# Dankort Schemeregler

Dateret: 20. november 2026

# Indhold

Ændringslog ..... 4
Definitioner ..... 7
**A – GENERELLE VILKÅR ..... 8**
A.1 – Aftalestruktur ..... 8
A.2 – Governance ..... 8
A.3 – Licensaftale ..... 8
A.4 – Dankort prismodel og gebyrer ..... 9
A.5 – Compliance og tvister ..... 9
**B – KORTUDSTEDELSE ..... 10**
B.1 – Generelle krav ..... 10
B.2 – Behandling af kort hos udsteder ..... 10
B.3 – Tekniske specifikationer og design ..... 11
B.4 – Bestilling af kort ..... 12
B.5 – PIN-kode ..... 13
B.6 – [udgået] ..... 13
B.7 – Forsendelse fra kortleverandør og aktivering ..... 13
B.8 – Fornyelse og udskiftning af kort ..... 14
B.9– Spærring og sletning af kort ..... 15
B.10 – Inddragne/indleverede kort ..... 16
B.11 – Indsigelser og tilbageførsler ..... 16
B.12 – Indberetning af Dankort tredjemandsmisbrug ..... 17
B.13 – Leverandører af produkter (3rd party vendors and suppliers) ..... 18
B.14 – Virtualisering og udstedelse af token ..... 18
**C– INDLØSNING ..... 19**
C.1 – Generelle krav til indløser ..... 19
C.2 – Forpligtelser overfor kontoførende pengeinstitut ..... 20
C.3 – Tilslutning af betalingsmodtager ..... 20
C.4 – Tilslutning af PSP (Payment Service Provider) ..... 21
**D – KORTMODTAGELSE ..... 21**
D.1 – Generelle krav ..... 21
D.2 – Terminaler ..... 22
D.3 – Adgangskontrolsystemer ..... 23
D.4 – Hæveautomater ..... 23

D.5 – Kort ikke tilstede (CNP) ..... 23
D.6 – Dankort Card Manager (DCM) ..... 24
D.7 – [udgået] ..... 25
D.8 – Fordelsprogrammer ..... 25
D.9 – Delegeret autentifikation ..... 26
**E – TRANSAKTIONSBEHANDLING ..... 27**
E.1 – Generelle krav ..... 27
E.2 – Behandling af "kort ikke tilstede" (CNP) transaktioner ..... 27
E.3 – Posteringer på kontoen ..... 28
E.4 – Krav til understøttelse af Dankort Secured by Nets ..... 28
E.5 – Krav til udsteder i forbindelse med Dankort advarselsservice ..... 29
E.6 – Behandling af reservationer for kort med saldokontrol ..... 29

## Ændringslog

| Version | Afsnit | Ændring |
|---|---|---|
| 20.11.2026 | Definitioner | Opdateret definition af ”Licenshaver” til også at omfatte indløsere. Rettet ”indløst” til ”modtaget” i definition af ”Dankort”. |
| | B.14.3 | Præciseret undtagelse fra kravet |
| | C.1.4 + C.1.6 | Frist for indsendelse indsat |
| | C.1.8 – C.1.11 | Tilføjet krav vedr. robusthed |
| 22.05.2026 | A.1 | Figur med aftalestruktur (4-hjørnemodel) opdateret |
| | A.4 | Vejledning fjernet |
| | A.5.4 + A.5.5 | Tilføjet krav om overholdelse af lovgivning og schemeregler, inkl. ret til at foretage revision og kontrol |
| | B.3.8 | Præcisering vedr. kontrolcifre |
| | B.14.1 | Rettet forældet krav om at bruge token BIN 357106 og 07 |
| | C.1.6 | Tilføjet krav om at indløser skal være PCI certificeret |
| | C.1.7 | Tilføjet krav om at indløser skal offentliggøre listepriser |
| | C.3.8 | Tilføjet pligt til at ajourføre registrering af betalingsmodtagere |
| | D.7 | Afsnit vedr. ”Dankort på mobilen” udgået |
| | E.1.1 | Ændret så det fremgår at udstedere får transaktioner fra Dankort-netværket |
| | E.6 | Tilføjet krav til behandling af reservationer for kort med saldokontrol |
| 14.10.2025 | A.1 | Figur med aftalestruktur ændret for at åbne for priser/gebyrer mod indløser |
| | A.3.6 | Tilføjet krav om indløserlicens |
| | A.4 | Mere klar opdeling af priser for de forskellige typer licensholdere |
| | B.1.2 | Tilføjet krav om co-badged kortprodukt med omgående reservation, dækningskontrol |
| | C.1.1 | Ændring så indløser formelt skal aflevere transaktioner til scheme |
| | C.1.2 + C.3.4 | Indløser skal registrere en konto i et pengeinstitut med Dankort licensaftale til at modtage udbetalinger |
| | C.3.8 | Indløser skal registrere alle betalingsmodtagere hos Dankort scheme |
| | C.4.3 | Krav til PSP-aftaler vedr. registrering af terminaltype |
| | D.1.2 | Præciseret at register over godkendelser skal deles med Dankort scheme |
| | D.2.13 | Nyt krav om aflevering af digitale kvitteringer |
| 16.05.2025 | B.3 | Tilføjet miljøkrav B.3.15-B.3.17 |
| | B.3 | Tilføjet krav B.3.14 vedr. kortnumre for firmakort |
| 31.01.2025 | B.3.10 | Krav ændret |
| | B.5.1 | Krav ændret |
| | B.8.4 | Fjernet gammel “med virkning fra” dato |
| | B.14.3 | Fjernet gammel “med virkning fra” dato |
| 31.05.2024 | Definitioner | Tilføjet definition af "Købsdato/tidspunkt" |
| | A.2 | Vejledning præciseret, udsendelsesdato ændret fra juli til august |

| | | |
|---|---|---|
| | B.1 | B.1 Overskrift ændret til "Generelle krav" |
| 31.01.2024 | A.5.1 | Krav ændret (tilføjet specifikation af proces ved tvister) |
| | B.11.1 og 2 | Krav ændret, tilføjet referencer til A.X.5 og A.X.6 |
| | B.11 | Afsnit ”Vejledning” fjernet |
| | B.11.3, 5 og 7 | Krav reduceret (erstattes af A.X.5 og A.X.6) |
| | C.1.5 | Krav tilføjet |
| | C.4.1 og 2 | Fjernet ”(med virkning fra 1/1/2024)” |
| 31.08.2023 | B.2.6 | Krav tilføjet |
| | B.3.2 | Krav udgået (inkl. bilag B.X.1) |
| | B.3.3 | Bilag B.X.2 og B.X.3 udgået |
| | B.3.10 – 13 | Krav tilføjet |
| | B.5 | Overskrift rettet fra ”Bestilling PIN-kode” til ”PIN-kode” |
| | B.6 | Krav udgået (inkl. bilag B.X.9) |
| | B.13.2 | Bilag B.X.7 og B.X.8 udgået, rettelse af ”Dankort og co-badged Dankort” til ”fysiske kort”, fjernet punkt 3 og 4 i liste (underskriftspanel, hologram m.v.) |
| | C.3.7 | Krav ændret |
| | D.2.11 | Tilføjet ”At betalingen blev udført med Dankort” |
| 28.04.2023 | B.14.3 | Krav tilføjet |
| 31.01.2023 | B.1 | Definition af co-badged præciseret, så det omfatter kort uanset form-faktor, samt ref. til IFRs definition. |
| | B.3.9 | Krav flyttet til nyt afsnit B.14 |
| | B.4.3 | Krav ændret (gælder kun fysiske kort) |
| | B.7.10 | Krav udgået |
| | B.7.11 og 12 | Nye krav vedr. kortaktivering tilføjet |
| | B.8.4 | Nyt krav vedr. understøttelse af Dankort Automatisk Kortopdatering |
| | B.14 | Nyt afsnit ”Virtualisering og udstedelse af token” |
| | C.1.3 | Nyt krav vedr. tidsfrister for indløser |
| | C.1.4 | Nyt krav vedr. attest fra indløser |
| | C.2 og C.3 | Ændrede overskrifter, ændret formulering af C.3.1 og 2 |
| | C.3.4 og C.4 | Nye krav om at indløser skal have aftale med PSPer fra 1/1/2024 |
| | D.2.1 | Krav til terminaler ændret fra PCI DSS/PTS til ”gældende standarder fra PCI og EMV”. |
| | E.1.2 | Krav tydeliggjort (ændret fra passiv formulering) |
| 18.08.2022 | B.11.4 | Henvisning til A.X.3 rettet til A.X.5 |
| 31.03.2022 | B.11.7 | Udsteders indsigelsesfrist for manglende dækning er udvidet fra 1 til 3 bankdage |
| | D.2.8 | Krav slettet |
| | D.2.12 | Krav vedr. PAR til digitale kvitteringer tilføjet |
| 31.01.2022 | Generelt indhold s. 3 | Ændringslog tilføjet (indholdsfortegnelse opdateret) |
| | | Henvisning til A.X.4 rettet til henvisning til A.X.5 |

| | | |
|---|---|---|
| | D.2.3 | Henvisning til A.X.3 Beløbsgrænser er rettet til D.X.1 Terminal parameters and features |
| | A.3.3 | Krav fjernet:<br><br>*Kontoførende pengeinstitutter skal rette henvendelse til indløser, når der sker overtræk på kontoen, som ikke er godkendt eller normalt for betalingsmodtager. For at mindske indløsers risiko skal henvendelsen fra pengeinstituttet ske indenfor rimelig tid efter der konstateres unormalt overtræk hos betalingsmodtager. Såfremt pengeinstituttet ikke retter henvendelse til indløser inden rimelig tid betragtes det som et godkendt overtræk, som indløser ikke er ansvarlig for.* |
| | E.5 | Tilføjelse af nyt krav: *Krav til udsteder i forbindelse med Dankort advarselsservice*<br><br>Indholdsfortegnelse opdateret |

## Definitioner

*Nedenstående er definitioner af de begreber, som går på tværs af schemereglerne. Begreber, der ikke går på tværs, er defineret i de kravsættende afsnit.*

| | |
|---|---|
| Betalingsmodtager | Den virksomhed, som indgår aftale med en indløser om at modtage betalinger med Dankort. |
| Brugeren | (se kortholder) |
| Dankort | Samlet betegnelse for betalingsinstrumentet (uanset formfaktor) udstedt af en Dankort udsteder og modtaget af en Dankort betalingsmodtager i henhold til nærværende regler. |
| EMV/EMVCo | Organisation, der specificerer standarder og godkender løsninger, fx for chipkort, terminaler og infrastruktur. |
| Indløser | Den virksomhed, som indgår aftale med betalingsmodtager om indløsning af betalinger med Dankort. |
| ISO | International Standardisation Organisation, som har til opgave at udarbejde internationale standards på en lang række områder. I forbindelse med Dankort danner ISO-standarderne grundlag for bl.a. anvendelsen af kryptografiske teknikker, kortdesign og chip- og magnetstribelayout. |
| Kontaktløs betaling | Kontaktløs betaling er en betaling med kortets chip uden at kortet sættes ind i kortterminalen. |
| Kontrolcifre | Et trecifret tal som er trykt på bagsiden af kortet. |
| Kortholder | Kortholder er den person, der efter aftale med udsteder om brug af Dankort har fået udstedt et Dankort. |
| Købsdato/tidspunkt | Den dato/det tidspunkt, hvor kortholder foretager et køb, og dermed autoriserer betalingsmodtager til et eller flere træk på kontoen knyttet til kortholders Dankort. |
| Licenshaver | Den virksomhed, der har indgået en Dankort licensaftale med Nets om fx udstedelse eller indløsning. |
| PAN | Primary Account Number er en betegnelse for kortnummeret. |
| PIN | Den personlige hemmelige 4-cifrede kode, der er knyttet til kortet. |
| Telefonordre | En betalingstransaktion, hvor brugeren bestiller en ydelse hos en betalingsmodtager via telefon, og hvor hverken brugeren eller kortet er til stede hos betalingsmodtager. |
| Udsteder | Udsteder er et pengeinstitut, som på grundlag af en licens fra Nets udsteder Dankort til kortholdere. |
| Wallet | En personlig softwarebaseret løsning, hvor kortholder har sit Dankort på sin mobiltelefon. |

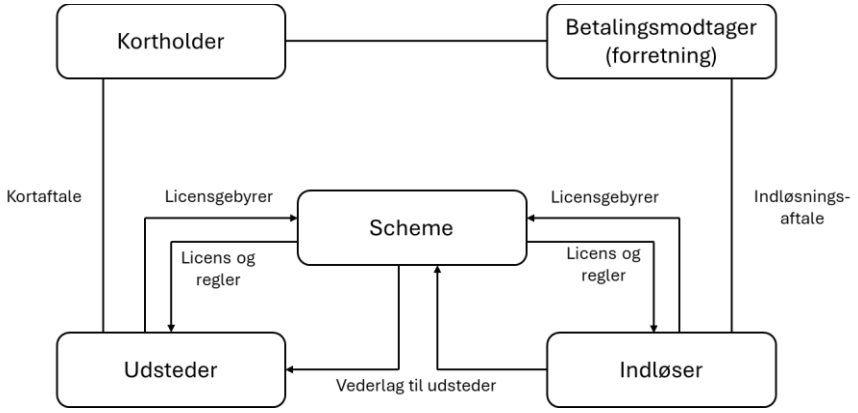
# A – GENERELLE VILKÅR

## A.1 – Aftalestruktur

**Vejledning**

*Dankorts aftalestruktur er baseret på 4-hjørnemodellen, der illustrerer forholdet mellem kortholder, betalingsmodtager (forretning), indløser og udsteder samt Dankort schemets placering i forhold til disse parter.*

*Dankort scheme stiller krav til udstedere og indløser. Det er således udsteder og indløsers ansvar at sikre at deres aftaleparter, herunder underleverandører, overholder kravene i Dankort schemeregler.*




## A.2 – Governance

**Vejledning**

*Justeringer til schemereglerne offentliggøres som udgangspunkt to gange årligt – henholdsvis i januar og i august. Efter behov kan Dankort scheme dog offentliggøre justeringer på andre tidspunkter af året.*

*Tilføjelse af nye Dankort schemeregler, der vurderes at medføre væsentlige omkostninger for parterne, sker så vidt muligt med en implementeringsfase således, at det er muligt for de berørte aftaleparter at gennemføre evt. nødvendige justeringer inden et krav træder i kraft.*

## A.3 – Licensaftale

**Krav**

A.3.1 Pengeinstitutter skal have licens for at kunne udstede Dankort til sine kunder, samt for at være kontoførende pengeinstitut for en betalingsmodtager. Licensen erhverves ved at indgå aftale med Dankort scheme.

A.3.2 Kontoførende pengeinstitutter skal stille en konto til rådighed for betalingsmodtagere, der har en aftale om indløsning af Dankort.

A.3.3 Udgået

A.3.4 Før det kontoførende pengeinstitut retter henvendelse til indløser skal tabet opgøres og pengeinstituttet vurdere, hvorvidt det er muligt at inddrive overtrækket hos betalingsmodtager. Indløser skal ikke dække renter og gebyrer tilskrevet kontoen som følge af overtrækket.

A.3.5 Kontoførende pengeinstitutter og indløser skal følge forretningsgang for information og tabsopgørelse i bilag A.X.1.

A.3.6 Indløsere af Dankort skal have en licens for at kunne indgå aftale med betalingsmodtagere. Licensen erhverves ved at indgå aftale med Dankort scheme.

## A.4 – Dankort prismodel og gebyrer

**Krav**

A.4.1 Kortudstedende licenshavere skal årligt betale et licensgebyr til Dankort scheme, som fremgår af bilag A.X.2 "Priser og vederlagssatser for udstedere af Dankort". Af bilaget fremgår desuden øvrige gebyrer, som kortudstedende licenshavere skal betale.

A.4.2 Kortindløsende licenshavere skal årligt betale et licensgebyr til Dankort scheme, som fremgår af bilag A.X.7 "Priser og vederlagssatser for indløsere af Dankort". Af bilaget fremgår desuden øvrige gebyrer og sikkerhedsstillelse, som kortindløsende licenshavere skal betale.

A.4.3 Licenshavere, som alene er kontoførende jf. A.3.2, skal ikke betale licens eller gebyrer.

## A.5 – Compliance og tvister

***Krav***

A.5.1 På anmodning fra Dankort scheme skal licenshaver udarbejde dokumentation for overholdelse af Dankort scheme regler, samt ledelseserklæring, hvis scheme tillige anmoder om dette. Dokumentation og erklæring kan omfatte alle regler eller en delmængde.

Ledelseserklæring skal attesteres af licenshavers ledelse og eksterne revisor. Det skal af attestationen fremgå, om revisor er enig i erklæringen, eller om revisor har særlige forbehold eller bemærkninger til erklæringen. Eventuelle forbehold eller bemærkninger skal klart fremgå af attestationen.

Licenshaver skal fremsende dokumentation og erklæringen til Dankort scheme indenfor fristen angivet i anmodningen.

Såfremt Dankort scheme konstaterer tilfælde af manglende efterlevelse kan Dankort scheme udstede påbud om berigtigelse af det eller de pågældende forhold indenfor en frist fastsat af Dankort scheme.

Licenshaver skal berigtige forhold vedrørende manglende overholdelse af schemereglerne indenfor den af Dankort scheme fastsatte tidsfrist. Såfremt det eller de pågældende forhold ikke berigtiges indenfor den fastsatte frist skal licenshaver betale et evt. ikke-efterlevelsesgebyr fastsat af Dankort scheme for manglende berigtigelse. Samtidig kan Dankort scheme give skærpet påbud om hastig berigtigelse af forholdet.

A.5.2 Ved manglende efterlevelse af et skærpet påbud om hastig berigtigelse kan licenshaver fratages licensen af Dankort scheme, og må således ikke udstede Dankort eller behandle Dankort transaktioner. Dankort scheme kan også delvist fratage licensen, således at licenshaver indenfor et område fratages retten til at operere.

A.5.3 Enhver tvist mellem Dankort scheme og en licenshaver vedrørende overholdelse af Dankort schemereglerne skal afgøres ved voldgift ved Voldgiftsinstituttet efter de af Voldgiftsinstituttet vedtagne regler herom.

A.5.4 Licenshaver skal overholde alle gældende love, regler, bekendtgørelser, retningslinjer og regulatoriske krav, der er relevante for licenshavers virksomhed og ydelser i henhold til Dankort Scheme reglerne. Dette omfatter, men er ikke begrænset til, regler om hvidvaskning af penge og finansiering af terrorisme (AML), kundekendskabsprocedurer (KYC), sanktionslovgivning, databeskyttelse samt øvrige finansielle og regulatoriske krav fastsat af kompetente myndigheder.

A.5.5 Licenshaver skal have interne politikker, procedurer, systemer og kontroller til sikring af overholdelsen af Dankorts scheme krav. Dankort scheme, samt dennes revisorer, interne eller eksterne rådgivere og relevante myndigheder har med rimeligt varsel ret til at foretage kontrol og revision af licenshavers relevante processer, systemer, dokumentation og kontroller i det omfang, det er nødvendigt for at verificere licenshavers overholdelse af denne bestemmelse.

# B – KORTUDSTEDELSE

## B.1 – Generelle krav

**Definition** Et co-badged betalingskort er et kort (uanset formfaktor), der integrerer to eller flere betalingsbrands og derved har adgang til adskillelige netværk for gennemførelse af transaktioner. Se også EU's interchange fee regulation (IFR) artikel 2.

**Krav**

B.1.1 For brugerregler vedrørende co-badged Dankort skal udsteder sikre, at beskrivelser og valgmuligheder for Dankort-delen fremgår mindst lige så tydeligt, som beskrivelser og valgmuligheder for den del, der vedrører det andet Scheme.

B.1.2 *[med virkning fra 1/4 2027]*

Udstedere skal tilbyde et debet-kortprodukt med følgende funktionalitet:

- Kortholder kan omgående se reservationer og bogføringer på kontoen
- Udsteder kan afvise autorisationer, hvor der ikke er dækning for på kontoen
- Co-badged med et internationalt kortselskab

## B.2 – Behandling af kort hos udsteder

**Krav**

B.2.1 Udsteder skal have fastsat procedurer, der sikrer at et udstedt Dankort tilgår kortholder personligt eller sendes direkte fra kortproducent til kortholders adresse.

B.2.2 Udsteder skal vedligeholde en beholdningsoversigt i form af en log over Dankort modtaget af udsteder fra kortproducent, som ikke er udleveret til kortholder. Oversigten skal ajourføres, hver gang Dankort indlægges i eller udtages fra beholdningen. Der skal findes interne forretningsgange, der foreskriver periodisk afstemning af beholdningen mod beholdningsoversigten.

| | |
|---|---|
| B.2.3 | Kortholder skal anmodes om via netbank, telefon, selvbetjeningsautomat eller ved personlig fremmøde hos udsteder at aktivere sit Dankort inden for en af udsteder valgt aktiveringstidsfrist dog maksimum 60 kalenderdage. |
| B.2.4 | Såfremt kortet ikke er aktiveret senest 60 kalenderdage efter forsendelse fra udsteder, skal Dankortet spærres og et nyt kort skal bestilles af kortholder. |
| B.2.5 | Udsteder skal sikre, at kort der returneres håndteres af en organisatorisk funktion, der er adskilt fra funktioner, der deltager i den administrative behandling af PIN-breve. |
| B.2.6 | Udsteder skal benytte virksomheder, som har en gældende PCI CPP ("Card Production and Provisioning") godkendelse. |

## B.3 – Tekniske specifikationer og design

**Krav**

| | |
|---|---|
| B.3.1 | Alle nyudstedte og genudstedte kort med kontakt og/eller kontaktløs chip funktionalitet skal være i overensstemmelse med EMV. |
| B.3.2 | [udgået august 2023] |
| B.3.3 | Alle Dankort skal følge specifikationer angivet i bilag B.X.6. |
| B.3.4 | Specifikationerne skal anvendes ved såvel nyudstedelse som genudstedelse. |
| B.3.5 | Dankort må kun produceres og personaliseres af producenter godkendt af Dankort scheme. Fortegnelse over godkendte producenter fremgår af dankort.dk. |
| B.3.6 | Løbetid på Dankort (inkl. co-badged Dankort) skal være højst 4 år regnet fra udstedelsesmåneden + 3 måneder. |
| B.3.7 | Udsteder skal hos Dankort scheme indhente godkendelse af designet af det areal, der er til udsteders disposition, forinden et nyt Dankort eller co-badged Dankort design tages i brug. |
| B.3.8 | Kortnummeret for et fysisk Dankort skal være 16 cifre (se B.14.1 for regler vedr. virtualiserede kortnumre/tokens). Sidste ciffer skal være et kontrolciffer og beregnes efter ISO standard 7812 Annex C (Luhn algoritmen). De første 4 cifre for Dankort, der er co-badged med Visa, skal være 4571, og for øvrige Dankort skal de være 5019. De følgende 4 cifre skal være udsteders registreringsnummer. |
| B.3.9 | [flyttet til B.14 januar 2023] |
| B.3.10 | Dankort logo skal gengives på kortet som det forefindes på dankort.dk. Logoet skal være synligt på kortets forside. Såfremt Dankort vises sammen med andre kortlogoer skal logoerne have samme synlighed, og hvis det andet kortlogo er gengivet i farve skal Dankorts logo også. På fysiske kort skal logoet være mindst 9 x 15 mm og med en margin på mindst 2 mm til øvrige elementer på kortet. |
| B.3.11 | Kortet må ikke have afbildning, som kan resultere i afvisning af kortet, eller som kan medføre andre problemer i betalingssituationen. Billedmateriale må ikke indeholde elementer, som kan forstyrre eller forveksles med nogen af de til kortet påkrævede sikkerhedselementer. |
| B.3.12 | Såfremt udsteder tilbyder individuelle kortdesigns administrerer udsteder reglerne for udformning. Udsteder er ansvarlig for enhver tvist, der måtte opstå som følge af et afbildet motiv. Udsteder er forpligtet til at holde Dankort scheme skadesløs for ethvert krav eller tab, som hidrører fra udstedelsen af et kort med individuelt design. |
| B.3.13 | Udsteder skal tilbagekalde og udskifte Dankort med individuelle designs, som måtte være udstedt uden at overholde reglerne for kortdesign. |

B.3.14 Til kort, som udstedes til erhvervsbrug, skal udsteder sikre at de første 10 cifre er indenfor intervaller, som udsteder eksklusivt anvender til denne type kort. Udsteder skal oplyse Dankort scheme om disse intervaller via mail til dankortscheme@nets.eu senest 3 måneder før første udstedelse indenfor intervallet. Scheme formidler disse til indløser, som stiller dem til rådighed for forretninger, der ønsker mulighed for at identificere kort til erhvervsbrug.

**Vejledning** *Med henvisning til European Sustainability Reporting Standards (ESRS) og dens standarder for bæredygtighedsrapportering, der gælder for alle de virksomheder, der er omfattet af EU-direktivet Corporate Sustainability Reporting Directive (CSRD), stiller scheme nedenstående krav til udstedere af Dankort. Nedenstående krav skal gøre udstedere og scheme i stand til at lave den påkrævede rapportering af bl.a. ESRS E1 og E2.*

B.3.15 *[gældende fra 1. april 2028]*

På anmodning fra scheme skal udsteder levere data om $CO_2E(q)$-emissioner (jf. Eurostats definitioner, se https://ec.europa.eu) for kortproduktion og materiale, herunder materialer til kort og chip/modul, produktionsprocesser og transport af råmaterialer (se nedenstående tabel).

| Data | Eksempel | Datatype |
|---|---|---|
| Materiale type | rPVC | Kvalitativ |
| Materiale til kort | 20 | Kvantitativ, co2e/g |
| Materiale til modul | 20 | Kvantitativ, co2e/g |
| Produktion | 5 | Kvantitativ, co2e/g |
| Transport af råmaterialer | 10 | Kvantitativ, co2e/g |
| Total | 0+20+20+5+10 | Sum af kvantitativ, co2e/g |

B.3.16 *[gældende fra 1. april 2028]*

Udsteder skal producere kort i materialer, der minimerer plastforbrug, såsom RPVC, PLA, rPET, certificeret træ eller ethvert andet nyt og/eller alternativt materiale, ligeledes minimerer plastforbrug.

B.3.17 *[gældende fra 1. april 2028]*

Den samlede $CO_2E(q)$-udledning pr. nyudstedt kort må ikke overstige 100 gram.

## B.4 – Bestilling af kort

**Krav**

B.4.1 I forbindelse med bestilling af kort skal pengeinstituttet give kunden adgang til information, der beskriver betalingsmidlets anvendelsesmuligheder og de sikkerhedsforanstaltninger, der er knyttet til betalingsmidlet.

B.4.2 Der skal være oprettet en konto i pengeinstituttet før kortbestilling initieres.

B.4.3 Der skal til alle fysiske Dankort udstedes en PIN-kode.

B.4.4 Medkontohavere eller fuldmagtshavere, der har adgang til at hæve på kontoen, skal tildeles særskilt betalingsinstrument, fx Dankort og PIN-kode.

B.4.5 Kortfremstilling skal baseres på de oplysninger (kortholderens navn, adresse m.v.), som udsteder har registreret til det pågældende kontoforhold.

## B.5 – PIN-kode

**Krav**

| | |
|---|---|
| B.5.1 | PIN-koden skal altid holdes hemmelig og må kun oplyses til kortholder. |
| B.5.2 | PIN-brev og brev med Dankort må ikke sendes samme dag til kortholderen. Kravet om forskellig fremsendelsesdag gælder ikke, hvis PIN-koden fremsendes som SMS eller hvis den rekvireres elektronisk i kortholders netbank. |
| B.5.3 | PIN-brevet skal sendes til kortholders postadresse. Kortholder må ikke være registreret med et pengeinstitut som c/o-adresse. |
| B.5.4 | Elektronisk PIN-kode via SMS skal sendes direkte til det mobiltelefonnummer kortholder har ladet registrere til formålet. |
| B.5.5 | Elektronisk PIN-kode via SMS må kun sendes til kortholder, når kortholder anmoder om fremsendelse af PIN-koden. |
| B.5.6 | Hvis PIN-kode fremsendes via SMS skal udsteder meddele særskilt identifikationskode til brugeren. |
| B.5.7 | Der må max. ske tre forkerte forsøg på at hente koden via SMS. Herefter blokeres udsendelsen af elektronisk PIN og udsteder informeres. Genudstedelse må først ske efter fornyet kontakt til kunden. |
| B.5.8 | Udsteder skal oplyse kortholder om sikker håndtering og opbevaring af PIN-koden – herunder sletning af PIN koden på mobiltelefonen og forsigtighed ved rekvirering af PIN-kode i det offentlige rum. |
| B.5.9 | Postforsendelse skal ske direkte fra den funktion, der udskriver PIN-brevene. Forsendelse skal ske som almindelig post. |
| B.5.10 | Kan koden ikke huskes af kortholder kan der udsendes et nyt PIN-brev/rekvireres en ny elektronisk PIN med samme kode i overensstemmelse med reglerne for udstedelse af PIN-kode til Dankort. |
| B.5.11 | Hvis kortholder ønsker at benytte en PIN-kode fra et eksisterende kort, skal følgende krav være opfyldt:<br>1. Der må ikke udsendes ny/ændret PIN-kode til allerede udstedte Dankort.<br>2. Bestilling og udsendelse af PIN-brev/Elektronisk PIN skal følge Dankort-reglerne uanset til hvilket kort PIN-brevet/elektronisk PIN udsendes.<br>3. PIN-koden skal stamme fra kort udstedt af Dankort-udstederen.<br>4. Der må ikke bestilles og udsendes en PIN-kode, hvor bare ét af kortene, der benytter samme kode er spærret som følge af:<br>• Mistanke om eller konstatering af 3.-mandsmisbrug med kort, hvis misbrug har fundet sted ved anvendelse af PIN-kode<br>• Stjålet/bortkommet kort og mistanke om kompromittering af PIN-kode |

## B.6 – [udgået]

## B.7 – Forsendelse fra kortleverandør og aktivering

**Vejledning**

*Kravene i dette afsnit er fastlagt med henblik på:*
*• At muliggøre forsendelse af kort direkte til kortholder*
*• At kortholderen oplever det som enkelt og sikkert at få et nyt kort*

**Krav**

B.7.1 Ved fremsendelse af kort til kortholder skal der anvendes en neutral standardkuvert forsynet med returadresse fastsat af udsteder.

B.7.2 Kortholderens bekræftelse af modtagelse af kort skal ske
- a) ved anvendelse af en bekræftelsesløsning baseret på aktiveringsnummer
- b) ved personligt fremmøde i pengeinstitut med kontrol af kortholders identitet
- c) ved anden sikker identifikation af kunden i fx netbank eller selvbetjeningsautomater

B.7.3 Aktiveringsnummeret skal tildeles tilfældigt og skal udgøre 5 cifre. Som alternativ kan udsteder vælge at lade nummeret bestå af minimum de sidste 4 cifre i kortholders cpr.nr.

B.7.4 Tilfældigt tildelte aktiveringsnumre skal udskrives direkte fra udsteders system på et dokument, der udleveres personligt eller fremsendes separat til kunden.

B.7.5 Aktiveringsnummeret må ikke registreres, kopieres eller opbevares decentralt hos udsteder.

B.7.6 Udsteder må kun opbevare aktiveringsnummeret med henblik på senere bekræftelse.

B.7.7 Udsteder skal sikre, at kortholder er i besiddelse af en aktiveringsvejledning, senest når kortet modtages.

B.7.8 [udgået – januar 2021]

B.7.9 Udsteder skal sende påmindelse til kunder, der ikke har aktiveret forsendte kort inden for den af udsteder valgte aktiveringsfrist således, at kortholder har tid til at aktivere kortet inden udløbet af den valgte aktiveringsfrist.

B.7.10 [udgået – januar 2023]

B.7.11 Udsteder må kun udsende co-badgede kort med kontaktløst deaktiveret, hvis aktiveringen på en terminal, der ikke modtager Dankort, også aktiverer Dankort kontaktløst. Hvis kortet i stedet udsendes med kontaktløst aktiveret skal det sikres, at kontaktløse transaktioner afvises indtil der er lavet en godkendt, online PIN-baseret betaling med kontakt.

B.7.12 Hvis co-badgede kort udsendes med andre applikationer aktiveret, så skal Dankort applikationen også være aktiveret.

## B.8 – Fornyelse og udskiftning af kort

**Vejledning**

*Behovet for fornyelse eller udskiftning af kort opstår:*

1. *når kortet udløber,*
2. *hvis kortet, herunder kortets magnetstribe, chip eller kontaktløse antenne er slettet eller ødelagt,*
3. *hvis kortet er bortkommet eller stjålet,*
4. *hvis kortholder har mistanke om, at uvedkommende kunne have fået kendskab til PIN-kode,*
5. *hvis udsteder af anden årsag vælger at ombytte kortet.*

*Hvorvidt PIN-koden til det tidligere udstedte kort vil kunne anvendes til det genudstedte kort vurderes af udsteder.*

**Krav**

B.8.1 [udgået – se ændringslog for april 2021]

B.8.2 Hvis det tidligere kort er bortkommet eller stjålet skal udsteder tildele ny PIN-kode.

B.8.3 Der skal bestilles nyt kort og ny PIN-kode, hvis kortholder giver besked til udsteder om, at andre kan have fået kendskab til koden.

B.8.4 Ved fornyelse af kort skal udsteder indberette relevante kortoplysninger til servicen Dankort Automatisk Kortopdatering, så forretninger/løsninger, der anvender gemt kort, kan blive opdateret. Denne forpligtelse gælder ikke, hvis kortholder har frameldt sig.

## B.9– Spærring og sletning af kort

**Vejledning**

*Et væsentligt led i sikkerheden er, at der i betalings-/udbetalingsøjeblikket foretages kontrol af, om det anvendte Dankort er spærret. Spærring kan ske af forskellige årsager – alle med det formål at hindre eller minimere misbrug.*

*Tidspunktet for anmeldelse og registrering af spærringer er af afgørende betydning for placering af ansvar for eventuelle tab i forbindelse med misbrug. Det er udsteder, der træffer den endelige afgørelse om, hvorvidt et Dankort fortsat skal være spærret eller om en spærring skal ophæves.*

**Krav**

B.9.1 [udgået – se ændringslog for april 2021]

B.9.2 Udsteder vurderer hvorvidt modtagne informationer om PIN-blokering eller forkerte PIN-forsøg skal medføre spærring.

B.9.3 Udsteder skal tilbyde kortholder 24-timers spærreservice alle dage på året.

B.9.4 [udgået – se ændringslog for april 2021]

B.9.5 [udgået – se ændringslog for april 2021]

B.9.6 Er der i forbindelse med spærring af kort tale om:

- situationer som nævnt under tilbagelevering eller
- situationer, hvor kortholder selv har spærret kortet

skal information om spærring stilles til rådighed for kortholder i form af kvittering for spærringen.

Der skal oplyses om dato og tidspunkt for spærring samt årsagen hertil.

B.9.7 Straks efter modtagelse af en anmeldelse, eller hvis der konstateres en brugsfrekvens, der giver anledning til mistanke om misbrug, skal udsteder foretage spærring. Er kortnummer ikke oplyst, skal kortets nummer hurtigst muligt fremfindes på grundlag af de øvrige modtagne oplysninger.

B.9.8 Udsteder skal straks ophæve spærring:

1. For kort, som fejlagtigt er spærrede
2. For spærrede kort, der er udløbet (disse kort skal slettes)
3. Når årsagen til spærringen er bortfaldet (fx spærring på grund af nu inddækket overtræk).

Kort skal altid stå spærret til udløb når:

- Kortet er spærret som følge af tredjemandsmisbrug
- Kortet er spærret på grund af mistanke om tredjemandsmisbrug
- Der er risiko for, at kortet kan være kopieret (gælder i alle tilfælde, hvor kortet har være tredjemand i hænde).

B.9.9 Konstaterer kortholder eller udsteder, at et kort fejlagtigt er spærret, skal udsteder fremsende underretning (fx brev eller mail) til kortholder, indeholdende oplysningerne i bilag B.X.4.

B.9.10 Kort der indleveres i forbindelse med ophør af konto skal destrueres og slettes. Dette gælder dog ikke, såfremt kortet er spærret, i disse tilfælde skal reglerne i forbindelse med ophævelse af spærring følges.

## B.10 – Inddragne/indleverede kort

**Krav**

B.10.1 Udsteder skal sikre procedure for:

- inddragelse af kort, der er spærret
- inddragelse af kort, hvor der er begrundet mistanke om forsøg på misbrug
- behandling af inddragne/indleverede kort

B.10.2 Proceduren for inddragelse skal som minimum indeholde følgende:

- Udsteder skal spærre inddragne/indleverede kort. Dette gælder dog ikke kort, som er inddraget i en pengeautomat som følge af en teknisk fejl.
- Opbevaring af inddragne eller indleverede kort skal ske i overensstemmelse med afsnit B.2. Dette gælder dog ikke kort, der udleveres til kortholder, makuleres eller sendes til Nets/udsteder samme dag de inddrages/indleveres/udtages af pengeautomat.
- Ved inddragelse/modtagelse/udtagelse af pengeautomat af indleverede kort eller udløb af en evt. opbevaringsperiode, skal kortet destrueres således at kortet ikke kan anvendes.
- Regler om fremsendelse, jf. B.7
- Regler om udtagning af inddragne kort fra ATM, jf. B.10.3

B.10.3 [udgået – se ændringslog for april 2021]

B.10.4 Kort, der er tilbageholdt i en pengeautomat på grund af en teknisk fejl, kan udleveres til kortholder i udbetalende pengeinstitut under iagttagelse af følgende forholdsregler:

- Årsagen til kortets tilbageholdelse skal undersøges på journalrullen.
- Kortholders identitet skal kontrolleres.

B.10.5 Dankort, der indleveres i forbindelse med ophør af en konto eller i øvrigt på udsteders eller kundens foranledning, skal destrueres og slettes i Dankort-registret.

B.10.6 Udsteder har i følgende tilfælde mulighed for at genudlevere kortet:

- Kortet er fejlagtigt spærret
- Kortet er spærret på grund af overtræk
- Kortet er tilbageholdt i en pengeautomat på grund af teknisk fejl.

Kortets magnetstribe og chip skal før udlevering valideres ved indlæsning i en terminal. Udsteder kontrollerer tillige, at kortet er aktivt.

## B.11 – Indsigelser og tilbageførsler

**Krav**

B.11.1 I tilfælde, hvor der rejses tvivl om hvorvidt en Dankort transaktion skal honoreres eller hvis en transaktion afvises af kortholder, skal udsteder følge reglerne for indsigelse og tilbageførsel i bilag A.X.5 og arbejdsgangene beskrevet i bilag A.X.6.

B.11.2 Udsteders forpligtelser:

- Udsteder skal undersøge og behandle alle indsigelser fra kortholder – herunder vurdere hvorvidt kortholder skal holdes ansvarlig.
- Ved ej vedkendelsessager skal udsteder bede kortholder underskrive tro & love erklæring hvor alle ej vedkendte transaktioner inkluderes.
- Beløb, der ønskes tilbageført, skal fratrækkes eventuel betalingsgaranti og/eller det beløb kortholder kan gøres ansvarlig for.

Kortholder skal orienteres om alle foretagne returneringer, samt i hvilket omfang denne gøres ansvarlig. Udsteder skal kunne dokumentere orientering af kortholder.

B.11.3 [krav flyttet til bilag A.X.6]

B.11.4 Udsteder garanterer overfor indløser at kortbetalinger vil blive dækket med de beløb, der fremgår under "Udsteders betalingsgaranti" i bilag A.X.5.

B.11.5 Fordeles en betaling på to eller flere transaktioner gælder den fastsatte betalingsgaranti for den samlede betaling.

B.11.6 Udsteders rettigheder ved ikke aktive og spærrede kort: Hele transaktionsbeløbet kan returneres hvis kortet ikke var registreret som aktivt på købstidspunktet.

B.11.7 [krav flyttet til bilag A.X.5]

## B.12 – Indberetning af Dankort tredjemandsmisbrug

**Vejledning** *Formålet med indberetning af tredjemandsmisbrug er at skabe et overblik, der giver baggrund for at iværksætte præventive tiltag, hvis udviklingen i misbrug skulle give anledning hertil. Der indberettes ikke kortholders eget misbrug i forbindelse med overtræk m.v.*

**Krav**

| | |
|---|---|
| B.12.1 | Udsteder skal indberette alle transaktioner, hvor der er tale om tredjemandsmisbrug til Dankort scheme – uanset baggrunden for misbruget (tabt, stjålet eller andre omstændigheder). |
| B.12.2 | Indberetning skal ske i forbindelse med sagens behandling Indberetning af misbrug, inklusiv misbrug i pengeautomater skal gennemføres via system stillet til rådighed af Dankort scheme. Pengeinstitut skal indberette al tredjemandsmisbrug, også hvor der ikke kan angives indsigelse. |
| B.12.3 | Transaktioner, hvor kortholder helt eller delvis hæfter for misbruget, skal indberettes med det fulde transaktionsbeløb. |
| B.12.4 | Transaktioner for hvilke, der har kunnet gøres regres over for indløser (betalingsmodtager), skal indberettes. |

## B.13 – Leverandører af produkter (3rd party vendors and suppliers)

**Krav**

| | |
|---|---|
| B.13.1 | Udstedere, der anvender underleverandører, er ansvarlige for at sikre at underleverandører lever op til Dankort scheme krav – på samme måde som hvis licenshaver selv udfører den pågældende opgave. |
| B.13.2 | For følgende produkter må udstedere kun anvende leverandører, der er godkendt af Dankort scheme:<br>• Produktion af fysiske kort<br>• Personalisering og levering af fysiske kort<br><br>Godkendte leverandører fremgår af dankort.dk |
| B.13.3 | Når udstedere anvender leverandører til opgaver, hvor Dankort scheme kræver en godkendt leverandør, skal udsteder have indgået en skriftlig aftale med leverandøren om overholdelse af Dankort schemeregler på det pågældende område. |

## B.14 – Virtualisering og udstedelse af token

| | |
|---|---|
| **Definition** | Ved ”virtualisering” forstås udsteders oprettelse af en digital udgave af et Dankort. Ved ”forespørger” forstås den, der anmoder om virtualisering, som fx kan være en walletudbyder. Ved ”token” forstås den data, der udgør den digitale repræsentation af et fysisk kort, når det virtualiseres. En token er kendetegnet ved, at den teknisk er begrænset til alene at kunne anvendes af forespørger, og at den ikke indeholder Dankortets kortnummer (PAN). |

**Krav**

| | |
|---|---|
| B.14.1 | Hvis udsteder tilbyder virtualisering af Dankort ved hjælp af tokenisering skal de udstedte tokens være med den længde og indenfor de intervaller, der fremgår af Dankorts BIN liste (gældende version kan findes på Nets TRG Portal). |
| B.14.2 | Når det fysiske kort udskiftes på grund af udløb skal udsteder sikre, at udstedte token fortsat fungerer, så kortholder ikke behøver at virtualisere sit kort igen. |

B.14.3 Hvis udsteder virtualiserer ikke-Dankort delen af et co-badged kort, fx til en wallet, skal udsteder ligeledes virtualisere Dankort-delen, så det virtualiserede kort også er co-badged (dvs. hvor kortet er integreret af to eller flere betalingsbrands, jf. definitionen i "B.1 – Brugerregler for Dankort og øvrig information til kortholder"). Dette er dog ikke et krav, hvis forespørger generelt ikke understøtter digitale co-badgede kort (uanset om det Dankort eller andre kort).

Virtualiseringen skal ske senest samtidigt med at udsteder virtualiserer ikke-Dankort delen af det co-badgede kort.

# C– INDLØSNING

## C.1 – Generelle krav til indløser

**Definition**

*Indløser kan indgå aftaler med betalingsmodtagere, der ønsker at kunne modtage Dankort som betalingsmiddel i deres forretning. Betalingsmodtager afleverer betalingstransaktioner foretaget med Dankort til indløser, som efterfølgende sikrer at omsætning udbetales til betalingsmodtager. For Dankort anvendes PBS clearing/sumclearing til afregning af Dankort betalingsmodtagere eller indløser, samt for opkrævning af kortforbrug hos Dankort udstedere.*

**Krav**

C.1.1 Indløser er ansvarlig for at aflevere transaktioner til Dankort scheme for debitering/kreditering af kortholder.

C.1.2 Indløser er ansvarlig for at registrere den konto, en betalingsmodtagers omsætning skal udbetales til, hos Dankort scheme. Kontoen skal enten tilhøre indløser eller betalingsmodtager. Kontoen skal være i et pengeinstitut med Dankort licensaftale, og pengeinstituttet skal deltage i sumclearingen, da Dankort omsætning udbetales via sumclearingen.

C.1.3 Indløser skal behandle alle clearingtransaktioner, som modtages fra betalingsmodtager inden kl. 23.00, således at de afregnes til denne førstkommende bankdag. Indløser skal udføre afregningen ved senest kl. 00:30 (00:20 fra 2025) på bankdage at sende clearingleverancer til sumclearingen.

C.1.4 Senest den 31/12 hvert år skal indløser attestere overfor Dankort scheme at indløsers forretningsgange og løsninger er i overensstemmelse med kravene til indløser i nærværende schemeregler.

C.1.5 I forbindelse med indsigelser og krav om tilbageførsler fra udsteder skal indløser følge reglerne i bilag A.X.5 og arbejdsgangene beskrevet i bilag A.X.6.

C.1.6 Indløser skal være PCI certificeret og skal senest den 31/12 hvert år sende gældende PCI certifikat til Dankort scheme.

C.1.7 Indløser skal offentliggøre listepriser for sin indløsning af Dankort-betalinger, samt evt. gebyrer knyttet hertil. Priserne skal dække alle typer Dankort-betalinger. Offentliggørelsen skal ske på indløsers hjemmeside. Ved opdatering af priserne skal indløser give besked til Dankort scheme.

C.1.8 Indløser skal vedligeholde en plan for fortsat leverance af virksomhedens ydelser (en Business Continuity Plan), hvis der indtræder en operationel hændelse. Indløser skal teste planen en gang årligt.

C.1.9 Indløser skal vedligeholde en plan for hurtig genoprettelse af IT-driften (en Disaster Recovery Plan), hvis der indtræder et driftsproblem. Indløser skal teste planen en gang årligt.

C.1.10 Indløser skal månedligt udarbejde interne opgørelser af oppetider på indløserens kritiske systemer.

C.1.11 Indløser skal internt klassificere driftshændelser ud fra en konsekvensvurdering. Efter håndtering af en hændelse med høj konsekvensvurdering skal indløser internt udføre en hovedårsagsanalyse.

## C.2 – Forpligtelser overfor kontoførende pengeinstitut

**Krav**

C.2.1 Indløser skal indestå for tab hos pengeinstitut som følge af manglende dækning for indløsers træk på betalingsmodtagers konto. Indløser må alene foretage træk på betalingsmodtagers konto som følge af:

- krediteringer
- betaling for betalingskortaftale, herunder gebyrer
- chargebacks

Anvendes betalingsmodtagers konto til anden brug skal indløser alene dække den del af overtrækket som stammer fra træk fra indløser. Når indløser har vurderet kravet og dokumentationen skal indløser straks betale det pågældende beløb.

**Vejledning** Såfremt indløser og kontoførende pengeinstitut ikke kan blive enige om fortolkning af reglerne træffes afgørelse af Dankort scheme.

## C.3 – Tilslutning af betalingsmodtager

**Krav**

C.3.1 Indløser skal indgå en betalingskortaftale med betalingsmodtager inden denne kan modtage Dankort betalinger.

C.3.2 Indløser skal sikre at betalingskortaftalen indeholder krav til betalingsmodtager om, at denne til enhver tid overholder gældende regler og vilkår for Dankort betalingskortaftaler, som publiceret på dankort.dk.

C.3.3 Indløser skal indløse alle betalinger med Dankort fra betalingsmodtagere, der har indgået en indløsningsaftale.

C.3.4 Indløser må kun indgå Dankort betalingskortaftale med betalingsmodtagere, der opfylder følgende krav:

- Betalinger med Dankort skal overføres til en konto udpeget af betalingsmodtager.
- Betalingstransaktion og afregningsvaluta skal være DKK. Indløser vil via national clearing afregnes i DKK.
- Anvender en PSP, jf. ”C.4 – Tilslutning af PSP (Payment Service Provider)”, som indløser har indgået aftale om modtagelse Dankort-transaktioner med.

C.3.5 Indløser skal opbevare indløsningsaftale med senere ændringer i minimum 1 år efter aftalens ophør.

C.3.6 Indløser skal foranledige overvågning af den enkelte betalingsmodtager med henblik på at begrænse misbrug. Overvågningen skal som minimum inkludere debet- og kredit transaktioner.

C.3.7 Hvis indløser mistænker at en kreditering, eller en serie af krediteringer, er misbrug, og det samlede beløb er over kr. 10.000, skal indløser anmode udsteder (evt. via udsteders serviceleverandør) om spærring af kortet.

C.3.8 Indløser skal registrere alle betalingsmodtagere, som den har indgået Dankort betalingskortaftale med, efter anvisninger fra Dankort scheme. Indløser skal opdatere denne registrering, så den til enhver tid er korrekt. Aftaler, som er ophørt eller opsagt, skal afregistreres som anvist af Dankort scheme.

## C.4 – Tilslutning af PSP (Payment Service Provider)

**Definition** *En Payment Service Provider (PSP) er en underleverandør til betalingsmodtager, der på vegne af denne formidler betalingstransaktioner til indløser.*

**Krav**

C.4.1 Indløser må kun modtage betalingstransaktioner fra PSPer, som indløser har indgået aftale om modtagelse af Dankort betalingstransaktioner med.

C.4.2 Indløser skal sikre at aftalen med PSPen indeholder krav om, at denne til enhver tid overholder gældende regler og vilkår for Dankort betalingskortaftaler, som publiceret på dankort.dk. Aftalen skal give indløser mulighed for at opkræve løbende bod af PSPen ved manglende overholdelse.

C.4.3 Indløser skal sikre at aftalen med PSPen indeholder krav om, at denne oplyser indløser om anvendt type af betalingsterminal (integreret eller stand-alone) for betalingsmodtagere i fysisk handel ved opsætning eller udskiftning af betalingsterminal.

# D – KORTMODTAGELSE

## D.1 – Generelle krav

**Definition** *Kortmodtagelse omfatter krav til alle typer løsninger (herefter "Løsning(er)"), hvor kortholder kan anvende sit Dankort. Dette inkluderer fx terminaler og hæveautomater.*

*Kortmodtagelse omfatter ikke processing, dvs. den del af en transaktion hvor den er sendt til behandling hos indløser og udsteder.*

**Krav**

D.1.1 Indløser må kun acceptere Dankort transaktioner fra Løsninger, der er godkendt af Dankort scheme, eller hvor der foreligger dispensation fra Dankort scheme.

D.1.2 Indløser må godkende Løsninger på vegne af Dankort scheme, hvis typen af Løsning fremgår af dette afsnit (D), og Løsningen lever op til de specificerede krav. Indløser skal have en skriftlig forretningsgang for sådanne godkendelse og skal vedligeholde et register over godkendelser, som deles med Dankort scheme.

D.1.3 Hvis en Løsning godkendt af indløser ikke længere opfylder kravene i dette afsnit (D), og der ikke foreligger dispensation fra Dankort scheme, skal indløser trække godkendelsen tilbage. Indløser kan i så fald give et varsel, dog maksimalt på 6 måneder.

D.1.4 Løsninger, der håndterer fulde kortnumre, skal benytte PCI-DSS godkendte virksomheder og systemer til denne håndtering.

D.1.5 Løsninger, der håndterer PIN-koder, skal benytte PCI PIN godkendte virksomheder og systemer til denne håndtering.

## D.2 – Terminaler

**Definition** *En terminal er et apparat, der er i stand til at læse et Dankort, og derefter sender enten en debiterings- eller krediteringstransaktion til transaktionsbehandling.*

**Krav**

D.2.1 Terminaler skal være certificerede i henhold til gældende standarder fra PCI og EMV.

D.2.2 Terminalen skal understøtte læsning af chip via et kontakt interface og/eller kontaktløs læsning af chip. Dog skal terminalen tilbyde minimum samme understøttelse for Dankort som tilbydes for andre kortprodukter.

D.2.3 Terminaler, der understøtter kontaktløst, skal understøtte JCB Contactless (J/Speedy) og Visa Paywave og Mastercard M/Chip.

D.2.4 Terminaler må ikke udskrive informationer fra chip eller magnetstriben på skærm, kvitteringer osv., udover de informationer, der er krævet af nærværende regler.

D.2.5 Betjente terminaler, der benyttes til debiteringer, skal tilbyde kortholderverifikation ved brug af PIN-kode.

D.2.6 Indløser skal i forbindelse med godkendelsen af terminaler sikre, at anvendelsen af øvrige betalingsapplikationer i terminalen ikke kan forringe sikkerheden for Dankort.

D.2.7 Terminalen skal indrettes således, at hvis der i betalingssituationen er tidsforskydning mellem kortkontrol og afregning, skal kortholderverifikation være sket enten i forbindelse med kortkontrol eller beløbsaflevering. Det afleverede beløb skal fremgå tydeligt for kortholderen enten ved kortkontrol eller afregning.

D.2.9 Terminaler skal konfigureres med de parametre, som fremgår af bilag D.X.1 ”Terminal parameters and features”.

D.2.10 Terminaler skal tilbyde kortholder en kvittering med oplysninger om gennemførte/forsøgte transaktioner, medmindre der er et andet system, som sikrer at kortholder har let adgang til tilsvarende oplysninger.

D.2.11 Kvitteringer skal indeholde følgende oplysninger:

- At betalingen blev udført med Dankort
- Maskeret kortnummeret, jf. PCI DSS, eller tilsvarende kortidentifikation, fx maskeret token
- Identifikation af terminalen
- Identifikation af transaktionen
- For chipbaserede transaktioner applikationens identifikation (AID)
- Beløb (DKK)
- Dato og tidspunkt
- Transaktionsresultat
- Forretningsnavn og ekspeditionssted

Valgfrie oplysninger:

Applikationens transaktionstællere (ATC).

D.2.12 Det er en forudsætning for godkendelse af terminaler, der kan integreres med en forretnings kassesystem, at de via integrationen kan videregive PAR data (Payment Account Reference). Dette er med henblik på at understøtte digitale kvitteringer. Terminalen skal kunne læse PAR data både fra kortet og fra svaret på autorisationen. Ved uoverensstemmelse anvendes data fra autorisationen. Hvis data kun er tilgængelig fra en af kilderne skal dette bruges.

D.2.13 *[med virkning fra 1.1.2028]*

Indløser skal sikre, at fysiske forretninger, der anvender integrerede løsninger, leverer kvitteringsdata for køb med Dankort til Dankort scheme for de kortholdere, der har tilmeldt sig modtagelse af elektroniske kvitteringer fra Dankort. Dankort scheme stiller en grænseflade til rådighed, der skal anvendes til at validere om et anvendt kort er tilmeldt, samt at aflevere de kvitteringsdata, der knytter sig til betalingen.

## D.3 – Adgangskontrolsystemer

**Definition** *Adgangskontrolsystemer er apparater, der er i stand til at læse et Dankort, og herefter give adgang til en fysisk facilitet, uden at der sker en betaling. Det kan fx benyttes til at give adgang til et lobby-område med en hæveautomat.*

**Krav**

D.3.1 Uautoriseret kortlæsning skal vanskeliggøres ved udformning af kortlæserenheden eller andre tekniske foranstaltninger.

D.3.2 Kortholder må ikke anmodes om PIN ved anvendelse af et adgangskontrolsystem.

## D.4 – Hæveautomater

**Definition** *En hæveautomat er et ubetjent apparat, der udbetaler kontanter efter at have debiteret Dankortet. En hæveautomat betragtes som en ubetjent terminal, og skal derfor udover kravene i dette afsnit opfylde kravene til ubetjente terminaler i afsnit "D.4 – Hæveautomater".*

**Krav**

D.4.2 En hæveautomat skal foretage stærk autentifikation (fx kræve både kort og PIN) af kortholder ved alle udbetalinger, uanset beløbsstørrelse.

## D.5 – Kort ikke tilstede (CNP)

**Definition** *Kort ikke tilstede (i det følgende "CNP" – Card Not Present) er modtagelse af kortet, hvor der ikke sker en autentifikationen af kortholder ved hjælp af det besiddelseselement, som en fysisk repræsentation af kortet udgør. For at udgøre en fysisk kortrepræsentation skal der på vegne af udsteder være sket en ilægning af kortdata til en fysisk genstand (fx plastikkort, telefon, nøglering), som ikke kan kopieres til en anden genstand.*

*Eksempler på CNP er netbetalinger, postordre og telefonordre.*

**Krav**

D.5.1 Hvis kortholder er til stede i betalingsøjeblikket må indløser kun acceptere CNP betalingen, hvis betalingen er autentificeret med en af følgende:

- Dankort Secured by Nets (se E.4)
- delegeret autentifikation (se D.9)
- kortnummer, udløbsdato og kontrolcifre

Dog kan indløser undtagelsesvis acceptere betalinger, som ikke er autentificerede, hvis Dankort Secured by Nets er ramt af driftsforstyrrelser.

D.5.2 Indløser skal kræve kontrolcifre i de betalingssituationer, som fremgår af D.X.2 "Card-not-present CVC requirements".

D.5.3 CNP systemer skal sende transaktionerne online til processing hos udsteder.

D.5.4 CNP systemer skal være i stand til at autentificere betalinger med Dankort Secured by Nets.

D.5.5 CNP systemer til nethandel skal ved hjælp af tidssvarende kryptering sikre fortrolighed og integritet af kortoplysninger og øvrige betalingsdata.

D.5.6 CNP systemer skal tilbyde kortholder en kvittering indeholdende minimum følgende oplysninger:

- Maskeret kortnummeret, jf. PCI-DSS, eller tilsvarende kortidentifikation, fx maskeret token
- Ordrenummer/transaktionsnummer
- Beløb
- Dato og tidspunkt
- Forretningsnavn
- Transaktionsresultat

D.5.7 CNP systemer må ikke give kortholder mulighed for at indtaste den til kortet hørende PIN-kode.

D.5.8 CNP systemer skal benytte en PSP (Payment Service Provider) til håndtering af fulde kortnumre, autentifikation og autorisation, som er godkendt af Dankort. Liste over godkendte PSP'ere kan ses på dankort.dk.

## D.6 – Dankort Card Manager (DCM)

**Definition** *En "Dankort Card Manager" (herefter DCM) er en personlig softwarebaseret løsning, hvor kortholder kan registrere sine kortoplysninger med henblik på efterfølgende at kunne hente kortoplysninger på en nem og sikker måde til brug for fremtidige online køb.*

**Krav**

D.6.1 Virksomheder, der ønsker godkendelse af en løsning til DCM, skal overfor indløser attestere at vilkårene for DCM-løsning i D.X.3 "Vilkår for Dankort Card Manager" overholdes.

D.6.2 Virksomheder, der ønsker godkendelse af en løsning til DCM, skal overfor indløser beskrive DCM-løsning, som krævet i D.X.3 "Vilkår for Dankort Card Manager".

D.6.3 Indløser skal sikre, at betalinger foretaget ved hjælp af en DCM løsning er markeret så udsteder kan identificere, hvilken DCM der blev anvendt.

## D.7 – [udgået]

## D.8 – Fordelsprogrammer

**Definition**

*Dankort og Dankort-varemærkerne kan indgå i forskellige løsninger der udbydes under betegnelsen Fordelsprogrammer. Fordelsprogrammer er en samlebetegnelse for loyalitetsprogrammer og donationsprogrammer.*

*Et loyalitetsprogram er et koncept, der udbydes med henblik på, at kortholder kan optjene bonus, rabatter og lignende ved brug af Dankortet. Kortholder tilmelder sig et konkret loyalitetsprogram og registrerer sit Dankort hos udbyderen af loyalitetsprogrammet. Udbyderen forestår håndtering af loyalitetsprogrammet, herunder beregning af bonus, rabatter m.v.*

*Donationsprogrammer fungerer således, at forretninger kan tilmelde sig et donationsprogram til fordel for et specifikt formål, hvorefter virksomheden donerer et fastsat beløb eller procentsats, hver gang der foretages køb hos virksomheden med et tilmeldt Dankort. Kortholder registrerer sig ligeledes hos udbyderen af donationsprogrammet og registrerer sit Dankort samt de formål, kortholder ønsker at støtte. Konceptet er således baseret på omsætningsafhængige donationer.*

**Krav**

| | |
|---|---|
| D.8.1 | Indløser skal sikre, at de forretninger som den har Dankort indløsningsaftaler med, ikke igangsætter fordelsprogrammer (eller laver væsentlige ændringer) uden at programmet er godkendt af indløser, samt at der er indgået aftale mellem indløser og udbyderen af programmet. |
| D.8.2 | Ved godkendelse af et program skal indløser forbeholde sig retten til at kræve ny godkendelse, herunder, men ikke begrænset til, ændringer i krav fra Dankort, lovkrav eller ændringer i industri standarder. |
| D.8.3 | Indløser skal i sin aftale med udbyder fastsætte, at kortdata må ikke opbevares hos forretninger tilknyttet fordelsprogrammet. |
| D.8.4 | Indløser skal i sin aftale med udbyder fastsætte, at udbyder er ansvarlig for at fordelsprogrammet overholder de til enhver tid gældende krav fastsat af Dankort scheme, herunder krav om sikkerhedsgodkendelser, samt den til enhver tid gældende lovgivning. |
| D.8.5 | Indløser skal i sin aftale med udbyder fastsætte, at udbyder uden unødigt ophold skal rapportere til indløser alle episoder af formodet eller bekræftet tredjemandsmisbrug eller datakompromittering relateret til materiale eller data, der indeholder information om kortdata eller transaktionsinformation relateret til løsningen og/eller Dankort. |
| D.8.6 | Indløser skal i sin aftale med udbyder fastsætte, at såfremt der opstår sikkerhedsbrud, skal udbyder af fordelsprogrammet følge indløsers anvisninger, herunder efterfølgende undersøgelse af sikkerhedsbruddet og eventuel etablering af yderligere sikkerhedsprocedurer til imødegåelse af fremtidig kompromittering af kortdata. |
| D.8.7 | Indløser skal i sin aftale med udbyder fastsætte, at fordelsprogrammet ikke må forhindre kortholdere i at registrere et Dankort i flere eller øvrige udbyderes fordelsprogrammer. |
| D.8.8 | Indløser skal i sin aftale med udbyder fastsætte, at udbyder af fordelsprogrammet skal indgå aftale med kortholder om brug af fordelsprogrammet. |

Aftalevilkår skal accepteres af kortholder, fx i forbindelse med indrullering og skal efterfølgende være let tilgængelig for kortholder. Aftalen skal som minimum indeholde følgende elementer:

1. Beskrivelse af udbyders fordelsprogram (gennemsigtighed)
2. Oplysning om håndtering og opbevaring af kortdata
3. Oplysning om eventuelle priser og omkostninger ved brug af fordelsprogrammet
4. Information om procedurer for fornyelse og sletning af kortnummer samt aftale.
5. Ændrings- og opsigelsesbetingelser
6. Ansvarsbetingelser for udbyder
7. Krav til beskyttelse af password eller øvrige adgangskontroller, der giver adgang til fordelsprogrammet

D.8.9 Med henblik på evt. scheme-fastsat godtgørelse af udsteder, skal indløser i sin aftale med udbyder fastsætte, at udbyder indenfor 10 arbejdsdage efter udløb af et kvartal skal indsende en opgørelse af antal tilmeldte Dankort pr. udsteder (angivet i ciffer 5 til og med 8 i kortnummeret). Indløser skal endvidere fastsætte en ret til, at udbyder attesterer opgørelsen af ledelsen eller af en statsautoriseret revisor.

## D.9 – Delegeret autentifikation

**Definition**

*Delegering af autentifikation betyder at stærk autentifikation af kortholder, i henhold til betalingslovens krav, ikke udføres af udsteder, men i stedet udføres af en løsning, som udbydes enten af forretningen, eller en af godkendt DCM-løsning. Autentifikationen er dermed delegeret af udsteder via scheme til indløser (og forretning) eller til en DCM-løsning.*

*Løsningen giver mulighed for en smidig købsafvikling for transaktioner, hvor kortet ikke aflæses fysisk i en terminal.*

**Krav**

D.9.1 Indløser skal modtage og behandle ansøgninger om godkendelse til delegeret autentifikation fra alle forretninger. Indløser skal følge følgende proces:

1. Ansøger indsender udfyldt og underskrevet blanket til indløser.
2. Indløser vurderer om kravene er opfyldt, og hvis de er, indstilles løsningen til godkendelse af Dankort scheme, sammen med et id af løsningen.
3. Dankort scheme godkender løsningen og føjer den til listen over godkendte løsninger. Listen er tilgængelig på dankort.
4. Indløser åbner for modtagelse af betalinger, som er markeret med delegeret autentifikation, fra løsningen.
5. Indløser giver besked om godkendelsen til ansøger.

D.9.2 Indløser skal sikre at løsningen overholder følgende krav:

- Ved tilføjelse af kortet benyttes både ”Dankort Secured by Nets” og løsningens egen autentifikation
- Løsningens autentifikation skal overholde myndighedernes krav til stærk autentifikation af kortholder
- Med undtagelse af lav-værdi, kan løsningen ikke anvendes til betaling uden autentifikation
- Der benyttes mindst 2 forskellige faktorer i hver sin kategori
- Faktorerne er uafhængige
- Kodeord/PIN har en kompleksitet på mindst 4 tal
- Kodeord/PIN vises ikke i klartekst
- Kodeord/PIN opbevares ikke i klartekst
- Kopiering af besiddelsesfaktorer er ikke muligt med almindeligt tilgængelige værktøjer
- Der benyttes tidssvarende mekanismer/algoritmer til beskyttelse af data

- Ved køb skal kortholder skal have adgang til information om beløb og forretningens navn
- Der er udpeget en intern sikkerhedsansvarlig for løsningen
- Der er realtids overvågning af misbrugsforsøg
- Forsøg på misbrug bliver rapporteret automatisk til den sikkerhedsansvarlige
- Sikkerheden revideres af uafhængig tredjepart

D.9.3 Indløser skal sikre at information om delegeret autentifikation er markeret i transaktionen, så udsteder kan udlede dette i autorisation og settlement.

D.9.4 Indløser overvåger forretninger, der benytter delegeret autentifikation, og skal give advarsel, hvis tredjemandsbrug 3 kalendermåneder i træk er over 2 basispoint.

Indløser og forretning skal herefter aftale en handlingsplan for nedbringelse af tredjemandsmisbrug. Såfremt en aftale ikke kan indgås, eller aftalen ikke efterleves, fratages forretningen godkendelsen til at anvende delegeret autentifikation.

D.9.5 Indløser indestår for tredjemandsmisbrug overfor udsteder. Der er ikke betalingsgaranti for tredjemandsmisbrug.

# E – TRANSAKTIONSBEHANDLING

## E.1 – Generelle krav

**Vejledning** *Afsnittet beskriver udsteders rolle i behandling af transaktioner, modtaget fra netværket til de leveres til udstedernes datacentraler. Udsteders datacentraler bogfører herefter transaktionerne på kortholderens konto.*

**Krav**

E.1.1 Udsteder skal modtage og behandle alle Dankort transaktioner fra Dankort-netværket. Udsteder må ikke forhindre sine kortholdere i at anvende løsninger til kortmodtagelse, som er godkendt af Dankort scheme, jf. kapitel D.

E.1.2 Udsteder skal modtage og behandle 10 daglige bogføringsleverancer (ISO 8583 leverancer) indeholdende oplysninger om Dankort-forbrug, så udsteder bogfører transaktionerne på kortholders konto. Bogføringsfiler sendes på følgende tidspunkter hver dag: 14:00, 16:00, 17:30, 18:00, 19:00, 20:00, 21:00, 22:00, 23:30 og 01:00.

E.1.3 Løsninger, der håndterer fulde kortnumre, skal benytte PCI-DSS godkendte virksomheder og systemer til denne håndtering.

E.1.4 Løsninger, der håndterer PIN-koder, skal benytte PCI PIN godkendte virksomheder og systemer til denne håndtering.

## E.2 – Behandling af ”kort ikke tilstede” (CNP) transaktioner

**Krav**

E.2.1 Transaktioner, der er markeret som initieret af betalingsmodtager (merchant initiated, MIT) eller abonnementsbetalinger, må ikke afvises af udsteder med krav om yderligere autentifikation medmindre der ligger en konkret, aktuel sikkerhedsmæssig risiko.

E.2.2 Transaktioner, der er markeret som autentificeret via delegeret autentifikation, må ikke afvises af udsteder med krav om yderligere autentifikation medmindre der ligger en konkret, aktuel sikkerhedsmæssig risiko.

## E.3 – Posteringer på kontoen

**Vejledning** *Formålet med at stille krav til posteringsinformation er at sikre kortholder overblik og mulighed for kontrol af, om den enkelte postering er korrekt. Kravene til posteringsinformation er derfor fastlagt med henblik på at give kortholder bedst mulige information.*

**Krav**

E.3.1 Ved hver postering skal som minimum vises:

1. Bogføringsdato
2. Beløb i danske kroner
3. Hvis der er tale om en international transaktion skal tillige angives valutakode og -beløb: Valutabeløbet modtaget fra indløser skal vises.
   Valuta angives med forkortelse, jf. ISO 4217.
4. Brugssted:
   Hævepostering: Pengeinstitutnavn, navn på hæveautomat eller pengeinstituttets registreringsnummer

   Betalingspostering: Forretningsnavn (evt. forkortet)
5. Transaktionsidentifikation:
   Hæveposteringer: De sidste 3 cifre af det transaktionsnummer, der er anført på kvitteringen

   POS-terminalposteringer: De sidste 3 cifre af det transaktionsnummer, der er anført på kvitteringen

   Notaposteringer: De sidste tre cifre af notanummer

   Internet-posteringer: De sidste 3 cifre af ordrenummeret

   Øvrige posteringer: De sidste 3 cifre af det transaktionsnummer, der er anført på kvitteringen.

## E.4 – Krav til understøttelse af Dankort Secured by Nets

**Definition** *Dankort Secured by Nets (DSBN) er en løsning til stærk autentifikation af kortholder i forbindelse med køb på internettet. Autentifikationen udføres af udsteder ved hjælp af en såkaldt Access Control Server (ACS), som er den komponent der behandler anmodningen om autentifikation.*

**Krav**

E.4.1 Udsteder skal sikre, at alle dets kortholdere kan indrullere deres kort i en DSBN ACS. Indrullering skal ske via udsteder eller ved brug af sikker autentifikationsmetode. Ved indrullering skal det sikres, at kortet tilhører den kortholder, som udfører indrulleringen.

E.4.2 Udsteder skal sikre, at dets DSBN ACS giver alle indrullerede kortholdere mulighed for at autentificere sig i forbindelse med køb på internettet.

| | |
|---|---|
| E.4.3 | Udsteder skal sikre, at dets DSBN ACS ikke kræver autentifikation af kortholder, hvis beløbet er under den lovmæssigt fastsatte maksimale grænse, og forretningen ikke eksplicit har bedt om autentifikation. |

## E.5 – Krav til udsteder i forbindelse med Dankort advarselsservice

| | |
|---|---|
| **Definition** | *Dankort advarselsservice er en notifikationsservice, som indløser kan tilbyde e-handelsforretninger for at minimere eller hindre misbrug. Hvis et betalingskort af udsteder er bekræftet misbrugt, og kortet har været anvendt til køb på en hjemmeside i de foregående timer, vil den pågældende forretning modtage en e-mail fra indløser umiddelbart efter. Derved har forretningen mulighed for at forsøge at stoppe forsendelsen af en vare og derved undgå tab. Dankort advarselsservice ændrer ikke på ansvaret for transaktioner, som derfor f.eks. følger de almindelige indsigelsesregler.* |
| **Krav** | |
| E.5.1 | Dankort advarselsservice er baseret på transaktionsinformation, som indgår i det almindelige Dankort transaktionsforløb. Når udsteder via autorisationsdata bekræfter at et betalingskort har været misbrugt, bliver meddelelsen videresendt til indløser, med henblik på at indløser kan advare forretningen. Udsteder skal sikre at dets forretningsgange o.l. understøtter denne brug af autorisationsdata, herunder ift. eventuelle underleverandører som udstederen anvender. |

## E.6 – Behandling af reservationer for kort med saldokontrol

| | |
|---|---|
| **Definition** | *Afsnittet beskriver udsteders forpligtelser ved behandling af reservationer for kort med saldokontrol. En forespørgsel om reservation modtages teknisk i form af en eller flere autorisationsanmodninger. Ved den efterfølgende afregning modtages en eller flere afregningstransaktioner (også kaldet "captures").* |
| **Krav** | |
| E.6.1 | Fra og med dagen, hvor udsteder godkender en reservation eller en fornyelse af en reservation, skal udsteder holde reservationen i 7 bankdage. Udsteder skal sikre, at kortholder har mulighed for at se reservationen, fx via netbank. |
| E.6.2 | Hvis en forretning fremsender afregningstransaktion efter udløb af reservationen, betragtes købet som for sent afregnet. Dette indebærer bl.a., at udsteder har mulighed for tilbageførsel, jf. reglerne i bilag A.X.5, hvis der ikke er dækning på kontoen. |
| E.6.3 | Udsteder skal understøtte behandling af reservationer på 0 kr. (anvendes til kontrol af kortstatus, fx i forbindelse med abonnementer og gem kort). Kortholder skal ikke have mulighed for at se disse. |
| E.6.4 | Udsteder skal understøtte behandling af kortstatusforespørgsel (Account Verification, anvendes til kontrol af kortstatus, fx i forbindelse med abonnementer og gem kort). |
| E.6.5 | Udsteder skal understøtte behandling af reservationsfornyelser (anvendes fx af forretninger, som ikke har kunnet afsende vare indenfor fristen angivet i E.6.1). |
| E.6.6 | Udsteder skal understøtte behandling af opdelte afregningstransaktioner, dvs. hvor forretningen foretager en enkelt reservation, men derefter sender flere mindre afregningstransaktioner (anvendes af forretninger i forbindelse med delleverancer). |
| E.6.7 | Udsteder skal understøtte delvis godkendelse af en reservation. Udsteder skal delvist godkende reservationer i situationer, hvor udsteder kun kan godkende et lavere beløb end det |

| | |
|---|---|
| | forretningen har forespurgt om, og hvor forretningen i forespørgslen har anvendt en transaktionstype, der giver mulighed for delvis godkendelse. |
| E.6.8 | Udsteder skal understøtte behandling af tillægsreservationer, dvs. hvor forretningen initialt laver en reservation af et estimeret beløb, og hvis dette viser sig ikke at være tilstrækkeligt, forespørger på at få reservationen forhøjet, hvorefter der sendes en enkelt afregningstransaktion. |
| E.6.9 | Udsteder skal understøtte annullering af reservationer, herunder delvis annullering (anvendes fx hvor en forretning ikke kan levere alle varer). Straks efter annullering skal reservationen overfor kortholder være fjernet/fremstå som slettet/justeret. |
| E.6.10 | Udsteder skal sikre, at en reservation overfor kortholder fremstår som afregnet/bogført straks efter udsteder har modtaget den endelige afregningstransaktion. |