængigheder mellem Kronos, VP-afviklingen og detailbetalingssystemerne. Endelig model ventes på plads medio 2018.

### INDHOLD

- 2 SIKKER OG EFFEKTIV  
INFRASTRUKTUR  
I DANMARK
- 5 INTERBANK  
BETALINGER  
I KRONER
- 8 INTERBANK-  
BETALINGER  
I EURO
- 9 DETAILBETALINGER
- 12 CLEARING OG  
AFVIKLING AF  
DETAILBETALINGER
- 13 VÆRDIPAPIR-  
AFVIKLING
- 17 VALUTAHANDELS-  
AFVIKLING

**Plads til  
forbedringer**

### Cyberrisici

har været i fokus i National-  
bankens overvågning i 2017

[Læs mere](#)

**Vigtig  
infrastruktur**

### 502 mia. kr.

afvikles der i gennemsnit  
betalinger for hver bankdag

[Læs mere](#)

## Sikker og effektiv infrastruktur i Danmark

Danmark er et af de mest digitaliserede lande i verden, og betalinger og finansielle transaktioner sker i vid udstrækning elektronisk. Det er vigtigt for samfundet og for den enkelte borger og virksomhed, at denne udveksling sker sikkert og effektivt. Den danske betalingsinfrastruktur er beskrevet i boks 1.

I international sammenligning har Danmark en moderne og velfungerende betalingsinfrastruktur. De centrale systemer og løsninger i infrastrukturen efterlever i høj grad internationale standarder for sikre og effektive systemer/løsninger. Det viser Nationalbankens overvågning<sup>1</sup>.

Straksbetalinger kan gennemføres inden for få sekunder, og afvikling af værdipapirer sker i overensstemmelse med bedste praksis. Systemerne og løsningerne i infrastrukturen fungerer stabilt, og der er kun sjældent nedbrud eller forsinkelser af betydning. Likviditet kan fordeles smidigt mellem de forskellige betalings- og afviklingssystemer, og generelt er der rigelig likviditet til at gennemføre afviklingen af betalinger mellem bankerne. Alligevel er der plads til forbedringer.

### Plads til forbedringer

Nationalbanken har tidligere givet anbefalinger, som endnu ikke er fuldt imødekommet. Samtidig ændrer omverdenen og de mulige trusler mod infrastrukturen sig løbende – det, der var tilstrækkeligt i går, er ikke nødvendigvis godt nok i morgen. Bedste praksis udvikler sig, og dermed skærpes kravene til infrastrukturens systemer og løsninger.

Nationalbanken er løbende i dialog med de ansvarlige for de centrale systemer og løsninger, som banken overvåger, om arbejdet med de åbne anbefalinger og andre mulige forbedringspotentialer. De involverede parter arbejder løbende på at øge sikkerheden og effektiviteten i infrastrukturens centrale systemer og løsninger.

### Nationalbankens overvågning

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

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

I denne rapport præsenteres konklusionerne fra Nationalbankens arbejde med overvågning af den danske betalingsinfrastruktur i 2017.

Nationalbankens overvågning har i 2017 fortsat haft særlig fokus på håndteringen af cyberrisici og på risici ved gensidige afhængigheder mellem systemerne i infrastrukturen. En vigtig del af dette arbejde sker på sektorniveau, dvs. i samarbejde mellem aktørerne i den finansielle sektor.

### Cyberrobusthed i fokus

De seneste år har budt på alvorlige cyberangreb. Angrebene på henholdsvis centralbanken i Bangladesh for to år siden og sidste år på Mærsk er to tydelige eksempler. Derfor har der på tværs i den finansielle sektor hos både myndigheder og private aktører været stor fokus på at ruste sig så godt som muligt mod cyberangreb.

<sup>1</sup> For en beskrivelse af Nationalbankens overvågning henvises til Danmarks Nationalbank, *Overvågningspolitik, 2015* ([link](#)).

## Betalingsinfrastrukturen i Danmark

Boks 1

Hver bankdag<sup>1</sup> afvikles i gennemsnit betalinger for 502 mia. kr. i den danske betalingsinfrastruktur svarende til næsten en fjerdedel af BNP.

Betalingsinfrastrukturen er det netværk af systemer, der gør det muligt for borgere, virksomheder og offentlige myndigheder at foretage betalinger og finansielle transaktioner.

Nationalbankens betalingssystem, Kronos, har en central rolle i infrastrukturen; både ved afvikling af store, tidskритiske betalinger mellem banker (interbankbetalinger) og i kraft af Nationalbankens rolle som afviklingsbank for de øvrige betalings- og afviklingssystemer. I Kronos afvikles dagligt interbankbetalinger for 74 mia. kr.

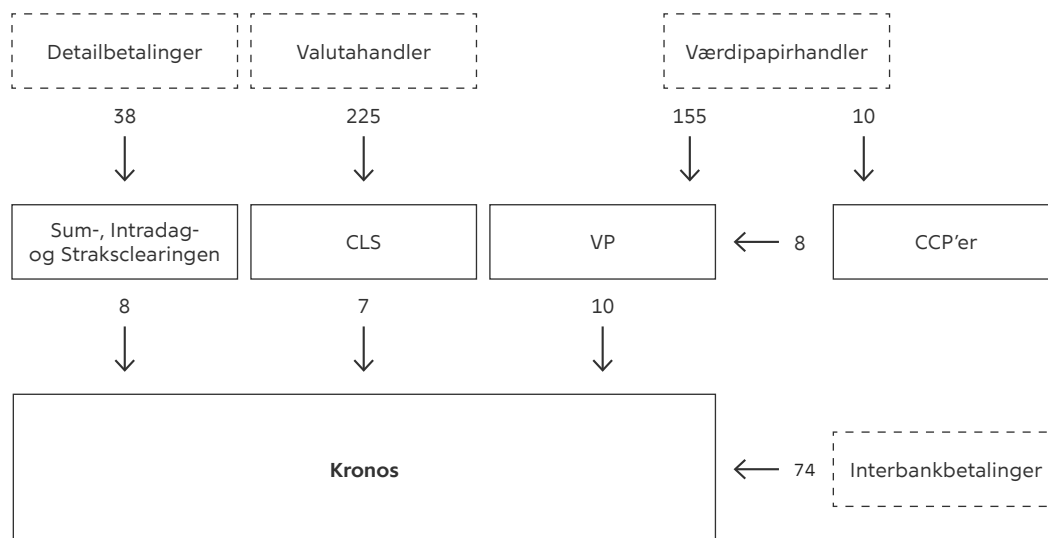
Detailbetalinger er betalinger mellem borgere, virksomheder og offentlige myndigheder, fx ved brug af Dankort eller konto til konto-overførsler. Detailbetalinger afvikles alt efter type i Sum-, Intradag- eller Straksclearingen.

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

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 og VP samt de tre detailbetalingssystemer Sum-, Intradag- og Straksclearingen, afvikler deres deltageres nettopositioner i Kronos. Nettopositionerne beregnes i de respektive systemer ved at modregne deltagernes tilgodehavender og forpligtelser. 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 38 mia. kr. til 8 mia. kr. dagligt, svarende til en reduktion på 79 pct. I CLS og VP reduceres likviditetsbehovet ved netting med henholdsvis 97 pct. og 94 pct.

### Betalingsflow, mia. kr., gennemsnit pr. bankdag i 2017



<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.

CPMI-IOSCO offentliggjorde i 2016 retningslinjer for cybersikkerhed i betalings- og afviklingssystemer.<sup>2</sup> Retningslinjerne uddyber de mere generelle CPMI-IOSCO principper<sup>3</sup> fra 2012 i lyset af den stigende cyberrisiko. Nationalbanken følger løbende arbejdet med at efterleve retningslinjerne. Ikke alle er lige langt fremme i dette arbejde, der er beskrevet nærmere i rapportens afsnit om overvågningen af de enkelte betalings- og afviklingssystemer.

### Sektorsamarbejde

Cyberrisiko adresseres også på sektorniveau, hvor der bl.a. arbejdes med cyberrobusthed i FSOR, Finansielt Sektorforum for Operationel Robusthed, jf. boks 2.

I regi af FSOR er der gennemført en omfattende kortlægning af de mest kritiske forretningsaktiviteter, processer, systemer og aktører i den finansielle sektor. Med det udgangspunkt er der bl.a. igangsat en nærmere analyse af mulige risici, der går på tværs af systemer og løsninger i infrastrukturen, jf. nedenfor om arbejdet med risici ved gensidige afhængigheder.

FSOR har etableret Den Finansielle Sektors Kriseberedskab, der ved alvorlige operationelle hændelser, som fx et omfattende cyberangreb, skal sikre en koordineret indsats på tværs af sektoren. Nationalbanken varetager formandskab og sekretariat for kriseberedskabet. Både i 2016 og 2017 blev der gennemført test af kriseberedskabet. Deltagelse i dette arbejde bidrager til, at de overvågede systemer efterlever CPMI-IOSCO principperne, der anbefaler at deltage i sektorberedskabstest.

Endvidere er det på sektorniveau besluttet at etablere et dansk intelligence-led red team-testprogram, hvor der fastsættes en fælles ramme for det testforløb, deltagerne skal igennem (*link*). Rammeverket skal sikre, at alle deltagere bliver underlagt et ensar-

### Finansielt Sektorforum for Operationel Robusthed

Boks 2

Finansielt Sektorforum for Operationel Robusthed, FSOR, blev etableret i 2016 med det formål at øge den operationelle robusthed i den danske finansielle sektor, herunder robustheden over for cyberangreb. FSOR har deltagelse af betalings- og afviklingssystemer, datacentraler, de største banker, realkreditinstitutter, finansielle interesseorganisationer og myndigheder.

FSOR har til opgave at:

- sikre et fælles overblik over operationelle risici, der kan ramme på tværs af sektoren og potentielt kan true den finansielle stabilitet i Danmark
- beslutte og sikre gennemførelsen af fælles tiltag til at sikre den finansielle sektors robusthed over for store operationelle hændelser, herunder cyberangreb
- skabe rammer for samarbejde og videndeling; både inden for sektoren, mellem forskellige sektorer og internationalt.

Nationalbanken varetager formandskab og sekretariat for FSOR.

tet højt minimumsniveau for cybertest. Der etableres et testteam i Nationalbanken, der skal understøtte deltagerne under testforløbet. I en red team-test gennemføres et simuleret cyberangreb mod systemer i produktion, dvs. livetest.

Nationalbanken, VP og Finans Danmark har, som systemejere, alle givet tilsagn om at deltage i det kommende red team-testprogram. Red team-test er et vigtigt værktøj til efterprøvning og styrkelse af cybersikkerheden og er en del af CPMI-IOSCO's retningslinjer for cybersikkerhed.

Endelig har den finansielle sektor etableret en fælles nordisk CERT<sup>4</sup>, Nordic Financial CERT, NFCERT. Formålet er bl.a. indsamling, deling og anvendelse

2 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 udarbejde retningslinjerne. I komiteen deltager repræsentanter fra en lang række centralbanker, fx ECB, Federal Reserve Bank og Bank of England.

3 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.

4 CERT står for Computer Emergency Response Team.

af information om cybertrusler og cyberangreb på tværs af Norden. Endvidere yder NFCERT ekspertbistand til håndtering af eventuelle cyberangreb. CPMI-IOSCO's retningslinjer for cybersikkerhed fremhæver videndeling som et vigtigt element i at være cyberrobust.

### Risici ved gensidige afhængigheder

Nationalbanken har tidligere anbefalet at styrke samarbejdet om at identificere og håndtere risici som følge af gensidige afhængigheder mellem Kronos, VP-afviklingen og detailbetalingssystemerne.

Dette samarbejde er nu formaliseret i en arbejdsgruppe mellem Nationalbanken, VP og Finans Danmark, der har til formål at identificere og vurdere risici ved gensidige afhængigheder og sikre, at der er robuste foranstaltninger til at håndtere og modgå de identificerede risici.

Risici kan fx opstå som følge af:

- samspillet mellem systemerne i infrastrukturen, som indebærer, at driftsproblemer i et system kan påvirke afviklingen i andre systemer, eller at udefrakommende problemer, som fx et cyberangreb, kan sprede sig mellem systemerne
- afhængigheden af fælles kritiske kommunikationsnetværk og fælles brug af centrale it-driftsleverandører.

Arbejdsgruppen om gensidige afhængigheder er ved at udvikle en fælles metode for styring af risici, som opstår via de gensidige afhængigheder<sup>5</sup>. Den fælles metode skal forankres i de enkelte aktørers risikostyring.

Arbejdsgruppen har samtidig igennem 2017 kortlagt eksisterende infrastruktur og forretningsprocesser samt identificeret en række risici relateret til gensidige afhængigheder. Disse risici vil blive vurderet, og hvis en risiko vurderes at overstige den fælles aftalte risikoappetit, vil modgående tiltag blive igangsat.

Risikostyring og overvågning af risici relateret til gensidige afhængigheder er en løbende proces, som skal varetages af VP, Finans Danmark og Nationalbanken i fællesskab. Den endelige model for samarbejdet forventes at være på plads medio 2018.

## Interbankbetalinger i kroner

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

Kronos er Nationalbankens RTGS-system for interbankbetalinger i danske kroner. I Kronos afvikles desuden pengepolitiske operationer og nettopositioner fra tilsluttede betalings- og afviklingssystemer.

### Brug

Der er 88 direkte deltagere i Kronos. Deltagerne består primært af danske banker, realkreditinstitutter og filialer af udenlandske banker.

I 2017 blev der dagligt gennemført ca. 5.000 interbankbetalinger i Kronos svarende til en daglig værdi af 74 mia. kr., jf. tabel 1. Det er et fald i forhold til 2016, hvor værdien var 83 mia. kr. Værdien af pengepolitiske operationer i form af salg af indskudsbeviser er steget, men det skyldes primært, at deltagerens indestående i Nationalbanken ofte har været større end deres individuelle folioramme. Nationalbanken konverterer den del af deltagerens indestående, der overskrider deres folioramme, til indskudsbeviser.

### Driftsstabilitet

Oppetiden<sup>6</sup> i Kronos var over 99,9 pct. i 2017, hvilket er tilfredsstillende. En hændelse medførte dog, at oppetiden i én måned var lavere end det aftalte servicemål. Den 30. marts 2017 betød

<sup>5</sup> Arbejdsgruppen har defineret gensidige afhængigheder som: Forretningsprocesser og/eller dataflow, der går på tværs af infrastrukturer og underliggende systemer, eller netværk, der deles af flere parter, og hvor nedbrud kan påvirke hinanden, således at én eller flere af parterne ikke kan fortsætte sin forretning uden samarbejde om genopretning.

<sup>6</sup> Oppetiden er den tekniske oppetid leveret af Kronos' driftsleverandør. Driftsafbrydelser, som forårsages af andre forhold, indgår ikke.

<b>Betalinger i Kronos</b>		Tabel 1				
Mia. kr., gennemsnit pr. bankdag	2013	2014	2015	2016	2017	
<b>Interbankbetalinger</b>	<b>96,1</b>	<b>92,0</b>	<b>99,3</b>	<b>83,0</b>	<b>74,0</b>	
- Heraf kundebetalinger	10,3	11,0	12,8	11,5	11,5	
<b>Pengepolitiske operationer</b>	<b>33,5</b>	<b>25,5</b>	<b>37,5</b>	<b>28,7</b>	<b>39,9</b>	
- Heraf salg af indskudsbeviser	33,4	24,9	37,3	28,6	39,9	
- Heraf pengepolitiske udlån	0,2	0,6	0,2	0,1	0,0	
<b>Overførsler til afviklingssystemer</b>	<b>196,5</b>	<b>329,5</b>	<b>389,6</b>	<b>292,7</b>	<b>320,9</b>	
- Heraf til Sum-, Intradag- og Straksclearingen	130,1	272,2	332,3	240,0	271,2	
- Heraf til VP-afviklingen	44,7	40,9	40,8	37,0	33,1	
- Heraf til CLS	21,8	16,5	16,5	15,7	16,6	
<b>Afviklede nettopositioner</b>	<b>21,7</b>	<b>25,8</b>	<b>27,6</b>	<b>25,1</b>	<b>24,8</b>	
- Heraf Sum-, Intradag- og Straksclearingen	3,1	7,0	7,6	7,6	8,0	
- Heraf VP-afviklingen	11,5	12,2	12,7	10,6	10,1	
- Heraf CLS	7,1	6,5	7,2	6,9	6,7	

netværksproblemer, at deltagerne i Kronos i et kortere tidsrum ikke kunne afsende og modtage betalinger. Der blev iværksat manuelle procedurer for at sikre, at CLS-afviklingen kunne gennemføres inden for de fastsatte tidsfrister.

Kronos blev derudover ramt af flere mindre hændelser i 2017, der dog ikke påvirkede systemets oppe-tid. Det vurderes, at der er blevet fulgt tilfredsstillende op på alle hændelser.

### Likviditet

Deltagerne i Kronos har i 2017 som helhed haft rigelig likviditet til at gennemføre deres betalinger. Figur 1 viser deltagernes likviditetsmæssige overdækning.

Traditionelt er likviditetsbehovet særligt stort på dage, hvor handler i forbindelse med auktioner over realkreditinstitutternes rentetilpasningsobligationer afvikles, dvs. typisk ved årets begyndelse og ved de kvartalsvise terminer. Den rigelige likviditet blandt

deltagerne i Kronos medvirkede til, at afviklingen af betalinger foregik uden problemer.

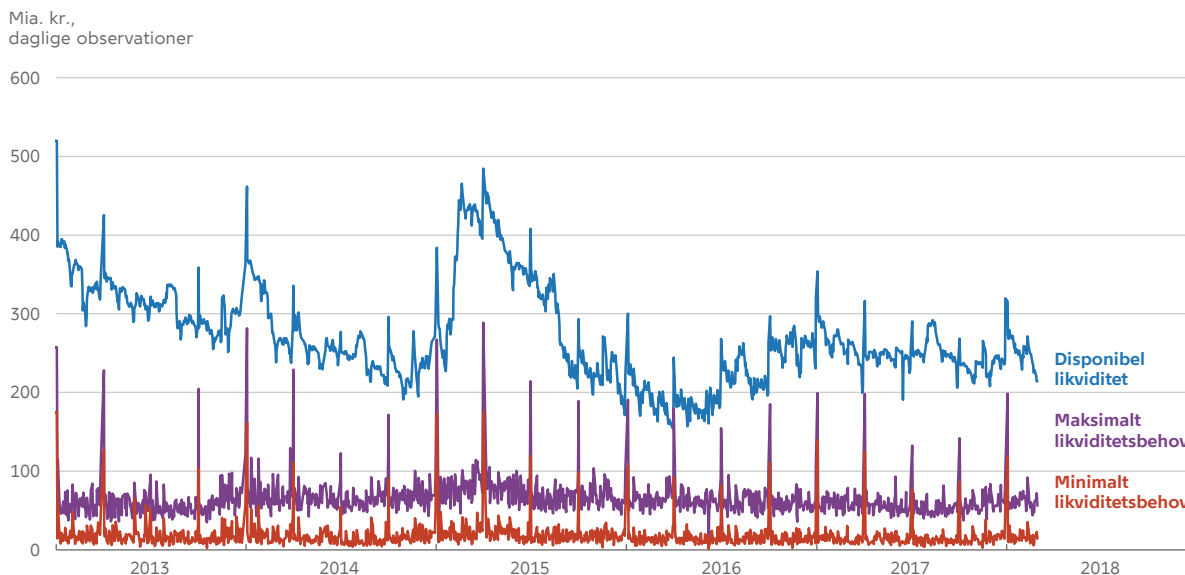
### Internationale standarder

Kronos efterlever langt hovedparten af kravene i CPMI-IOSCO principperne. I 2017 har Nationalbanken fortsat arbejdet med de fire forbedringspotentialer, som i 2016 blev identificeret ved vurderingen af Kronos mod principperne. Det drejer sig om arbejdet med styring af risici ved gensidige afhængigheder, jf. ovenfor, og arbejdet med analyse af risici som følge af indirekte deltagelse, jf. nedenfor. De øvrige forbedringspotentialer forventes håndteret ved idriftsættelsen af Kronos2.

I november 2017 offentliggjorde Nationalbanken en analyse af indirekte deltagelse i Kronos. Hovedparten af de indirekte deltagere er udenlandske banker, som via direkte deltagere afvikler betalinger i danske kroner. Indirekte deltagelse er en god løsning for banker, der ikke har indgående kendskab til det danske marked eller den fornødne operationelle

Deltagernes likviditetsbehov i Kronos

Figur 1



Anm.: Disponibel likviditet er deltagerens samlede trækingsadgang tillagt saldi på deres foliokonti, når Kronos åbner (kl. 7.00). Fra 24. juni 2013 inkluderes modtagne beløb i VP's handelsafviklingsblok 30 kl. 7.05. 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.

kapacitet til at deltage direkte. Afviklingen af kroner overlades således til de deltagere, som har danske kroner som et vigtigt marked og dermed har en udtalt interesse i at sikre, at afviklingen foregår så smidigt som muligt. Med analysen efterlever Kronos CPMI-IOSCO's krav om identificering og styring af risici ved indirekte deltagelse.

### Stresstest

Nationalbanken gennemfører årligt stresstest af likviditeten i Kronos. Stresstesten har til hensigt at måle effekten på betalingsafviklingen og deltagerens likviditet under forskellige former for stress. Et stressscenarie kan fx omfatte, at en stor deltager udgår af betalingsafviklingen, eller at deltagerens intradag-kredit begrænses. I praksis benyttes en betalingsimulator til at sammenligne de respektive stressscenarier med et benchmark-scenarie svarende til den faktiske betalingsafvikling i Kronos. I 2017 viste testen, at Kronos er robust over for de likviditetsstød, som stressscenarierne påfører systemet. Effekten på betalingsafviklingen er begrænset og kan afhjælpes med Kronos' nødprocedurer til afvikling af kritiske betalinger. Med gennemførel-

sen af årlige stresstests efterlever Nationalbanken CPMI-IOSCO's krav om at udføre stresstest af likviditeten i systemet.

### Cyberrobusthed

Nationalbanken har i 2017 udarbejdet en strategi for cybersikkerhed, der skal styrke cyberrobustheden af bankens kritiske forretningsaktiviteter, herunder Kronos og det kommende Kronos2, jf. nedenfor.

Med Kronos2 styrkes cyberrobustheden, idet systemet implementeres på en ny it-driftsplatform, der er designet med høje krav til sikkerhed, og som løbende kan justeres til at efterleve relevante krav.

Kronos'/Kronos2's efterlevelse af CPMI-IOSCO's retningslinjer for cybersikkerhed er blevet kortlagt, og sikkerheden i det kommende Kronos2 gennemgås af eksterne eksperter. Nationalbanken arbejder løbende på at udbedre de mangler, der identificeres.

### Systemændringer – Nyt system er på vej

Nationalbanken er ved at erstatte Kronos med Kronos2. Det nye system består af et RTGS-modul

til håndtering af kritiske betalinger og overførsler til afvikling af detailbetalinger, værdipapirhandler mv., et modul til håndtering af pengepolitiske operationer samt et modul til sikkerhedsstillelse. Perago-systemet benyttes til betalinger og pengepolitiske operationer og anvendes bl.a. også af Sveriges Riksbank og Norges Bank, mens Calypso-systemet benyttes til sikkerhedsstillelse.

I december 2017 besluttede Nationalbanken at udskyde idriftsættelsen af Kronos2. It-plattformen havde endnu ikke den ønskede stabilitet, der er helt afgørende pga. Kronos' centrale placering i dansk betalingsformidling. Endvidere vurderede Nationalbanken, at processerne til at forvalte systemet ikke var robuste nok. Datoen for idriftsættelsen af Kronos2 er 20. august i år.

## Interbankbetalinger i euro

Danmark er tilsluttet Target2, som er det fælleseuropæiske RTGS-system til afvikling af interbankbetalinger i euro. I Target2 afvikles betalinger mellem finansielle institutter, og der laves overførsler til brug for afvikling i andre systemer til betaling og afvikling af euro.

### Brug

Der er 28 danske deltagere i Target2. I 2017 gennemførte de danske deltagere interbankbetalinger for i gennemsnit 16,7 mia. euro om dagen. Der udveksles flest euro med deltagere i Tyskland, Finland, Frankrig og Holland.

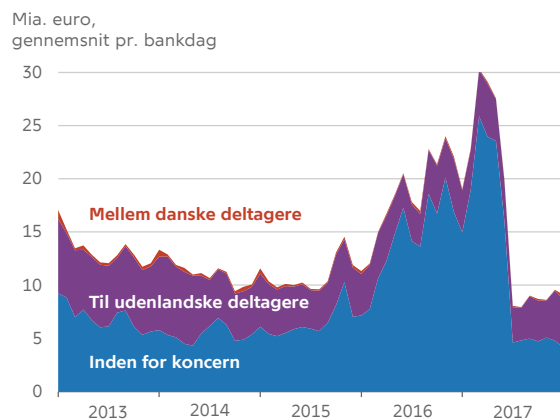
De danske deltagere benytter hovedsageligt Target2 til at gennemføre koncerninterne betalinger og betalinger til udenlandske deltagere. Der er, jf. figur 2, sket et fald i koncerninterne betalinger i løbet af andet halvår af 2017. Det skyldes en ændring i markedsdeltagernes praksis inden for likviditetsstyring.

### Driftsstabilitet

Driftsstabiliteten i de lokale komponenter af Target2, som Nationalbanken har ansvaret for, har i 2017 været tilfredsstillende. Der har i 2017 kun været enkelte mindre hændelser.

## Interbankbetalinger i Target2

Figur 2



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

Kilde: Danmarks Nationalbank.

## Systemændringer

Den Europæiske Centralbank, ECB, har de seneste år arbejdet på at modernisere den europæiske betalingsinfrastruktur. ECB er i gang med at udvikle et system i Target2 til straksbetalinger kaldet TIPS, Target Instant Payment Settlement. Dermed får danske banker mulighed for at cleare og afvikle straksbetalinger i euro. TIPS kommer til at understøtte multicurrency, dvs. systemet vil på sigt kunne anvendes til at håndtere straksbetalinger i andre valutaer end euro. TIPS i euro forventes at blive lanceret i november 2018.

ECB's styrelsesråd godkendte 6. december 2017 migreringen af Target2 til den mere moderne T2S-plattform<sup>7</sup>, hvilket både skal forøge sikkerheden og reducere driftsomkostningerne. Den konsoliderede platform vil tilbyde nye RTGS-services, herunder forbedrede procedurer for likviditetsstyring og en multicurrency-service. Target2-T2S-plattformen forventes sat i drift november 2021.

Styrelsesrådet godkendte endvidere etableringen af et fælles system kaldet ECMS, Eurosystem Collateral Management System, til håndtering af sikkerhedsstillelse i euro, der skal erstatte de eksisterende syste-

<sup>7</sup> Den it-plattform, som understøtter det europæiske afviklingssystem for værdipapirhandler, Target2-Securities, T2S.



mer fra 19 nationale centralbanker. Det nye system forventes idriftsat november 2022.

## Detailbetalinger

Betalinger mellem borgere og virksomheder kan ske med sedler og mønter eller ved brug af forskellige elektroniske betalingsløsninger. Det er fx Dankort til betaling af indkøb i supermarkedet, Betalingsservice til huslejen, eller en konto til konto-overførsel via netbank eller MobilePay. Der blev i 2017 gennemført detailbetalinger for i gennemsnit 26,4 mia. kr. pr. dag.

Nationalbanken overvåger de betalingsløsninger, der har størst betydning i Danmark, jf. boks 3.

### Nationalbankens overvågning af betalingsløsninger

Boks 3

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

Nationalbanken følger løbende udviklingen i de forskellige andre betalingsløsninger 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 på 0,2 mia. kr.<sup>1</sup> er dog fortsat begrænset sammenlignet med de overvågede betalingsløsninger, fx Dankort på 1,2 mia. kr. pr. dag.

Endvidere er de mest systemkritiske dele af MobilePay dækket af Nationalbankens overvågning af detailbetalingsystemerne og Dankort, idet MobilePay benytter sig af konto til konto-overførsel og fx Dankort for at gennemføre en betaling.

1. [www.mobilepay.dk](http://www.mobilepay.dk) (link).

### Driftsstabilitet

Driftsstabiliteten i Nets' systemer vedrørende Dankort og Betalingsservice var overordnet tilfredsstillende i 2017. I tredje kvartal var der dog to større hændelser, hvor fejl og nedbrud påvirkede tilgængeligheden af kortsystemet, og henholdsvis 250.000 og 1,2 mio. Dankort-transaktioner blev afvist. Det er Nationalbankens vurdering, at Nets' opfølgning på hændelserne har været tilfredsstillende.

Ved længerevarende nedbrud kan butikkerne sætte betalingsterminalerne i off-line mode og dermed blive ved med at tage imod betalinger med Dankort. Nets er ved at undersøge, hvordan udnyttelsen af denne løsning kan forbedres – evt. ved hjælp af et automatisk skifte til off-line mode i fx supermarkeder.

Betalingservice har ikke været ramt af hændelser med konsekvenser for systemets virkemåde i 2017.

### Misbruget af Dankort er lavt

Misbruget af Dankort er overordnet set lavt. I 2017 var misbruget i absolutte tal på 104 mio. kr.<sup>8</sup>, svarende til 0,23 promille af den samlede omsætning.<sup>9</sup>

Misbruget er også lavt set i forhold til den svindel, der finder sted med danske kort i udlandet.<sup>10</sup> For Visa/Dankort var misbruget i udlandet på 1,9 promille i 2017<sup>11</sup>, jf. figur 3.

### Misbrug af Dankort til at hæve kontanter og handle i butikker

Misbruget af stjålne eller tabte Dankort til at hæve kontanter eller handle i butikker lå i 2017 på 0,15 promille<sup>12</sup>, jf. figur 4.

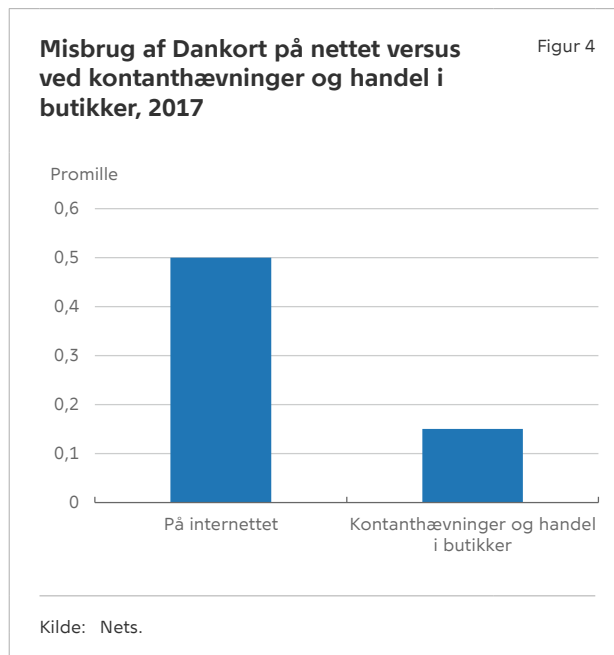
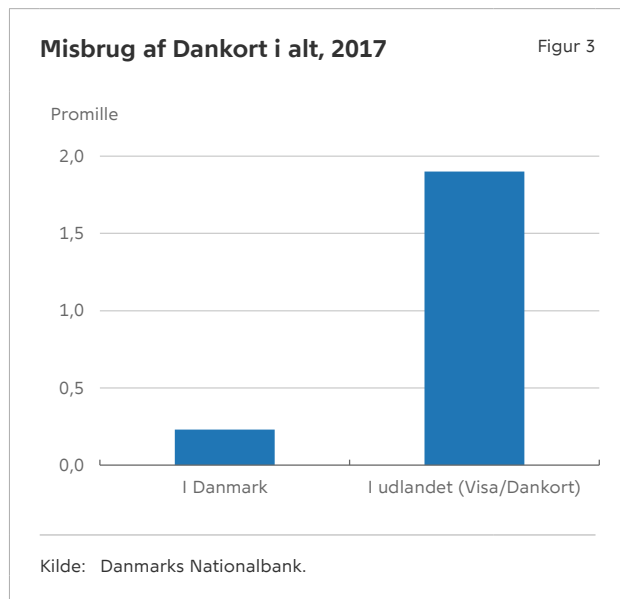
8 Nationalbankens Statistikbank, Betalinger (link), tabel DNBSMIS (vælg: Type 1.1, Kat. 1, Danmark, Værdi, 2017 K1-4).

9 Nationalbankens Statistikbank, Betalinger (link), tabel DNBSMIS (vælg: Type 1.1, Kat. 1, Danmark, Andel af saml. værdi af tr., 2017 K1-4).

10 Se Danmarks Nationalbank, Misbrug af danskernes betalingskort sker især i e-handlen, Danmarks Nationalbank Statistik (Betalinger, 2. kvartal 2017), 12. december 2017 (link).

11 Nationalbankens Statistikbank, Betalinger (link), tabel DNBSMIS (vælg: Type 1.1, Kat. 1, Udland, Andel af saml. værdi af tr., 2017 K1-4).

12 Nets' statistik for misbrug af Dankort (link).

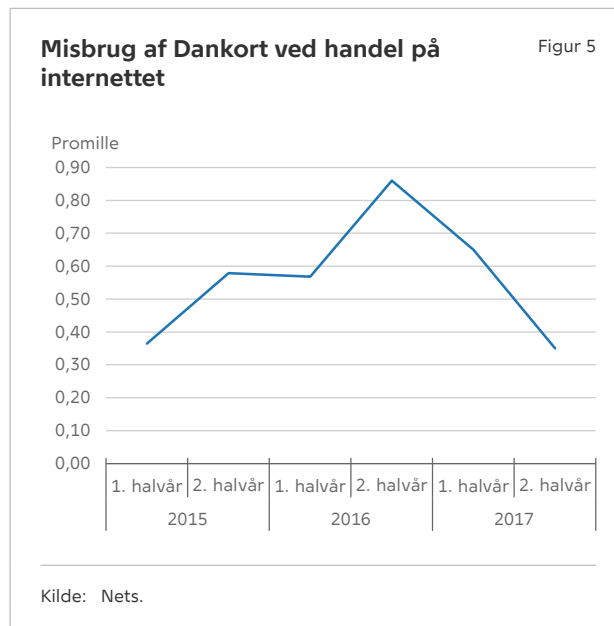


Nationalbanken har bedt Nets undersøge muligheden for at styrke overvågningen af ulovlige kontanthævninger. Nets har på den baggrund udviklet en teknisk løsning, der kan medtage alle kontanthævninger i overvågningen. Nets har indledt dialog med udstederne om denne mulighed, og spørgsmålet drøftes også på Betalingsrådets møde 9. maj 2018.

#### Misbrug af Dankort til at handle på internettet

Misbruget af Dankort til handel på internettet var i 2017 tre gange højere end misbruget i forbindelse med kontanthævninger og handel i butikker, jf. figur 4.

Misbruget af Dankort til at handle på internettet er dog faldet gennem 2017 og er nu nogenlunde på niveau med misbruget i 1. halvår 2015, jf. figur 5.



Nets vurderer, at faldet er et resultat af de tiltag, som Nets gennemførte i begyndelsen af 2017 for at styrke sikkerheden af Dankort, nemlig Fraud Prevention og Dankort Secured by Nets.<sup>13</sup>

<sup>13</sup> *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. *Dankort Secured by Nets* er en løsning, der bygger på stærk autentifikation, hvor brugeren foruden oplysningerne på Dankortet også afkræves en kode, som Nets sender på SMS, før købet kan færdiggøres. Metoden, som også kendes fra køb på internationale kort, benyttes, hvis der handles for over 450 kr.

### Internationale standarder

Nationalbanken offentliggjorde i maj 2017 en vurdering af Dankort efter ECB's standarder for kortsystemer<sup>14</sup>. Hovedkonklusionen var, at Dankort fungerer stabilt med høj tilgængelighed og lavt misbrug. Vurderingen indeholdt samtidig en række anbefalinger til Nets.

Nationalbanken anbefalede bl.a. en udvidelse af Nets' risikovurdering af Dankort, en mere systematisk håndtering af viden i relation til Dankort og en styrkelse af rammerne for beslutninger og kommunikation vedrørende Dankort.

Nets har efterfølgende arbejdet på at efterleve Nationalbankens anbefalinger. I første kvartal af 2018 var Nets i mål med størstedelen af anbefalingerne:

- Nets har gennemført en udførlig risikovurdering af Dankort, der omfatter flere forskellige typer risici i modsætning til før, hvor risikovurderingen fokuserede på it-plattformen. Der er ligeledes etableret en proces for årlig opdatering af risikovurderingen.
- Nets' styring af outsourcing er blevet styrket. Nets' sikkerhedskrav viderestilles til de eksterne leverandører, og der følges mere systematisk op. Blandt andet gennemføres regelmæssige møder og årlige risikovurderinger af outsourcete aktiviteter. Der er etableret et "Vendor Management Board", der skal sikre informationsdeling og en koordineret opfølgning hos Nets vedrørende eksterne leverandører.
- Generelt har Nets etableret et bedre organisatorisk og operationelt overblik med hensyn til Dankort.

Nets arbejder fortsat med Nationalbankens anbefaling om at styrke rammerne for beslutningsprocesser og kommunikation vedrørende Dankort.

Nationalbanken har for nylig igangsat en vurdering af Betalingsservice efter ECB's standarder for direkte debiteringssystemer.

### Regulering

Den 1. januar 2018 trådte Lov om betalinger i kraft. Loven implementerer EU's nye betalingstjenestedirektiv, også kaldet PSD2.<sup>15</sup> Med denne lovgivning har rammevilkårene for betalinger i Danmark og resten af EU ændret sig betydeligt.

Med PSD2 er der bl.a. indført en ret for brugere, som har en betalingskonto, til at benytte denne konto ved hjælp af en tredjepartsudbyder, uden der er indgået en aftale mellem brugerens bank og tredjepartsudbyderen.<sup>16</sup> Dermed åbner PSD2 fx for, at nye tjenesteudbydere kan tilbyde brugerne mulighed for at betale regninger fra deres konto uden direkte kontakt med deres bank – dvs. uden at skulle anvende fx Dankort eller gå ind på netbank.<sup>17</sup>

PSD2 vil sikre, at langt de fleste udbydere af betalingstjenester kommer under tilsyn, og at alle betalinger på internettet – bortset fra visse afgrænsede tilfælde – skal godkendes af brugeren via stærk (to-faktor) autentifikation, dvs. hvor brugeren på to forskellige måder skal bevise sin identitet, hvilket mindsker risikoen for misbrug.<sup>18</sup>

Formålet med de nye regler er at øge konkurrencen i markedet og forbedre sikkerheden ved gennemførelse af betalinger.

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

15 Lov om betalinger justerer desuden en række danske særregler, herunder kontantpligten.

16 De nærmere krav til, hvordan tredjepartsudbydere skal have adgang til at iværksætte en betaling fra brugernes betalingskonti, træder dog først i kraft i september 2019.

17 Fremkomsten af tjenester fra nye udbydere, hvor brugerne kan anvende deres bankkonto uden om bankerne, betegnes ofte som "open banking".

18 De nærmere krav om stærk kundaautentifikation og undtagelserne hertil træder dog først i kraft i september 2019.

## 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, der er den finansielle sektors projekt- og forvaltningsselskab, og leveres af Nets.

I Sumclearingen afvikles alle kortbetalinger, Betalingservice samt Nets' øvrige betalingsprodukter én gang i døgnet på bankdage. I Intradagclearingen afvikles konto til konto-overførsler som fx netbank-overførsler, lønudbetalinger og offentlige udbetalinger. Afviklingen sker på faste tidspunkter fem gange i døgnet på bankdage. Både Sum- og Intradagclearingen er nettoafviklingssystemer.

Straksclearingen er et realtidsafviklingssystem, hvor konto til konto-overførsler under 500.000 kr. gennemføres på få sekunder døgnet rundt alle ugens dage. Det kan lade sig gøre, fordi bankerne har finansieret overførslerne på forhånd. Straksclearingen anvendes primært til netbankoverførsler og til betalinger via MobilePay.

### Brug

Der er 52 direkte deltagere i detailbetalingssystemerne og 31 indirekte deltagere, som afvikler gennem en direkte deltager. Transaktionsomfanget i detailbetalingssystemerne udgjorde i gennemsnit 38,4 mia. kr. pr. bankdag i 2017, hvilket er en stigning på 5,5 pct. i forhold til 2016, jf. tabel 2.

Antallet af transaktioner i Straksclearingen er fortsat steget, jf. figur 6. Stigningen skyldes især, at betalinger med MobilePay bliver afviklet i Straksclearingen. Opgørelser viser, at mere end 3,7 mio. danskere benytter MobilePay.<sup>19</sup>

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

**Betalinger i Sum-, Intradag- og Straksclearingen**

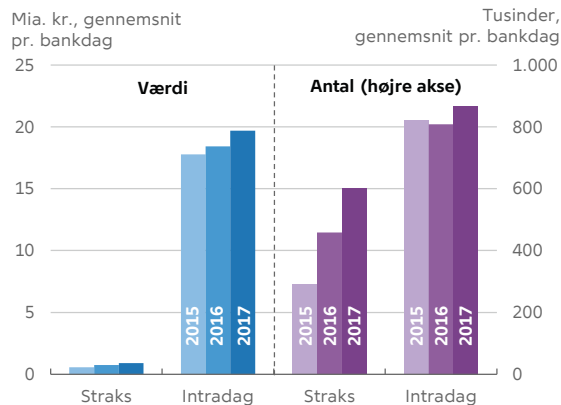
Tabel 2

Mia. kr., gennemsnit pr. bankdag	2013	2014	2015	2016	2017
Sumclearingen	29,1	17,9	16,7	17,2	17,8
Intradagclearingen	13,8	17,0	17,8	18,4	19,7
Straksclearingen	-	0,5	0,6	0,8	0,9
I alt	42,9	35,4	35,0	36,4	38,4

Kilde: Nets.

**Betalinger i Intradag- og Straksclearingen, 2015-17**

Figur 6



Kilde: Nets.

19 [www.mobilepay.dk](http://www.mobilepay.dk) (link).

### Driftsstabilitet

Driften af detailbetalingssystemerne er i 2017 overordnet set forløbet tilfredsstillende. Der var en større hændelse i systemerne 26. april, hvor et dybtliggende hovedkabel blev gravet over. Kabelskaden påvirkede sektorens centrale netværk og medførte, at der i over 8 timer ikke kunne sendes transaktioner til clearing, og at de normale afviklingsaktiviteter mellem Nets og Nationalbanken ikke blev gennemført som planlagt. At der gik over 8 timer, før netværkstrafikken blev reetableret, skyldtes en uklar governancestruktur for netværket. På baggrund af hændelsen blev det besluttet at implementere et nyt netværk, jf. nedenfor om systemændringer.

### Likviditet

Deltagerne reserverer likviditet på konti i Nationalbanken til afvikling af deres nettopositioner. Hvis en deltager ikke reserverer tilstrækkelig likviditet, bliver deltageren henlagt, og der beregnes nye nettopositioner for de øvrige deltagere, der risikerer ikke at modtage den forventede likviditet til afviklingen. Der har i 2017 ikke været tilfælde, hvor en deltager blev henlagt, hvilket bl.a. skyldes, at samtlige deltagere anvender mindst et af de automatiserede værktøjer til likviditetsstyring.

### Internationale standarder

Nationalbanken er ved at færdiggøre en vurdering af detailbetalingssystemernes efterlevelse af CPMI-IOSCO principperne. Vurderingen offentliggøres medio 2018.

Nationalbanken har tidligere anbefalet, at Finans Danmark gennemfører en analyse af detailbetalingssystemernes efterlevelse af CPMI-IOSCO's retningslinjer for cybersikkerhed. Finans Danmark vil iværksætte analysen, når ovennævnte vurdering er gennemført.

### Systemændringer

Den finansielle sektor er ved at etablere et helt nyt netværk til clearing og afvikling af detailbetalinger, som skal erstatte det gamle netværk. Netværket hedder e-connect, og TDC er valgt som leverandør. Projektet varetages af e-nettet, der skal sikre leverandørstyring på vegne af sektoren. e-nettet varetager også den overordnede governance for deltagerne i

det nye netværk. Netværket forventes implementeret i løbet af 2018.

Når danske kroner tilsluttes Target2-Securities, forlænges åbningstiden i Kronos, hvilket muligvis senere afviklinger i detailbetalingssystemerne. I den forbindelse er det tidligere besluttet at rykke de sidste afviklingstidspunkter i Intradag- og Straxclearingen til senere på dagen. Derved vil en større andel af dagens transaktioner blive afviklet samme dag, som de er foretaget.

En gruppe af større svenske, danske, norske og finske banker undersøger i øjeblikket mulighederne for at etablere en fælles nordisk betalingsinfrastruktur for alle banker i Norden. Deres vision er, at de nordiske lande skal være det første område i verden, hvor der hurtigt og nemt kan foretages nationale og internationale betalinger i flere valutaer (svenske, danske og norske kroner samt euro).

## 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.

### Brug

VP-afviklingen har 145 deltagere, hvoraf 60 er udenlandske markedsdeltagere. Der blev afviklet værdipapirer for 162,7 mia. kr. i gennemsnit pr. bankdag i 2017, jf. tabel 3. Det er et fald på 7,5 pct. i forhold til 2016. Faldet var størst for obligationer, mens den afviklede værdi af investeringsforeningsbeviser fortsatte den opadgående tendens fra årene før.

### Driftsstabilitet

Oppetiden<sup>20</sup> i VP-afviklingen var 100 pct. i 2017. Forsinkelser i Target2-Securities, det europæiske afviklingssystem for værdipapirhandler, har i enkelte tilfælde forsinket den natlige afvikling i VP's systemer, men har ikke påvirket VP's tilgængelighed.

<sup>20</sup> Oppetiden er den tekniske oppetid leveret af VP's driftsleverandør.

**Aktier, investeringsbeviser og obligationer afviklet i VP**

Tabel 3

År, Gennemsnit pr. dag	I alt		Obligationer		Aktier		Investeringsforeningsbeviser	
	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.	Antal handler, tusinde	Værdi, mia. kr.
2013	51,5	172,0	3,3	146,1	25,7	21,3	22,5	4,6
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

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

VP og Nationalbanken følger løbende hændelser i VP for at kunne vurdere operationelle risici. Overordnet set vurderes driftsstabiliteten i VP-afviklingen at have været tilfredsstillende i 2017. VP har fulgt rettidigt op på hændelserne, som har haft begrænsede konsekvenser.

### Afviklingsprocent

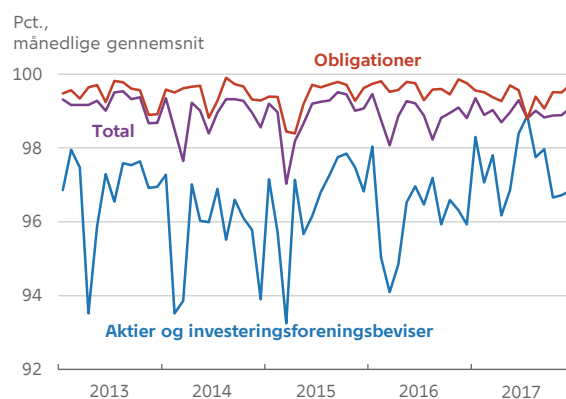
Ifølge bedste praksis skal værdipapirhandler afvikles, to dage efter at handlerne er indgået. Afviklingsprocenten måler andelen af værdien af de handler, der afvikles rettidigt. I 2017 var den samlede afviklingsprocent i VP 99,0 pct., hvilket var lidt højere end året før, jf. figur 7. Hvis deltagere i VP-afviklingen i en længerevarende periode har for lav afviklingsprocent, vil de blive mødt med sanktioner, herunder mulighed for bøder på op til 100.000 kr. I 2017 har der været tildelt to bøder til deltagere med for lav afviklingsprocent.

### Likviditet

VP's deltagere reserverer likviditet på konti i Nationalbanken til VP's nettoafviklingsblokke. Hvis VP's dækningskontrol viser, at en køber ikke har tilstrækkelig likviditet, vil de indrapporterede køb som udgangspunkt blive udskudt til den efterfølgende afviklingsblok. Deltagere, der er i likviditetsmæssigt overtræk, kan tildeles en bøde, der afhænger af, hvor mange gange deltageren har været i overtræk inden for de seneste seks måneder.

**Afviklingsprocenter i VP-afviklingen**

Figur 7



Anm.: I figuren er afviklingsprocenten opgjort for værdien af afviklingen. For aktier og investeringsforeningsbeviser er afviklingsprocenten beregnet som et vægtet gennemsnit af de to papirtyper, mens totalen er et vægtet gennemsnit af alle papirtyper.

Kilde: VP Securities A/S.

I 2017 var der i alt 71 overtræk i VP, hvortil der blev tildelt 29 bøder, jf. figur 8. Antallet af overtræk var dermed lavere end i 2016, og antallet af bøder er halveret. Udviklingen i antal overtræk følges med henblik på at kunne vurdere sanktionssystemets effektivitet.

### Ny regulering og lovgivning

Den fælleseuropæiske regulering af værdipapircentraler, CSDR, har fundet anvendelse i dansk lovgivning siden 2015. CSDR skal bl.a. sikre en ensartet regulering af værdipapircentraler i EU med henblik på at øge den internationale konkurrence. Fremover skal en virksomhed ansøge om licens, jf. CSDR, for at kunne fungere som værdipapircentral i EU.

VP ansøgte om licens under CSDR i maj 2017. Danmarks Nationalbank og ECB deltog i vurderingen af VP's ansøgning som relevante myndigheder, dvs. myndigheder med høringsret. ECB er relevant myndighed for VP, fordi mere end 1 procent af VP's samlede afvikling sker i euro.

VP fik tildelt sin CSDR-licens med virkning fra den 3. januar 2018 som en af de første værdipapircentraler i EU. Fremadrettet skal VP rapportere til Finanstilsynet, Nationalbanken og ECB efter reglerne i CSDR. Ved årsskiftet 2017/18 blev den eksisterende værdipapirhandelslov ophævet og afløst af kapitalmarkedsloven. Denne ændring skete bl.a. for at sikre en bedre sammenhæng med CSDR, i forbindelse med at VP skal fungere efter det nye lovgrundlag.

### Internationale standarder

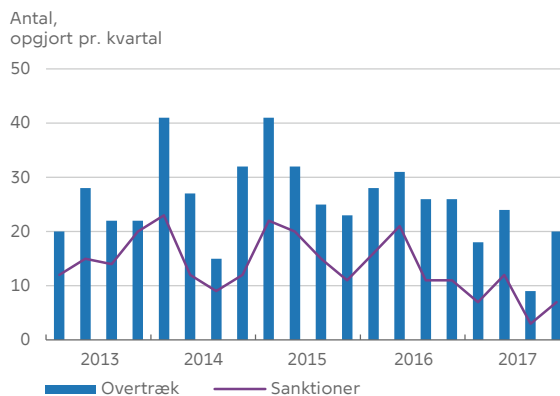
Reglerne i CSDR er afstemt med CPMI-IOSCO principperne, som danner grundlag for Nationalbankens overvågning af den finansielle infrastruktur.

VP efterlever langt hovedparten af kravene i CPMI-IOSCO principperne. Det viser resultaterne af den vurdering, som Nationalbanken og Finanstilsynet offentliggjorde i 2016.<sup>21</sup>

I vurderingen er der givet fire anbefalinger til VP – herunder at sikre uafhængighed i bestyrelsen. I forbindelse med gennemgangen af VP's CSDR-an-

Overtræk og sanktioner i VP-afviklingen

Figur 8



Anm.: En deltager sanktioneres kun med bøder, hvis deltageren selv er skyld i sit overtræk. Det vil sige, der gives ikke bøder, hvis overtrækket skyldes manglende betalinger fra en anden deltager, der har reserveret for lidt likviditet til afviklingen.

Kilde: VP Securities A/S.

søgning har Finanstilsynet vurderet, at der er sikret en tilstrækkelig uafhængighed i VP's bestyrelse.

VP deltager i samarbejdet med Finans Danmark og Nationalbanken om styring af risici ved gensidige afhængigheder. Når samarbejdet er blevet formaliseret, vurderes VP at opfylde CPMI-IOSCO's princip om at styre risici ved gensidige afhængigheder.

VP har desuden fremlagt, hvordan man vil efterleve CPMI-IOSCO's princip vedr. en deltagers nedbrud, afvikling eller konkurs. På baggrund af dokumentationen vurderer Nationalbanken, at VP efterlever princippet.

Endelig gav Nationalbanken en anbefaling vedr. styring af forretningsmæssige risici. Anbefalingen går på, at VP skal sikre en tættere sammenhæng mellem risikostyring, genopretningsplan og afviklingsplan. Denne anbefaling er også givet i forbindelse med gennemgangen af CSDR-ansøgningen.

Nationalbanken vurderer løbende de tiltag, som VP iværksætter for at efterleve kravene fra CPMI-IOSCO principperne.

21 Jf. Danmarks Nationalbank og Finanstilsynet, Vurdering af VP Securities, februar 2016 ([link](#)).

### Cyberrobusthed

VP har i efteråret 2017 besvaret ECB's spørgeskemaundersøgelse vedr. VP's cybersikkerhedsberedskab. Besvarelsen viser, at VP har styrket sit beredskab mod cyberangreb i 2016 og 2017.

VP gennemfører i 2018 en såkaldt red team-test, der gennemføres som et simuleret cyberangreb mod systemer i produktion uden dog at skade disse eller VP's drift. De indledende testresultater bekræfter, at VP har et stærkt cyberforsvar.

### Systemændringer

Som et led i at styrke sin nordiske position har VP indgået aftale med Sveriges Riksbank om at afvikle værdipapirhandler mv. i svenske kroner i VP. Løsningen er taget i brug marts 2017. Endvidere vil VP i løbet af 2018 etablere et nyt og mere effektivt link til den svenske værdipapircentral, Euroclear Sweden, til brug for handel med svenske værdipapirer via VP.

### Target2-Securities

Target2-Securities, T2S, er et europæisk afviklings-system for værdipapirhandler ejet af ECB. Formålet med T2S er, at grænseoverskridende værdipapirhandler skal håndteres lige så sikkert, billigt og effektivt som nationale handler.

I alt er der 20 værdipapircentraler fra 18 lande, der nu afvikler på T2S, herunder VP. Euroafviklingen, der udgør lidt over 1 pct. af den samlede afvikling, sker hovedsageligt på T2S.<sup>22</sup> Euro er foreløbig den eneste afviklingsvaluta på T2S, men fra oktober 2018 tilsluttes danske kroner afviklingssystemet.

13 danske banker er direkte deltagere i T2S og har derfor en T2S-afviklingskonto i Nationalbanken. Heraf har tre banker etableret en eurokonto ved en centralbank i euroområdet for at have direkte adgang til euro. De øvrige banker har indgået aftale med en korrespondentbank.

### CCP-clearing

I Danmark gennemføres handel med aktier og repoer gennem en central modpart, også kaldet central counterparty, CCP, jf. boks 4.

### Hvad er en CCP?

Boks 4

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.

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

De tre CCP'er EuroCCP, LCH Clearnet og Six X-clear clearer aktiehandler, mens Nasdaq Clearing clearer repoforretninger. Efter CCP-clearingen afvikles handlerne i VP.

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 vigtigste lande, CCP'en opererer i. Nationalbanken følger udviklingen bl.a. via deltagelse i tilsynskollegiet for EuroCCP.

<sup>22</sup> Der vil stadig være mulighed for euroafvikling i VP's egne systemer i blok 50 kl. 14.15.



## Valutahandelsafvikling

En valutahandel består af to modsatrettede betalinger i to forskellige valutaer.<sup>23</sup> Ved traditionel afvikling gennemføres de to betalinger uafhængigt af hinanden, fx via korrespondentbanker i de pågældende valutaer. Hvis de to betalinger ikke gennemføres samtidig, påføres parterne en afviklingsrisiko. Det internationale afviklingssystem for valutahandler, CLS, reducerer afviklingsrisikoen ved at afvikle begge sider af handlen samtidig (payment-versus-payment, PvP).

CLS ejes af store internationale banker og afvikler handler i 18 tilsluttede valutaer, herunder danske kroner.

Nationalbanken deltager i den fælles overvågning af CLS, jf. boks 5.

### Brug

Over 80 pct. af valutahandler i danske kroner gennemføres via CLS.<sup>24</sup> Både finansielle institutter og erhvervsvirksomheder deltager i CLS-afviklingen i danske kroner. Hvis man ikke selv er direkte deltager i CLS, kan man afvikle valutahandler via en af de fire banker, som har direkte adgang til afviklingen af danske kroner i CLS.

Værdien af handler i CLS i danske kroner fortsatte i 2017 den stabile udvikling, jf. figur 9. Den gennemsnitlige daglige værdi af handler i danske kroner var 225 mia. kr. i 2017. Værdien af afviklede handler er især stor i dagene omkring udenlandske helligdage og ved kvartalsskifter. CLS-afviklingen i danske kroner satte rekord den første bankdag i 2. kvartal 2017, 3. april. Den samlede værdi af handler var denne dag på 612 mia. kr.

### Driftsstabilitet og likviditet

Indbetalingerne til CLS sker via de nationale RTGS-systemer; for danske kroner via Kronos.

Derfor er driftsstabiliteten i CLS afhængig af stabiliteten i RTGS-systemerne. I 2017 påvirkede en enkelt hændelse i Kronos CLS-afviklingen. Den 30. marts

### Overvågning af CLS

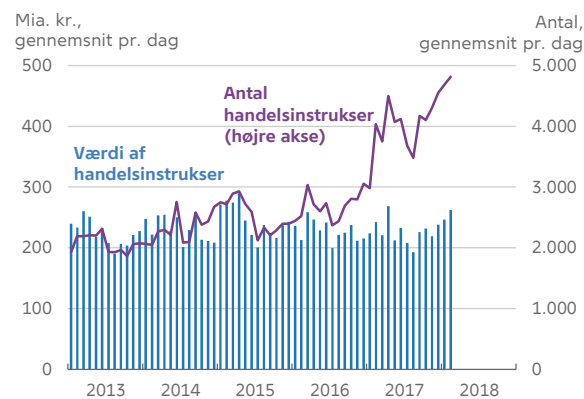
Boks 5

Overvågningen af CLS tager udgangspunkt i CPMI-IOSCO principperne. CLS offentliggør hvert andet år en opdateret beskrivelse af systemets efterlevelse af principperne.<sup>1</sup> Overvågningen af CLS foregår i den fælles overvågningskomitee, 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](#)).

### Handelsinstrukser i CLS

Figur 9



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>23</sup> Fx vil en handel i kroner mod euro medføre en betaling i kroner fra den ene part til den anden og en betaling i euro den anden vej.

<sup>24</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.

2017 var betalingsafviklingen i Kronos påvirket af netværksproblemer, så CLS ikke kunne modtage betalinger. Der blev iværksat manuelle procedurer for at sikre, at CLS-afviklingen kunne gennemføres inden for de fastsatte tidsfrister.

De danske deltagere reserverer tilstrækkelig likviditet til CLS-afviklingen.

### Systemændringer

CLS arbejder fortsat på lanceringen af CLSNet, som er en standardiseret, automatisk bilateral netting service<sup>25</sup>, beregnet til FX-handler, som afvikles uden for CLS. Det vil være muligt for deltagerne at indsende FX-handler i mere end 125 forskellige valutaer. Servicen bliver bygget på en platform baseret på distributed ledger-teknologi (DLT). CLSNet kan enten tilgås direkte via DLT eller via SWIFT-netværket.

Endvidere forventer CLS at lancere en separat service, der kan afvikle CCP-clearede produkter. De første deltagere i den nye CCP-service forventes at blive Eurex Clearing og LCH Clearnet.

Endnu et nyt initiativ under udvikling er CLSNow<sup>26</sup>, som vil gøre det muligt at fjerne afviklingsrisikoen for handler inden for samme dag, bl.a. det ben af in/out swaps<sup>27</sup>, som i dag afvikles uden for CLS.

I CLSNow afvikles begge ben af handlen samtidigt (PvP), og afviklingen foregår brutto. Servicen vil på sigt være tilgængelig for alle CLS-valutaer<sup>28</sup>.

25 CLS, CLSNet ([link](#)).

26 CLS, CLSNow ([link](#)).

27 In/out swaps bruges i CLS til at mindske store positioner for at minimere likviditetsrisici ved afviklingen.

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

## OM RAPPORT



Rapporter er tilbagevendende beretninger om Nationalbankens virke.

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

