

DANMARKS NATIONALBANK

17. MAJ 2017 — NR. 4

Vurdering af Dankort

- Betalinger med Dankort udgør omkring 60 pct. af omsætningen i detailhandlen; kontanter og andre betalingskort står for resten. Det er vigtigt, at Dankort er sikkert og velfungerende.
- Dankort fungerer stabilt med høj tilgængelighed, og misbrug med Dankort er lavt i international sammenligning.
- Nationalbanken har vurderet Dankort, som er ejet af Nets A/S, efter ECB-standard for kortsystemer. Nationalbankens vurdering indeholder anbefalinger til Nets. Nets bør sikre en mere systematisk håndtering af viden i relation til Dankort. Nets udarbejder i dag risikoanalyser af den it-plattform, som Dankort kører på. Dette arbejde bør udvides i form af en risikovurdering, der dækker alle relevante aspekter af Dankort. Nets bør styrke rammerne for beslutningsprocesser og kommunikation vedrørende Dankort.

KONTAKT

Ole Mikkelsen
Kommunikations-
og presserådgiver

omi@nationalbanken.dk
+45 3363 6027

SEKRETARIAT
OG KOMMUNIKATION



Et sikkert

og velfungerende
Dankort er vigtigt.

Læs mere



Begrænset misbrug

af Dankort
og høj stabilitet.

Læs mere



Anbefalinger

i forhold til
ECB-standarden

Læs mere

Betalinger med Dankort udgør den største del af betalinger i detailhandlen. Det er vigtigt, at Dankort er velfungerende, og at misbrug med Dankort er lavt. Dankort bør derfor leve op til internationale standarder for kortsystemer.

ECB har udarbejdet standarder for velfungerende kortsystemer ([link](#)), som bl.a. VISA, MasterCard, American Express og lokale betalingskort-schemes i Europa vurderes efter.

Nationalbanken har vurderet Dankorts efterlevelse af ECB-standard for kortsystemer.

Nets ejer Dankort og giver pengeinstitutterne tilladelse til at udstede Dankort. Nets er dermed kortorganisation for Dankort, også kaldet "scheme-ejer" eller "governance authority", og det er Nets, der bør sikre, at Dankort lever op til ECB-standard.

Nationalbankens vurdering af Dankort dækker de dele af Nets' virksomhed, som bidrager til Dankorts funktion. Ansvar for, at Dankort fungerer, er forankret i forskellige grene af Nets' organisation, fx håndteres de juridiske aspekter og regelsæt omkring Dankort, kontakten med Nets' kunder og ansvaret for it-infrastrukturen i forskellige dele af Nets.

I denne publikation gennemgås indledningsvis baggrund og metode for vurderingen. Herefter sammenfattes Nationalbankens bedømmelse af, om Nets efterlever ECB's standard for kortsystemer. I de følgende afsnit beskrives Nets' efterlevelse af standarden og Nationalbankens anbefalinger og bemærkninger til forbedringer.

Fakta om Nets

Nets A/S er en nordisk udbyder af en række produkter inden for bl.a. betalingsformidling og kort- og informationsservices med hovedsæde i Danmark. Nets er kortorganisation for Dankort, men tilbyder også andre produkter, fx Betalingsservice. Nets' kunder omfatter mere end 240 pengeinstitutter og 300.000 forretninger i Norden.

Virksomhedens historie går tilbage til 1968. Siden 2010 har den været kendt under navnet Nets. I 2014 blev Nets solgt til ATP og to amerikanske kapitalfonde, Advent International og Bain Capital. I 2016 blev Nets børsnoteret.

Danskerne og Dankort i tal

Danmark er et af de lande i Europa, hvor kortbetalinger udgør den største andel af de samlede betalinger. Dankort er danskernes fortrukne betalingsløsning: Betalinger med Dankort udgjorde i 2016 omkring 60 pct. af omsætningen i detailhandlen. Der blev i 2016 foretaget 1,3 mia. betalinger med Dankort til en samlet værdi af 379 mia. kr.

Der er udstedt samlet ca. 5,4 mio. Dankort og Visa/Dankort. Hver myndig borger i Danmark har i gennemsnit 1,2 Dankort. Praktisk talt tager alle forretninger i Danmark imod Dankort.

Centrale aktører i relation til Dankort

Nets ejer Dankort og varetager derudover også en række forskellige roller i relation til Dankort. Nets

- er eneindløser af Dankort-betalinger, dvs. Nets sikrer, at betalingsmodtageren får sine penge ved en kortbetaling.
- udfører kortudstederservice, dvs. bistår udsteder med fx håndtering af transaktioner, udsendelse af PIN-kode, kundeservice og overvågning af misbrug.
- processerer kortbetalinger, herunder leverer Nets den infrastruktur mellem kortudsteder og kortindløser, der sikrer udveksling af information mellem parterne. Nets er i processor-rollen bl.a. ansvarlig for at samle dagens Dankort-transaktioner og beregne, hvad det enkelte pengeinstitut skal betale eller modtage fra hvert af de øvrige pengeinstitutter.
- er operatør af det danske clearing- og afviklingssystem Sumclearingen, hvor den endelige afvikling af Dankort-betalingerne sker på vegne af Finans Danmark.

Pengeinstitutter, der ønsker at udstede Dankort, skal indgå en licensaftale med Nets. Ved indgåelse af licensaftalen forpligter pengeinstitutterne sig bl.a. til at opfylde Dankort-schemereglerne, som stiller krav til sikkerhed mv. For at opnå licens kræves det, at udsteder er et pengeinstitut under tilsyn af Finanstilsynet eller tilsvarende myndighed i et andet land inden for EU. Endvidere kræves det, at udsteder har indgået aftale med Finans Danmark, som ejer Sumclearingen.

Nets har indgået licensaftaler med 77 pengeinstitutter, heraf er 6 udenlandske filialer i Danmark.

For at kunne modtage Dankort skal en forretning have indgået en betalingskortaftale med Nets. Der er tale om standardvilkår, som er ens for alle be-

talingsmodtagere; dog skelnes der mellem krav til fysisk handel og ikke-fysisk handel.

Kortholder er den person, som kortet er udstedt til, og som har ret til at bruge kortet.

Andre aktører er fx

- udbydere af såkaldte betalingsmoduler – eller gateways – til handel på internettet,
- terminalleverandører og
- kortproducenter.

Forløb af en Dankort-betaling

En Dankort-betaling gennemføres i en række trin. Først initieres betalingen ved, at kortholder benytter kortet i en forretning, og afslutningsvist indsættes beløbet på forretningens konto. De trin, der er forbundet med en Dankort-betaling i den fysiske handel, er beskrevet i boks 1. Da Nets varetager flere funktioner i behandlingen af en betaling, jf. ovenfor, er Nets' rolle i de enkelte trin angivet i parentes.

Da afviklingen i Sumclearingen foregår om natten, tager hele forløbet af en Dankort-betaling typisk en dag, dvs. foretages betalingen en onsdag, vil pengene blive indsat på forretningens konto torsdag. I weekender og på helligdage tager afviklingen længere tid.

Nationalbankens overvågning

Nationalbankens overvågning af de vigtigste danske betalingsløsninger er forankret i Nationalbanklovens § 1, hvoraf det fremgår, at Nationalbanken har til opgave at "opretholde et sikkert pengevæsen her i landet samt at lette og regulere pengeomsætning og kreditgivning". Rammerne for overvågningen er nærmere beskrevet i Nationalbankens overvågningspolitik ([link](#)). Overvågningen af Dankort sker i henhold til ECB's generelle standarder for betalingsløsninger fra 2009, som er udmøntet i specifikke rammer for overvågning af kortsystemer ([link](#)).

ECB's standarder stiller krav om:

1. Et velfunderet juridisk grundlag i alle relevante jurisdiktioner.
2. Adgang til komplet information for alle aktører inkl. relevant information om finansielle risici.
3. Tilstrækkelig sikkerhed, operationel stabilitet og forretningsvidereførelse.
4. Effektiv og pålidelig ledelse og styring med klar rolle- og ansvarsfordeling.
5. At finansielle risici i relation til clearing og afvikling er styrede og begrænsede.

Forløbet af en dankortbetaling

Boks 1

1. Betalingen initieres ved, at kortholder bruger sit kort i forretningens terminal, indtaster sin PIN-kode og godkender betalingen.
2. Forretningen sender, via Nets eller anden transaktionsindsamler, en forespørgsel til Nets (indløser) for verifikation af kort og kode.
3. Nets (indløser) sender forespørgslen til Nets (kortudstederservice), der enten godkender eller afslår betalingsanmodningen.
4. Nets (indløser) modtager svar fra Nets (kortudstederservice), der videreformidles til forretningens terminal.
5. Hvis betalingen godkendes, går transaktionen igennem, og forretningen udleverer varen.
6. Forretningen sender en anmodning til Nets (indløser) om at modtage penge for købet. Nets (indløser) videresender anmodningen til Nets (processor), der leverer den infrastruktur mellem kortudsteder og kortindløser, der sikrer udveksling af information mellem parterne.
7. 10 gange daglig sendes information fra Nets (processor) til kortholders pengeinstitut om køb foretaget med Dankort – og kortholders konto debiteres.
8. Nets (processor) er ansvarlig for og stiller clearing og afvikling til rådighed for parterne i Dankort. Nets (processor) samler dagens dankorttransaktioner og andre betalinger, der indgår i PBS-clearingen, og beregner, hvad det enkelte pengeinstitut skal betale eller modtage fra hvert af de øvrige pengeinstitutter. Disse beløb sendes til Sumclearingen, hvor de lægges sammen med de tilsvarende beløb fra den dokumentløse clearing.¹
9. I Sumclearingen foretages den endelige clearing og afvikling på pengeinstitutternes afviklingskonti i Nationalbanken.
10. Efter afvikling i Sumclearingen indsætter forretningens pengeinstitut beløbet på dennes konto.

¹ Dankort-transaktioner cleares i PBS-clearingen og i den dokumentløse clearing, der begge er en del af Sumclearingen. I PBS-clearingen indgår fx dankortbetalinger via fysiske online-terminaler i forretninger og køb på internettet, betalinger i udlandet med Visa/Dankort og internationale debetkort udstedt af danske pengeinstitutter. I den dokumentløse clearing indgår kontanthævninger med Dankort i en filial eller i en kortautomat hos andre pengeinstitutter end kortholders.

Nationalbanken overvåger clearing- og afviklings-systemer i andet regi, og de dele af Standard 5, der er omfattet af denne overvågning, er ikke vurderet i forbindelse med vurderingen af Dankort.

Samarbejde mellem Nationalbanken og Finanstilsynet

Nationalbanken samarbejder med Finanstilsynet, jf. den samarbejdsaftale, der er indgået af de to myndigheder ([link](#)). Samarbejdet har fokus på at undgå dobbelt myndighedskontrol og at udnytte myndighedernes ressourcer bedst muligt.

Finanstilsynets tilsyn med Nets er beskrevet i boks 2. I relation til Nets har Nationalbankens arbejde flere grænseflader til Finanstilsynets arbejde. Helt overordnet holder Nationalbanken og Finanstilsynet løbende hinanden orienteret om sager, og Nationalbanken deltager som observatør på tilsynets it-inspektioner hos Nets.

Finanstilsynets it-inspektioner er beskrevet nærmere i boks 3. Nationalbankens vurderinger af Nets' efterlevelse af de dele af ECB's Standard 3 og 4, som bl.a. omhandler it-sikkerhedsstyring, drift, beredskabsplaner, outsourcing og revision, bygger så vidt muligt på Finanstilsynets arbejde. Som udgangspunkt vurderer Nationalbanken ikke områder, som Finanstilsynet fører tilsyn med. Det sker kun i de tilfælde, hvor der er en særskilt vinkel til Dankort.

Nets har en tilladelse som betalingsinstitut, bl.a. fordi Nets tilbyder indløsning af Dankort. Finanstilsynet fører derfor tilsyn med, at Nets overholder kravene i Betalingstjenesteloven, herunder påser Finanstilsynet, at Nets efterlever EBA's retningslinjer for sikre internetbetalinger. Betalingstjenesteloven og EBA's retningslinjer for sikre internetbetalinger har overlap til de ECB standarder, som Nationalbanken vurderer Dankort efter, og Nationalbanken og Finanstilsynet samarbejder derfor om forhold, der har berøringsflader til begge myndigheder. Eksempelvis har Nationalbanken fulgt Finanstilsynets og Nets' drøftelser vedrørende sikkerhedsløsningen "Dankort Secured by Nets", som benyttes ved betalinger med Dankort på internettet. Løsningen, der medfører, at der er stærk autentifikation ved betalinger på internettet, er samtidig væsentlig for Nets' efterlevelse af et af kravene i Standard 3, som netop kræver, at der kan foretages stærk autentifikation, når der betales med kort, både i fysisk handel og i ikke-fysisk handel.

Finanstilsynets tilsyn af Nets som datacentral og betalingsinstitut

Boks 2

Nets er en datacentral, der er væsentlig for den danske betalingsinfrastruktur, jf. § 343q, Lov om finansiell virksomhed (FIL) ([link](#)). Det fremgår af kapitel 20c i FIL, at datacentralerne skal efterleve regler om betryggende kontrol- og sikringsforanstaltninger på it-området. De nærmere regler er fastsat af Ledelsesbekendtgørelsens bilag 5 om it-sikkerhed ([link](#)).

Nets er i øvrigt omfattet af Bekendtgørelse om systemrevisionens gennemførelse i fælles datacentraler ([link](#)).

Nets skal desuden iagttage de samme regler ved outsourcing, som gælder finansielle virksomheder som fx pengeinstitutter, jf. Bekendtgørelse om outsourcing af væsentlige aktivitetsområder ([link](#)).

Finanstilsynet fører tilsyn med reglernes overholdelse og foretager en række aktiviteter i forbindelse med tilsynet af Nets. Finanstilsynet

- gennemfører efter en risikobaseret tilgang it-inspektioner (se yderligere om disse i boks 3),
- orienteres løbende om væsentlige hændelser,
- gennemgår systemrevisionens protokollater.

Finanstilsynet giver i henhold til Betalingstjenesteloven tilladelse til og fører tilsyn med betalingsinstitutter, herunder Nets ([link](#)). Tilladelsen bygger på en gennemgang af, at lovens krav er opfyldt.

Finanstilsynet fører løbende tilsyn med, at Nets opfylder Betalingstjenesteloven, herunder godkender Finanstilsynet outsourcing af væsentlige driftsmæssige funktioner. Finanstilsynet har indarbejdet EBA's retningslinjer for sikre internetbetalinger ([link](#)) i tilsynet med betalingstjenesteloven.

Grænseflader til andre myndigheder

Nationalbankens arbejde har grænseflader til andre myndigheder end Finanstilsynet.

Det gælder Konkurrence- og Forbrugerstyrelsen, der bl.a.

- fører tilsyn med overholdelse af adgang til betalingssystemer, jf. §40, Betalingstjenesteloven ([link](#)),
- gennemfører omkostningsstudier af Dankort som beskrevet i bekendtgørelse nr. 605 af 03/06/2016 ([link](#)) samt
- fører tilsyn med, at Nets opfylder forordningen om interbankgebyrer for kortbaserede betalings-transaktioner, den såkaldte MIF-forordning ([link](#)). MIF-forordningen har til formål at medvirke til, at der opnås øget konkurrence om de ydelser, der leveres i forbindelse med en kortbetaling.

Nationalbanken har også grænseflader til Datatilsynet, der påser, at Persondataloven efterleves ([link](#)).

Nationalbanken har ikke vurderet de områder, som ligger inden for de nævnte myndigheders ressort.

Afgrænsning og metode

Nationalbankens vurdering af Dankort er baseret på Nets' egenvurdering, som indeholder Nets' svar på en lang række spørgsmål relateret til ECB's standarder for kortsystemer. Nets har desuden fremsendt omfattende dokumentation, herunder aftalesæt i relation til Dankorts aktører, organisationsplaner, sikkerhedspolitik, risikoanalyser mv. Nationalbanken og Nets har løbende haft drøftelser om vurderingen.

Nationalbanken har på baggrund af vurderingen givet en række anbefalinger og bemærkninger til Nets. Disse anbefalinger og bemærkninger er gennemgået i det følgende.

Finanstilsynets it-inspektioner

Boks 3

Finanstilsynet tilpasser it-inspektionerne til den konkrete virksomhed, der undersøges, bl.a. på baggrund af en vurdering af væsentlighed og risiko. Følgende områder vil ofte indgå i en it-inspektion:

- It-strategi, it-sikkerhedsstrategi og it-governance, herunder it-sikkerhedsstyring og it-risikostyring
- It-beredskabsplanlægning og test af it-beredskabet
- Outsourcing – efterlevelse af outsourcingbekendtgørelsen og kontrol med leverandører
- Rettighedstildeling, adgangsstyring og logiske adgangskontroller
- Fysisk sikring og adgangsstyring
- It-driftsafvikling og overvågning
- Systemrevision – intern og ekstern
- Change management og projektstyring
- Administration og vedligeholdelse af netværk og systemprogrammer
- Strategi og sikringsforanstaltninger mod it-kriminalitet.

Kilde: Finanstilsynets hjemmeside ([link](#)).

Samlet bedømmelse

Nationalbanken har foretaget en vurdering af Dankort mod ECB-standard.

Bedømmelsen af de fem standarder kan antage én af fem kategorier: *Observed*, *broadly observed*, *partly observed*, *not observed* eller *not applicable*, jf. boks 4.

Nationalbankens vurdering af Dankort er som følger:

Standard 1 (Et velfunderet juridisk grundlag i alle relevante jurisdiktioner): *Broadly observed*

Standard 2 (Adgang til komplet information for alle aktører inkl. relevant information om finansielle risici): *Broadly observed*

Standard 3 (Tilstrækkelig sikkerhed, operationel stabilitet og forretningsvidereførelse): *Partly observed*

Standard 4 (Effektiv og pålidelig ledelse og styring med klar rolle- og ansvarsfordeling): *Broadly observed*

Standard 5 (At finansielle risici i relation til clearing og afvikling er styrede og begrænsede): *Observed*

Dankort efterlever mange af de krav, som ECB stiller til kortsystemer. Nationalbanken har imidlertid identificeret forbedringspotentiale. På de væsentligste områder er givet en anbefaling. På de andre områder er givet en bemærkning.

Nets bør adressere anbefalinger og bemærkninger. Nationalbanken vil følge op på fremdriften i forbindelse med Nationalbankens løbende overvågning.

Nedenfor beskrives Nationalbankens vurdering af Nets' efterlevelse af kravene i ECB-standard for kortsystemer. For hver standard beskrives først ECB's krav, og Nationalbankens overordnede bedømmelse af Nets' efterlevelse af dem. Afslutningsvist beskrives Nationalbankens anbefalinger og bemærkninger til de enkelte standarder.

Skala for vurdering af standarden

Boks 4

I bedømmelsen af hver standard er der anvendt følgende retningslinjer for brugen af kategorierne:

- *Observed* benyttes, når alle væsentlige kriterier er efterlevet, og eventuelle mangler er af mindre karakter, og tilpasninger kan ske løbende som en del af den normale drift.
- *Broadly observed* benyttes, når der er identificeret en eller flere mangler, der bør adresseres inden for en fastlagt tidsramme.
- *Partly observed* benyttes, når der er identificeret en eller flere væsentlige mangler, der kan blive alvorlige, hvis de ikke straks adresseres. Udbedring af disse bør have høj prioritet.
- *Not observed* benyttes, når der er identificeret en eller flere alvorlige mangler, der kræver omgående handling. Udbedring af disse bør have højeste prioritet.
- *Not applicable* benyttes, når standarden ikke finder anvendelse på grund af strukturelle, juridiske eller institutionelle forhold.

Standard 1: Et velfunderet juridisk grundlag i alle relevante jurisdiktioner

Standard 1 vedrører det juridiske grundlag for kortsystemet, herunder:

- Lovgivning og kompetente domstole skal være klart identificerede.
- Relevant national lovgivning og EU-lovgivning skal efterleves, og kortorganisationen skal løbende foretage vurderinger af, om lovgivningen bliver overholdt.
- Kortsystemets regler og procedurer skal være komplette, entydige og skal håndhæves.
- Kortsystemets aktører skal indgå juridisk bindende aftaler, og disse aftaler skal være komplette, entydige og skal håndhæves.

Nationalbanken har forholdt sig til, om Nets har en proces for at sikre, at relevant lovgivning er overholdt. Nationalbanken har ikke vurderet, om Nets opfylder relevante love, idet der er andre myndigheder, der påser dette, herunder primært Finanstilsynet, Konkurrence- og Forbrugerstyrelsen samt Datatilsynet.

Vurdering

Dankort-schemet opererer alene i Danmark og er underlagt dansk ret.

Nets har i 2016 startet et "regulatory forum", der har til formål at sikre en ensartet proces for opfølgning på nye love og regler eller ændringer i eksisterende love og regler.

Regler og procedurer for Dankort er udmøntet i Dankort-schemereglene. Aktører i schemet skal hvert år afgive en ledelseserklæring og en revisor-påtegnet erklæring til Nets om, at schemereglernes sikkerhedskrav er overholdt. Nets sikrer håndhævelse af reglerne ved at følge op på bemærkninger og forbehold. Nets opdaterer løbende Dankort-schemereglene. Fx blev reglerne ændret ved udstedelse af kort med kontaktløs funktion. Nets har oplyst, at de ikke har modtaget klager vedrørende schemereglene. Hvis en aktør påpeger en uhensigtsmæssighed, indgår Nets i en dialog herom og ændrer i reglerne, hvis det skønnes formålstjenligt.

Nets har udarbejdet standardkontrakter for kortudstedere og forretninger, henholdsvis en licensaftale og en betalingskortaftale. I aftalerne beskrives, hvor-

dan de håndhæves, herunder handlemulighederne ved misligholdelse, og hvordan tvister skal løses. Nets sikrer, at aftalerne er entydige ved at foretage ændringer, hvis Nets bliver opmærksom på, at noget er uklart. Fx blev betalingskortaftalen ændret for at tydeliggøre, at det er forretningens ansvar at fremsende information om lukning af forretningen til Nets. Kompletthed sikres ved at ændre i relevante aftaler og regler, fx ved nye funktionaliteter såsom kontaktløs funktion.

Standard 1 vurderes at være: Broadly observed med følgende anbefalinger og bemærkninger:

Anbefaling til Standard 1

Nationalbanken anbefaler, at arbejdet i Nets' "regulatory forum" i højere grad formaliseres og struktureres. Der bør være en klar og dokumenteret rolle- og ansvarsfordeling for arbejdet, herunder hvordan roller og ansvar er fordelt mellem Nets' første, anden og tredje organisatoriske forsvarslinje, dvs. henholdsvis de operative enheder, compliancefunktionen og den interne revision.

Bemærkning til Standard 1

Nets foretager ændringer i relevante aftaler og regler, når der er behov herfor. Der er ikke udarbejdet en formel forretningsgang for opdatering af aftaler og regler vedrørende Dankort-schemet. Nets bør udarbejde en sådan. Det vil sikre, at relevante ændringer foretages på et klart og systematisk grundlag, og det vil mindske tab af viden, hvis centrale medarbejdere stopper.

Standard 2: Adgang til komplet information for alle aktører inkl. relevant information om finansielle risici

Standard 2 vedrører en tydelig rolle- og ansvarsfordeling og adgang til information, herunder:

- Roller og ansvar afledt af regler og kontraktuelle forhold for kortsystemets aktører skal dokumenteres klart og opdateres løbende.
- Der skal være en procedure for at klassificere information.
- Relevant information skal være tilgængelig for nuværende og potentielle aktører.
- Der er specifikke krav til information vedrørende 1) priser og gebyrer, 2) finansielle risici ved at deltage i Dankort, 3) indsigelser, 4) misbrug og 5) imødegåelse af misbrug, herunder krav til, hvilken information kortorganisationen skal sikre, at kortholdere får fra deres udsteder.
- Ved driftsforstyrrelser i kortsystemet stilles krav til kommunikation med relevante aktører. Der stilles desuden krav om kommunikation ved store ændringer.

Vurdering

De forskellige aktørers roller og ansvar i Dankort fremgår af Dankort-schemereglene. Schemereglene er opbygget systematisk, og det fremgår tydeligt, hvilke aktører der er ansvarlige for at efterleve hvilke krav.

Nets har udarbejdet procedurer for klassificering af information.

Alle aktører i Dankort kan finde information om Dankort på nets.eu og dankort.dk. Udstedere har desuden adgang til et lukket site, INFONET, hvor bl.a. prislister for licenshavere fremgår, mens forretningerne kan finde priser på Nets' hjemmeside. Information om finansielle risici fremgår af relevante aftaler og regler.

Nets stiller et indsigelsessystem til rådighed for udstederne, CLARA, og alle indsigelser sendes via dette system til Nets.

Information om misbrug og seneste misbrugstrends offentliggøres på nets.eu. Nets' arbejde med misbrug behandles detaljeret under Standard 3.

Der er krav til, hvilken information Nets skal sikre, at kortholderne får fra deres udsteder, fx vedrørende diverse sikkerhedstiltag. Nets har pålagt kortudstederne nogle af disse krav, idet de indgår i Dankort-schemereglene bl.a. i form af kortholderregler, som alle udstedere skal bruge. Det er ikke alle ECB's krav, der indgår i schemereglene, og dermed pålægger Nets ikke udstederne alle ECB-standardens krav.

Ved driftsforstyrrelser informerer Nets relevante interessenter via Nets' informationssystem (infocast). Nets har desuden et set-up for håndtering af hændelser.

Kommunikation af store ændringer til Dankort-schemets aktører sker til dels i Kortudvalget, Bankgruppen og Samarbejdsforum, hvor ændringer drøftes. I Kortudvalget og Bankgruppen deltager repræsentanter for de pengeinstitutter, der udsteder Dankort. I Samarbejdsforum deltager repræsentanter for detailhandelen og de pengeinstitutter, der udsteder Dankort. Desuden har projekter i Nets et kommunikationsspor rettet mod de forskellige interessenter.

Standard 2 vurderes at være: Broadly observed med følgende anbefalinger og bemærkninger:

Anbefaling til Standard 2 (1)

I ECB-standardens krav er der krav til, hvilken information Nets skal sikre, at kortholderne får fra deres udsteder. Nets bør pålægge udstederne at efterleve alle ECB-standardens krav til udstedere. Det vil sikre, at udstederne implementerer tiltagene på en ensartet og hensigtsmæssig måde, og at Nets har mulighed for at følge op på implementeringen.

Anbefaling til Standard 2 (2)

Nets bør udarbejde en generel og formel kommunikationsplan, der sikrer, at relevant information vedrørende Dankort er tilgængelig for relevante aktører via passende kommunikationskanaler, herunder kommunikation til relevante aktører ved større driftsforstyrrelser samt ved store ændringer.

Bemærkning til Standard 2

Nets har udarbejdet procedurer for klassificering af information. Nets bør sikre, at procedurerne følges.

Standard 3: Tilstrækkelig sikkerhed, operationel stabilitet og forretningsvidereførelse

Standard 3 stiller krav til en række områder, der understøtter en sikker og stabil drift. Områderne er behandlet hver for sig i det følgende:

- Kortorganisationens sikkerhedsstyring
- Fremstilling og distribution af kort
- Transaktioner
- Clearing og afvikling
- Beredskabsplanlægning
- Outsourcing

Det bemærkes, at Nets har fokus på efterlevelse af krav fra de internationale kortselskaber, fx VISA. De internationale kortselskaber påser, at deres krav efterleves. Det gælder fx krav til PCI-PIN ([link](#)) og PCI-DSS ([link](#)).

Standard 3 vurderes samlet set at være: Partly observed. Vurderingerne af de ovennævnte områder er gennemgået ét for ét, efterfulgt af de anbefalinger og bemærkninger, der knytter sig til det enkelte område.

Krav til kortorganisationens sikkerhedsstyring

Standardens krav vedrørende sikkerhedsstyring omfatter krav til:

- Kortsystemets sikkerhedspolitik og risikostyring.
- Operationelle krav vedrørende drift, hændelseshåndtering, ændringshåndtering, adgangspolitik, funktionsadskillelse, beskyttelse af sensitive data, og it- og datasikkerhed.
- Ledelse og medarbejdere, herunder krav til dokumenteret overblik over roller og ansvar.
- Assistance til kunderne 24/7.

Der er grænseflader til andre myndigheder. Finanstilsynet fører tilsyn med Nets' generelle it-sikkerhedsstyring, strategi, sikkerhedspolitikker og retningslinjer, samt Nets' procedurer for styring af adgange til systemer og funktionsadskillelse. Desuden fører Finanstilsynet tilsyn med Nets' hændelseshåndtering og ændringshåndtering. Datatilsynet påser, at Nets opfylder Persondataloven. Nationalbanken har ikke vurderet, om Nets opfylder Persondataloven.

Vurdering

Nets' sikkerhedspolitik har fokus på sikkerheden i Nets som virksomhed, mens Dankort-schemeregler-

ne er en udmøntning af regler og sikkerhedskrav til Dankorts aktører.

Nets' sikkerhedspolitik fastsætter de generelle retningslinjer for it- og datasikkerhed i Nets. Sikkerhedspolitikken stiller desuden en række krav til medarbejdere i Nets, fx vedrørende obligatorisk træning i sikkerheds-awareness.

Nets udarbejder risikoanalyser af den it-platform, som Dankort kører på. Alle risici vurderes i samarbejde mellem it-ejer og Group Risk Management. Risici, som vurderes at have stor konsekvens eller høj sandsynlighed, præsenteres for forretningsejer, og der fastlægges en handlingsplan. Aktiviteter til nedbringelse af en risiko skal beskrives, have en ejer og et gennemførelsestidspunkt. Der følges op på fremdriften.

Nets monitorerer den teknologiske udvikling og forbedrer løbende sikkerhed i Dankort.

Dankort kører stabilt. Der er kun få hændelser og nedbrud, der påvirker driftsstabiliteten. Ved nedbrud opfordrer Nets forretningerne til at benytte offline-funktionaliteten i terminalerne, så der fortsat kan tages imod betalinger. Nets har formaliserede procedurer for hændelses- og ændringshåndtering, samt for styring af adgange og funktionsadskillelse, som gælder for hele organisationen.

Nets har fremsendt organisationsdiagrammer for de dele af organisationen, der har en rolle i Dankort.

Nets yder kundeassistance 24/7.

Anbefaling til Standard 3 (1)

Nets udarbejder i dag risikoanalyser af den it-platform, som Dankort kører på. Dette arbejde bør udvides i form af en risikovurdering, der dækker alle relevante aspekter af Dankort, herunder organisation, personale, infrastruktur, tekniske emner, mulige sikkerhedsmæssige trusler og operationelle funktioner. Formålet er at få et samlet overblik over risici i relation til Dankort, således at der kan etableres passende kontrol- og sikringsforanstaltninger, og foretages de rette prioriteringer.

Anbefaling til Standard 3 (2)

Nets bør dokumentere og vedligeholde et samlet overblik over organiseringen af Dankort, herunder skal roller og ansvar tydeligt fremgå. Overblikket skal sikre en forståelse af og overblik over de forskellige funktioner i Nets, der håndterer aspekter af Dankort.

Anbefaling til Standard 3 (3)

Den enhed hos Nets, som har ansvaret for Dankort, bør skabe og vedligeholde et samlet overblik over hændelser og andre relevante informationer om it- og datasikkerhed, der vedrører Dankort. Disse input er væsentlige elementer i den samlede vurdering af, hvordan Dankort fungerer, og bør bl.a. benyttes i forbindelse med risikovurderingen af Dankort.

Krav til fremstilling og distribution af kort

Standarden stiller sikkerhedskrav til:

- Kort og terminaler
- Personalisering og levering af kort
- Produktion og installering af terminaler mv.

Kortorganisationen skal endvidere sikre, at kortholdere kan autentificere sig ved brug af stærk autentifikation.

Vurdering

Nets definerer sikkerhedskrav til kort og terminaler i Dankort-schemereglerne. Nets godkender alle terminaler, der kan benyttes under betalingskortaftalen. Der udstedes ikke kort uden om Nets.

Schemereglerne indeholder en række krav til procedurer og kontroller angående personalisering og levering af kort. Fx skal kortenes udformning følge særlige specifikationer. Der er endvidere krav til bestilling af Dankort og PIN-kode, returnerede PIN-kode-breve, forsendelsen fra kortleverandør, aktivering af kortet, behandling af kort hos udsteder, fornyelse og udskiftning af kort, spærring eller sletning af kort samt til håndtering af inddragne/indleverede kort. Der skal altid benyttes godkendte leverandører og producenter ved personalisering og levering af Dankort. Nets oplever ikke misbrug i forbindelse med personalisering og levering af kort.

Nets har udarbejdet kravspecifikation til terminaler, og der foreligger en skriftlig procedure for godkendelse af terminaler. Nets stiller desuden krav til opsætningen af terminalerne. Nets er ikke bekendt med brud på kontroller i forhold til terminalerne.

Nets stiller krav til autentifikations-procedurerne. I fysisk handel skal der benyttes PIN-kode, bortset fra kontaktløse betalinger under 200 kr. Der kan desuden afviges fra stærk autentifikation i fx brooverfarter og ved betaling af parkeringsafgifter. Begrundelsen er, at varerne er ikke omsættelige, og at transaktionshastigheden er af væsentlig betydning. Nets stiller "Dankort Secured by Nets" til rådighed på internettet for transaktioner over 450 kr., så disse kan foretages med stærk autentifikation. "Dankort Secured by Nets" fungerer således, at kortholder ved køb for over 450 kr. modtager en sms med en kode, der skal benyttes til at afslutte købet.

Krav til transaktioner

Standarden indeholder krav til:

- Gyldighedsperioder for betalingskort, betalingssessioner mv.
- Monitorering af, reaktion på og imødegåelse af misbrug.
- Beviser for transaktioners gyldighed
- Logning af transaktioner, adgang til systemer og data, mv.
- Kapacitetsstyring og -planlægning.

Finanstilsynets fører tilsyn med Nets' logning samt kapacitetsstyring og -planlægning.

Vurdering

Schemereglerne angiver gyldighedsperioden, som for Visa/Dankort højst må være 4 år regnet fra udstedelsesmåneden plus 3 måneder. PIN-koden følger kortet. Det betyder, at så længe kortet blot fornyes, kan PIN-koden følge det nye kort. Der må maksimalt foretages 3 forkerte forsøg på at skrive PIN-koden, før kortet spærres. Et spærret Dankort kan låses op igen. Hvis kortet er kompromitteret, skal det lukkes, og der skal udstedes et nyt kort.

Nets overvåger alle Dankort-transaktioner baseret på erfaring og foretager løbende analyser af misbruget med Dankort. Nets har igangsat to initiativer i 2017 med fokus på at mindske misbruget. Det ene er et "fraud prevention"-værktøj, der ved hjælp af kunstig intelligens analyserer misbrugstendenser og bruger resultaterne til at identificere forsøg på misbrug. Det andet er "Dankort Secured by Nets", jf. ovenfor. Misbrug med Dankort er lavt i international sammenligning.

Ved internetbetalinger kræver Nets, at der er time out for browservinduet efter maksimalt 15 minut-

ter. Der er ikke en mekanisme, der forhindrer dobbelt log-in på internettet, fx samtidig login på PC og Ipad. Nets følger udviklingen i misbrug tæt og har ikke oplevet misbrug som følge af, at der kan foretages dobbelt log-in.

Nets har klare regler for, hvornår og hvordan returneringen af en Dankort-transaktion skal finde sted, hvis en transaktion afvises af brugeren. I situationer, hvor kortholder ikke kan vedkende sig en transaktion gennemført i fysisk handel med PIN-kode/underskrift, og hvor chippen er aflæst, er der særlige regler for behandling af indsigelsen, idet der kan være tale om falske eller forfalskede kort. Hvis Nets beder om dokumentation for en kortbetaling, skal forretningen levere denne til Nets. Forretningen skal opbevare transaktionsdokumentation i 20 måneder regnet fra betalingsdatoen.

Nets har udarbejdet procedurer for logning af adgange til systemer og data, udførte handlinger i produktionsmiljøet mv.

Nets overvåger kortsystemet med henblik på at sikre, at der er kapacitet nok i systemet, også når belastningen er stor. Nets kan tilvejebringe ekstra kapacitet med kort varsel.

Bemærkning til Standard 3 (1)

Indberetninger vedrørende misbrug til Nets foregår manuelt. Nets har allerede planlagt et projekt vedrørende elektronisk indberetning af misbrug. Nets bør igangsætte projektet.

Bemærkning til Standard 3 (2)

I ECB-standardens er det et specifikt krav, at kortholder skal kunne vælge, at Dankort ikke kan anvendes til internethandel. Nets bør analysere kortholdernes behov for at kunne vælge, og muligheden for at lave en sådan løsning.

Bemærkning til Standard 3 (3)

Nets bør undersøge muligheden for, at alle kontantudtag i hæveautomater bliver en del af den centrale autorisationsproces hos Nets. Det vil styrke Nets' overvågning og forebyggelse af misbrug med Dankort.

Krav til clearing og afvikling

Kortorganisationen skal definere tekniske og organisatoriske sikkerhedskrav til clearing og afvikling, som fx relaterer sig til kapacitet, tilgængelighed, stabilitet, fortrolighed og mulighed for revision.

Vurdering

En Dankort-transaktion indgår først i PBS-clearingen (eller den dokumentløse clearing), og derefter Sumclearingen. Nationalbanken overvåger de nævnte clearinger i andet regi. Forhold vedrørende disse er derfor ikke vurderet i forbindelse med vurderingen af Dankort, jf. denne rapportes tekst under Standard 5.

Krav til beredskabsplanlægning

Standarden stiller krav til beredskabet. Der skal være:

- "Business impact analyses" (BIA'er), der identificerer de komponenter, der er centrale for kortsystemets funktion.
- Der skal være beredskabsplaner og test af disse.

Finanstilsynet fører tilsyn med Nets' arbejde med beredskabsplanlægning og test heraf.

Vurdering

Nets har siden 2016 udarbejdet BIA'er for kritiske services, herunder Dankort. Der er en række BIA'er, der er relevante for Dankort, herunder BIA'er vedrørende transaktionsbehandling, internethandel, kortproduktion, kortaktivering og autorisation.

Nets har en beredskabsplan, der med afsæt i de udarbejdede BIA'er opererer med krav til genetableringstider. Planen omfatter bl.a. beredskabet i forbindelse med Dankort. Derudover har Nets en plan for krisestyring, herunder krisekommunikation.

Nets tester løbende beredskabsplanen og planen for krisestyring. Forbedringspunkter dokumenteres og ansvarsplaceres.

Bemærkning til Standard 3 (4)

Nets bør genoverveje, hvilke BIA'er, der er relevante for Dankort, fx vil BIA'er vedrørende clearingsystemerne være relevante. Nets bør færdiggøre BIA'er inden for alle de områder, der er relevante for Dankort.

Krav til outsourcing

Standarden indeholder følgende krav til outsourcing:

- Risici relateret til outsourcing skal analyseres af outsourcing-virksomheden, og der skal stilles krav om, at leverandører analyserer egne risici i relation til de outsourcede aktiviteter.
- Kontrakter skal omfatte alle relevante forhold i forbindelse med de outsourcede aktiviteter, herunder beskrivelser af de forventede serviceniveauer.

- Der skal være en proces for monitorering og opfølgning på sikkerhed og tilgængelighed af de outsourcede services.

Finanstilsynet fører tilsyn med Nets' outsourcing af it-funktioner.

Vurdering

Nets outsourcer en række funktioner i relation til Dankort.

Nets har en proces for håndtering af outsourcing. Der udarbejdes kontrakter, bl.a. med bestemmelser vedrørende de forventede serviceniveauer. Nets foretager risikovurderinger af outsourcede services og kræver, at driftsleverandører gennemfører egne risikovurderinger. For en mindre leverandør til Dankort har Nets ikke opdateret sin risikovurdering på årlig basis.

Samme leverandør til Dankort efterlever ikke Nets' it-sikkerhedspolitik, ligesom Nets' monitorering og opfølgning på sikkerhed og tilgængelighed af outsourcede services i visse tilfælde ikke er fastlagt efter en sammenhængende og konsistent procedure.

Anbefaling til Standard 3 (4)

Nets bør på årlig basis opdatere sine risikoanalyser af alle outsourcede funktioner med relation til Dankort. Nets bør i den forbindelse indarbejde leverandørernes egne risikoanalyser af de outsourcede aktiviteter. Risikoanalysen bør danne udgangspunkt for etablering af passende kontrol- og sikringsforanstaltninger, og risici ved outsourcing bør være et væsentligt element i risikovurderingen af Dankort.

Anbefaling til Standard 3 (5)

Nets bør sikre, at leverandører til Dankort efterlever Nets' it-sikkerhedspolitik. Nets' monitorering og opfølgning på sikkerhed og tilgængelighed af de outsourcede services bør generelt ske på en systematisk og regelmæssig måde, som bør dokumenteres og kvalitetssikres.

Standard 4: Effektiv og pålidelig ledelse og styring med klar rolle- og ansvarsfordeling

Standarden stiller krav om:

- Klart definerede, effektive og transparente processer for beslutninger om forretningsmæssige mål og politikker.
- Roller og ansvar skal være klart definerede.
- Objektive, fair og transparente adgangskriterier for udstedere og indlødere.
- Effektive og transparente processer til at vurdere de services, der tilbydes kunderne.
- Effektivt internt kontrol framework, herunder revisionsfunktion.
- Løbende kontrol af de forretninger, der håndterer sensitive betalingsdata.

Finanstilsynet fører tilsyn med Nets' krav og procedurer vedrørende kontrol og rapportering. Konkurrence- og Forbrugerstyrelsen er myndighed vedrørende konkurrencespørgsmål. Nationalbanken har ikke forholdt sig til konkurrencespørgsmål.

Vurdering

Nets ejer Dankort, og Nets træffer de endelige beslutninger om produktet. Nets samarbejder med repræsentanter for udstederne og detailhandelen. Samarbejdet foregår i Bankgruppen, Kortudvalget og i Samarbejdsforum. Desuden nedsættes lejlighedsvis diverse arbejdsgrupper.

Udstedere skal opfylde en række kriterier for at kunne få licens og skal indgive ansøgning om licens til Nets, som ud fra en konkret vurdering afgør, om der kan gives licens. Nets har aldrig givet afslag på en udsteders ansøgning om licens. Ifølge licensbetingelserne er Nets ene-indløser af Dankort. Indløsningsgebyret er reguleret ved lov og bestemt af omkostningerne ved at drive Dankort.

Nets foretager en "Continual Service Improvement"-måling en gang om året, også kaldet CSI-måling. CSI-målingen er målrettet Nets' kunder, fx udstedere og forretninger. Resultatet fremlægges for bestyrelsen. Målingen er ikke produktrettet. Nets kan derfor ikke særskilt opgøre de resultater, der knytter sig til Dankort. Nets kender kun til kortholdernes vurdering af Dankort, hvis udstederne informerer Nets om de henvendelser, som de får.

Ansvaret for kontrol og sikkerhed er organiseret i tre forsvarslinjer (første, anden og tredje linje), dvs. henholdsvis de operative enheder, compliancefunktionen og den interne revision. Der foretages både intern og ekstern systemrevision. Nets initierer også revisioner af de virksomheder, som Nets outsourcer til, fx IBM. Intern revision følger månedligt op på revisionsanmærkningerne, og hvert kvartal udarbejder intern revision en oversigt over revisionsanmærkningerne til ledelsen. Intern revision kræver, at alle revisionsanmærkninger lukkes inden for 12 måneder fra det afsluttende møde. Hvis det ikke er muligt, skal anmærkningen præsenteres for "Audit Committee" og skal forinden være drøftet med CFO. Det er den ansvarlige revisor, der lukker anmærkningen.

De fysiske forretninger har ikke selv betalingsdata liggende. Nets kræver, at forretningernes terminaler, hvorigennem data sendes, skal være godkendt af Nets og dermed opfylde Nets' sikkerhedskrav, og herunder skal de opfylde PCI-DSS standarden. Internetforretninger skal benytte et internetbetalingsmodul, som er godkendt af Nets, og herunder overholder PCI-DSS standarden. Nets følger en gang årligt op på, om PCI-DSS certifikatet er fornyet.

Standard 4 vurderes at være: Broadly observed med følgende anbefalinger og bemærkninger:

Anbefaling til Standard 4 (1)

Nets bør styrke rammerne omkring beslutningsprocesserne i Kortudvalget, Bankgruppen og Samarbejdsforum. Nets bør sikre, at der er klart definerede, effektive og transparente processer for beslutninger om forretningsmæssige mål og politikker.

Anbefaling til Standard 4 (2)

Den enhed hos Nets, som har ansvaret for Dankort, bør skabe og vedligeholde et samlet overblik over de revisionsanmærkninger, der direkte og indirekte knytter sig til Dankort. Overblikket skal være med til at give et samlet billede af, hvordan Dankort fungerer, og bør bl.a. benyttes i forbindelse med udarbejdelse af en risikovurdering af Dankort.

Bemærkning til Standard 4

Nets laver ikke tilfredshedsundersøgelser med henblik på feedback vedrørende Dankort fra kortholderne. Nets bør undersøge muligheden for at lave en tilfredshedsundersøgelse i samarbejde med kortudstederne. Formålet er at sikre et effektivt Dankort, der lever op til kortholdernes behov.

Standard 5: Finansielle risici i relation til clearing og afvikling er styrede og begrænsede

Standarden stiller krav om:

- Overblik over clearing og afvikling.
- Finansielle risici i relation til clearing og afvikling skal være styrede og begrænsede.

De fleste krav under Standard 5 er ikke vurderet, fordi de vedrører clearing- og afvikling, dvs. PBS-clearingen, den dokumentløse clearing og Sumclearingen. Nationalbanken overvåger clearingerne i andet regi, og de er derfor ikke omfattet af vurderingen af Dankort.

Vurdering

Dankort-transaktioner cleares i PBS-clearingen og i den dokumentløse clearing, der begge er en del af Sumclearingen. I PBS-clearingen indgår eksempelvis Dankort-betalinger via fysiske online-terminaler i forretninger og køb på internettet, betalinger i udlandet med Visa/Dankort og internationale debetkort udstedt af danske pengeinstitutter. I den dokumentløse clearing indgår kontanthævninger med Dankort i en filial eller i en kortautomat hos andre pengeinstitutter end kortholders.

Nets kan som kortorganisation ikke få tab i forbindelse med clearing og afvikling af transaktionerne. Der kan imidlertid forekomme tab i Nets' rolle som indløser af Dankort, hvis kortholder indsender en indsigelse til en forretning, som forretningen ikke kan honorere. Kortholders pengeinstitut har pligt til at forsøge at inddrive Nets' udestående hos forretningen, men hvis det ikke kan ske, er Nets som indløser ansvarlig for eventuelle tab. For at minimere risikoen for tab kan Nets, baseret på sin vurdering af forretningen, forlange, at forretningen som led i sin ansøgning stiller en bankgaranti, før der kan indgås en betalingskortaftale. Nets sikrer desuden, at der for visse typer af betalingskortaftaler, fx spil-virksomhed, er indsat et maksimalt beløb, der kan anvendes pr. kort pr. dag.

Standard 5 vurderes at være: Observed.

Oversigt over anbefalinger og bemærkninger

Oversigt over Nationalbankens anbefalinger og bemærkninger fremgår af tabel 1. Nationalbanken og Nets har aftalt en tidsramme for Nets' opfølgning på anbefalinger og bemærkninger.

Anbefalinger og bemærkninger til Nets – fortsættes

Tabel 1

Anbefalinger

Bemærkninger

Standard 1

Et velfunderet juridisk grundlag i alle relevante jurisdiktioner:

- | | |
|--|--|
| <ul style="list-style-type: none"> Nationalbanken anbefaler, at arbejdet i Nets' "regulatory forum" i højere grad formaliseres og struktureres. Der bør være en klar og dokumenteret rolle- og ansvarsfordeling for arbejdet, herunder hvordan roller og ansvar er fordelt mellem Nets' første, anden og tredje organisatoriske forsvarslinje, dvs. henholdsvis de operative enheder, compliancefunktionen og den interne revision. | <ul style="list-style-type: none"> Nets foretager ændringer i relevante aftaler og regler, når der er behov herfor. Der er ikke udarbejdet en formel forretningsgang for opdatering af aftaler og regler vedrørende Dankort-schemet. Nets bør udarbejde en sådan. Det vil sikre, at relevante ændringer foretages på et klart og systematisk grundlag, og det vil mindske tab af viden, hvis centrale medarbejdere stopper. |
|--|--|

Standard 2

Adgang til komplet information for alle aktører inkl. relevant information om finansielle risici:

- | | |
|--|---|
| <ul style="list-style-type: none"> I ECB-standardens krav til, hvilken information Nets skal sikre, at kortholderne får fra deres udsteder. Nets bør pålægge udstederne at efterleve alle ECB-standardens krav til udstedere. Det vil sikre, at udstederne implementerer tiltagene på en ensartet og hensigtsmæssig måde, og at Nets har mulighed for at følge op på implementeringen. Nets bør udarbejde en generel og formel kommunikationsplan, der sikrer, at relevant information vedrørende Dankort er tilgængelig for relevante aktører via passende kommunikationskanaler, herunder kommunikation til relevante Dankort-aktører ved større driftsforstyrrelser samt ved store ændringer. | <ul style="list-style-type: none"> Nets har udarbejdet procedurer for klassificering af information. Nets bør sikre, at proceduren følges. |
|--|---|

Anbefalinger og bemærkninger til Nets – fortsat

Tabel 1

Anbefalinger

Bemærkninger

Standard 3

Tilstrækkelig sikkerhed, operationel stabilitet og forretningsvidereførelse:

- | | |
|--|--|
| <ul style="list-style-type: none"> • Nets udarbejder i dag risikoanalyser af den it-plattform, som Dankort kører på. Dette arbejde bør udvides i form af en risikovurdering, der dækker alle relevante aspekter af Dankort, herunder organisering, personale, infrastruktur, tekniske emner, mulige sikkerhedsmæssige trusler og operationelle funktioner. Formålet er at få et samlet overblik over risici i relation til Dankort, således at der kan etableres passende kontrol- og sikringsforanstaltninger, og foretages de rette prioriteringer. • Nets bør dokumentere og vedligeholde et samlet overblik over organiseringen af Dankort, herunder skal roller og ansvar tydeligt fremgå. Overblikket skal sikre en forståelse af og overblik over de forskellige funktioner i Nets, der håndterer aspekter af Dankort. • Den enhed hos Nets, som har ansvaret for Dankort, bør skabe og vedligeholde et samlet overblik over hændelser og andre relevante informationer om it- og datasikkerhed, der vedrører Dankort. Disse input er væsentlige elementer i den samlede vurdering af, hvordan Dankort fungerer, og bør bl.a. benyttes i forbindelse med risikovurderingen af Dankort. • Nets bør på årlig basis opdatere sine risikoanalyser af alle outsourcete funktioner med relation til Dankort. Nets bør i den forbindelse indarbejde leverandørernes egne risikoanalyser af de outsourcete aktiviteter. Risikoanalysen bør danne udgangspunkt for etablering af passende kontrol- og sikringsforanstaltninger, og risici ved outsourcing bør være et væsentligt element i risikovurderingen af Dankort. • Nets bør sikre, at leverandører til Dankort efterlever Nets' it-sikkerhedspolitik. Nets' monitorering og opfølgning på sikkerhed og tilgængelighed af de outsourcete services bør generelt ske på en systematisk og regelmæssig måde, som bør dokumenteres og kvalitetssikres. | <ul style="list-style-type: none"> • Indberetninger vedrørende misbrug til Nets foregår manuelt. Nets har allerede planlagt et projekt vedrørende elektronisk indberetning af misbrug. Nets bør igangsætte projektet. • I ECB-standard er det et specifikt krav, at kortholder skal kunne vælge, at Dankort ikke kan anvendes til internethandel. Nets bør analysere kortholdernes behov for at kunne vælge, og muligheden for at lave en sådan løsning. • Nets bør undersøge muligheden for, at alle kontantudtag i hæveautomater bliver en del af den centrale autorisationsproces hos Nets. Det vil styrke Nets' overvågning og forebyggelse af misbrug med Dankort. • Nets bør genoverveje, hvilke BIA'er, der er relevante for Dankort, fx vil BIA'er vedrørende clearingsystemerne være relevante. Nets bør færdiggøre BIA'er inden for alle de områder, der er relevante for Dankort. |
|--|--|

Standard 4

Effektiv og pålidelig ledelse og styring med klar rolle- og ansvarsfordeling:

- | | |
|---|--|
| <ul style="list-style-type: none"> • Nets bør styrke rammerne omkring beslutningsprocesserne i Kortudvalget, Bankgruppen og Samarbejdsforum. Nets bør sikre, at der er klart definerede, effektive og transparente processer for beslutninger om forretningsmæssige mål og politikker. • Den enhed hos Nets, som har ansvaret for Dankort, bør skabe og vedligeholde et samlet overblik over de revisionsanmærkninger, der direkte og indirekte knytter sig til Dankort. Overblikket skal være med til at give et samlet billede af, hvordan Dankort fungerer, og bør bl.a. benyttes i forbindelse med udarbejdelse af en risikovurdering af Dankort. | <ul style="list-style-type: none"> • Nets laver ikke tilfredshedsundersøgelser med henblik på feedback vedrørende Dankort fra kortholderne. Nets bør undersøge muligheden for at lave en tilfredshedsundersøgelse i samarbejde med kortudstederne. Formålet er at sikre et effektivt Dankort, der lever op til kortholdernes behov. |
|---|--|

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

Redaktionen er afsluttet
10. maj 2017

Anne Dyrberg Rommer
ady@nationalbanken.dk

Mikkel Steen Madsen
msn@nationalbanken.dk
FINANSIEL STABILITET



**DANMARKS
NATIONALBANK**