Dankort Schemeregler

Dateret: 31. januar 2024

Indhold

Ændringslog

Version	Afsnit	Ændring	Ansvarlig
31.01.2024	A.5.1	Krav ændret (tilføjet specifikation af proces ved tvister)	Espen Jürgensen
	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	Espen Jürgensen
	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	Espen Jürgensen
31.01.2023	B.1	Definition af co-badged præciseret, så det omfatter kort uanset form-faktor, samt ref. til IFRs definition.	Espen Jürgensen
	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	Anna Gissel
31.03.2022	B.11.7	Udsteders indsigelsesfrist for manglende dækning er udvidet fra 1 til 3 bankdage	Anna Gissel
	D.2.8	Krav slettet	Anna Gissel

	D.2.12	Krav vedr. PAR til digitale kvitteringer tilføjet	Espen Jürgensen
31.01.2022	Generelt indhold s. 3	Ændringslog tilføjet (indholdsfortegnelse opdateret)	Anna Gissel
		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	Anna Gissel
	A.3.3	Krav fjernet: *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.*	Anna Gissel
	E.5	Tilføjelse af nyt krav: *Krav til udsteder i forbindelse med Dankort advarselsservice* Indholdsfortegnelse opdateret	Anna Gissel

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 indløst hos 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.
Licenshaver	Et pengeinstitut, der har en gyldig Dankort licensaftale.
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.

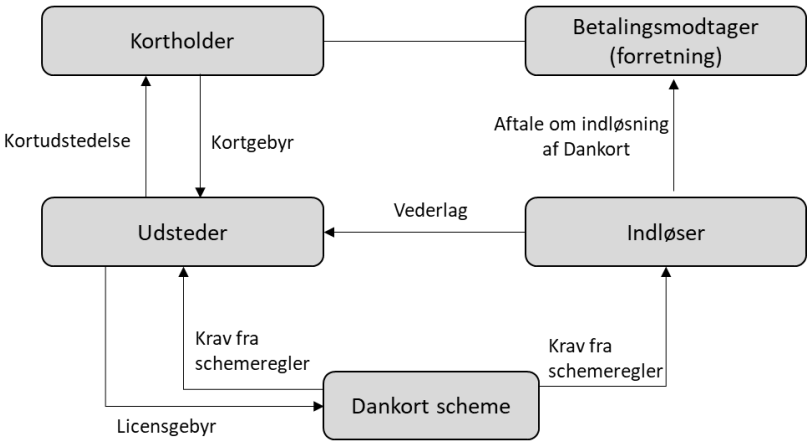
A – GENERELLE VILKÅR

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

Potentielle justeringer til schemereglerne offentliggøres to gange årligt – henholdsvis sidste uge i januar og sidste uge i juli.

Dankort scheme kan i særlige tilfælde offentliggøre justeringer til schemereglerne på andre tidspunkter af året end på de to angivne tidspunkter.

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.4 – Dankort prismodel og gebyrer

Vejledning

Dankort scheme fastsætter en samlet pris for indløsning af Dankort. Indløser beregner sig herefter betaling for ydelser som indsamling, transaktionsbehandling og indløsning.

En procentdel af omsætningen udbetales som vederlag til udstederne. Procentdelen fastsættes af Dankort scheme indenfor gældende regulering.

Der vil efter hvert årsskifte blive foretaget en opgørelse mellem de faktiske og de forventede indtægter/udgifter benyttet i beregningen af vederlagsbetalingen til udstederne. Afvigelser mellem de faktiske og forventede indtægter/udgifter vil blive indregnet i de kommende års vederlagssatser.

Krav

A.4.1 Licenshavende pengeinstitutter skal årligt betale et licensgebyr, hvilket fremgår af prislisten for Dankort jf. bilag A.X.2.

A.4.2 Ved indgåelse af aftale om licens til Dankort skal pengeinstituttet betale engangsgebyr for systemopsætning og tilslutning til Dankort infrastrukturen. Engangsgebyret fremgår af prislisten for Dankort jf. bilag A.X.2.

A.4.3 Øvrige gebyrer som tilfalder licenshavende pengeinstitutter, fremgår af prislisten for Dankort jf. bilag A.X.2.

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.

B – KORTUDSTEDELSE

B.1 – Brugerregler for Dankort og øvrig information til kortholder

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.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 Dankort skal være 16 cifre og opfylde 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 enten begge være i farve eller være hvide. 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.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 kendes af kortholder. PIN-brev, selvvalgt PIN-kode eller elektronisk PIN og det fysiske Dankort må derfor ikke mødes, før begge dele separat er kommet kortholder i hænde.

For udstedere, der understøtter selvvalgt PIN via netbank/mobilbank/mobil app, kan udsteder give adgang til at kortholder efterfølgende kan se denne PIN-kode i denne løsning. Udsteder kan også give adgang til, at kortholder med eller uden selvvalgt PIN-kode får adgang til at rekvirere denne kode via SMS.

Kortholder tilknytter selvvalgt kode til digitale kort i wallet.

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:

1. Der må ikke udsendes ny/ændret PIN-kode til allerede udstedte Dankort.
2. Bestilling og udsendelse af PIN-brev/Elektronisk PIN skal følge Dankort-reglerne uanset til hvilket kort PIN-brevet/elektronisk PIN udsendes.
3. PIN-koden skal stamme fra kort udstedt af Dankort-udstederen.
4. Der må ikke bestilles og udsendes en PIN-kode, hvor bare ét af kortene, der benytter samme kode er spærret som følge af:

- Mistanke om eller konstatering af 3.-mandsmisbrug med kort, hvis misbrug har fundet sted ved anvendelse af PIN-kode
- Stjålet/bortkommet kort og mistanke om kompromittering af PIN-kode

B.6 – [udgået – se ændringslog for august 2023]

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 (med virkning fra 1/10/2024)

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 tredjemands misbrug

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: • Produktion af fysiske kort • Personalisering og levering af fysiske kort 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 skal de udstedte tokens være 19 cifre. De første 6 cifre for Dankort, der er co-badged med Visa, skal være 357107, og for øvrige Dankort skal de være 357106.
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 *(med virkning fra 1/1/2025)*

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 ikke understøtter digitale co-badgede 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 udsteder for debitering/kreditering af kortholder.

C.1.2 Indløser må kun indgå Dankort betalingskortaftale med betalingsmodtagere, der benytter en konto i et pengeinstitut med Dankort licensaftale. Pengeinstituttet skal deltage i sumclearingen, da Dankort omsætning udbetales via sumclearingen.

Indløser kan aftale med betalingsmodtager at omsætning udbetales til indløser, til en konto i et pengeinstitut der har licens til udstedelse af Dankort og derved deltager i sumclearingen, hvorefter indløser udbetaler omsætning til betalingsmodtager, til en konto anvist af betalingsmodtager. Betalingsmodtager skal acceptere regler og vilkår for udbetaling af omsætning via indløser.

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 Indløser skal en gang årligt 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.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. Konto skal være i et pengeinstitut, der deltager i sumclearingen. Såfremt det er aftalt mellem indløser og betalingsmodtager kan omsætning udbetales til indløser til en konto i et pengeinstitut der deltager i sumclearingen, hvorefter indløser udbetaler omsætning til 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.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.

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.
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.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 – Dankort på mobilen

Definition *Dankort på mobilen er en personlig softwarebaseret Løsning, hvor kortholder kan virtualisere sit Dankort til mobiltelefonen. Virtualiseringen sker til en wallet, som er en sikker app (mobil applikation), der kan indeholde et eller flere virtualiserede kort. Kortet kan herefter anvendes til fysisk handel.*

Dankort på mobilen med begrænset trækningsret er en variant, hvor kortholder virtualiserer sit Dankort til en anden persons mobiltelefon. Kortholder giver hermed en anden person mulighed for at benytte kortholders virtuelle kort, men med begrænsede brugsmuligheder fastsat af kortholder og reglerne i dette afsnit.

Krav

D.7.1 Anvendelse af Dankort på mobilen til fysisk handel er ligestillet med anvendelse af kontaktløst Dankort i fysisk handel, og indløser skal derfor behandle både transaktioner og indsigelser efter samme regler.

D.7.2 Indløser skal modtage transaktioner, der er fortaget med Dankort på mobilen.

D.7.3 Indløser skal sikre, at grænserne for brug af Dankort på mobilen er de samme som for det fysiske, kontaktløse Dankort. Her skal indløser sikre, at et begrænset, virtuelt kort ikke kan anvendes ud over en grænse for maksimalt dagligt brug, som er fastsat af Dankort scheme.

D.7.4 Indløser skal sikre, at betalinger foretaget ved hjælp af Dankort på mobilen er markeret så udsteder kan identificere, hvilken løsning der blev anvendt.

D.7.5 Før indløser kan godkende en Løsning til Dankort på mobilen skal den certificeres af Dankort scheme. Certificeringen verificerer, at den pågældende Løsning lever op til vilkårene i D.X.4 "Dankort Wallet Requirements and Certification".

D.7.6 Virksomheder, der ønsker godkendelse af en løsning til Dankort på mobilen skal overfor indløser attestere at vilkårene i D.X.4 "Dankort Wallet Requirements and Certification" overholdes.

D.7.7 Virksomheder, der ønsker godkendelse af en løsning til Dankort på mobilen, skal overfor indløser beskrive løsningen, som krævet i D.X.4 "Dankort Wallet Requirements and Certification".

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 indløser 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 indløser. 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 for 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.

Bilag A.X.1 Forretningsgang for inddækning af tab som følge af overtræk på betalingsmodtagers konto

Opdateret: 31.01.2022

Ændringslog

Version	Afsnit	Ændring	Ansvarlig
31.01.2022	Information til indløser om overtræk	Krav fjernet: *Betalingsmodtagers pengeinstitut skal informere indløser om overtræk, der kan forventes at give anledning til tab for indløser. Dette skal ske snarest muligt.* *Hvis en betalingsmodtagers konto har været i konstant overtræk i mere end 5 hverdage, skal der under alle omstændigheder rettes henvendelse til indløser.*	Anna Gissel
	Opgørelse af tab hos pengeinstitutter	Krav om at pengeinstitut skal informere indløser er fjernet	Anna Gissel
	Opgørelse af tab hos pengeinstitutter	Justering: *Oplys om det kontonummer, hvor pengene skal indsættes.* Sætning fjernes da dette er angivet i afsnittet "Krav om inddækning af tab – oversigt over information som skal medsendes"	Anna Gissel

Opgørelse af tab hos pengeinstituttet

Når betalingsmodtagers pengeinstituttet har konstateret tab som følge af indløsers træk på betalingsmodtagers konto skal pengeinstituttet vurdere, om det er muligt at inddrive beløbet hos betalingsmodtager.

Såfremt hel eller delvis inddrivelse ikke er muligt, skal pengeinstituttet opgøre tabet ud fra følgende:

- Såfremt pengeinstituttet har bevilget kassekredit eller overtræk til kontoen hæfter pengeinstituttet for denne kredit. Det er først når den tilknyttede kredit er overskredet, at der kan rettes krav til indløser om inddækning af tab.

  Kun tab ud over den bevilgede kredit, der stammer fra indløsers træk, kan kræves tilbagebetalt.

- Renter og gebyrer pålagt af pengeinstituttet i forbindelse med overtræk skal IKKE indgå i opgørelsen.

Fremsendelse af opgørelse til indløser skal indeholde:

- information om opgørelsen, herunder dokumentation for det pågældende overtræk samt
- information om den vurdering, der ligger til grund for, at pengeinstituttet ikke mener at kunne inddrive beløbet hos betalingsmodtager.

Startdato for opgørelse af kontoen er det tidspunkt, hvor kontoen går i minus og, der ikke efterfølgende er inddækning af overtrækket.

Pengeinstituttet skal fremsætte skriftlig krav til indløser om tilbagebetaling af beløbet, fratrukket eventuelle renter og gebyrer.

Fremsendelse af oplysninger til indløser foretages her

Situation	Dokumentation
Konkurs	• Kontoforhold opgjort/opsagt • Kopi af opsigelse eller anden dokumentation for ophør af kontoforhold • Oplysning om kurator og dekretdato • Forretningsnummer • Størrelsen af det beløb, der kræves tilbage betalt • Dokumentation for tabets opgørelse i form af kopi af kontoudtog for perioden fra tidspunktet for Nets' træk til tidspunktet, hvor tilbagebetalingskravet gøres gældende. • Beskrivelse af tiltag for inddrivelse eller op- lysninger om, hvorfor inddrivelse ikke er forsøgt.
Kontoforhold opgjort/opsagt	• Kopi af opsigelse eller anden dokumentation for ophør af kontoforhold • Forretningsnummer • Størrelsen af det beløb, der kræves tilbage betalt • Dokumentation for tabets opgørelse i form af kopi af kontoudtog for perioden fra tidspunktet for indløsers træk til tidspunktet, hvor tilbagebetalingskravet gøres gældende • Beskrivelse af tiltag for inddrivelse eller oplysninger om, hvorfor inddrivelse ikke er forsøgt
Øvrige situationer, hvor tabet er opgjort	• Kontoen skal være opgjort • Kopi af opsigelse eller anden dokumentation for ophør af kontoforhold • Forretningsnummer • Størrelsen af det beløb, der kræves tilbage- betalt • Dokumentation for tabets opgørelse i form af kopi af kontoudtog for perioden fra tidspunktet for indløsers træk til tidspunktet, hvor tilbagebetalingskravet gøres gældende • Beskrivelse af tiltag for inddrivelse eller oplysninger om, hvorfor inddrivelse ikke er forsøgt

Krav om inddækning af tab – oversigt over information som skal medsendes

- Pengeinstitut navn
- Dato for indsendelse
- Forretningsnavn
- Forretningsnummer
- Opgørelsesdato – dato for opgørelse af pengeinstituttets krav
- Opgjort tab/størrelsen af det beløb, der kræves tilbagebetalt
- Dokumentation for tabets opgørelse (se ovenfor)
- Beskrivelse af vurdering til grund for pengeinstituttets krav. Hvorfor vurderes, at pengene ikke kan inddrives.
- Information om kontonummer, hvor pengene skal indsættes
- Information om, hvorvidt der har været tilknyttet en kassekredit eller godkendt overtræk.
- Underskrift

A.X.5 Regler for indsigelser og tilbageførsler

Opdateret 31.01.2024

Ændringslog

Version	Afsnit	Ændring	Ansvarlig
31.01.2024	(tabel)	Årsagskode 4544: "Kan også anvendes, hvis kortholder er trukket for et abonnement, som forretningen ikke tydeligt havde oplyst om."	Espen Jürgensen
	(tabel)	Årsagskode 4717: "For at kunne anvende denne årsag skal kortholder have nægtet modtagelse eller sendt varen retur i samme stand indenfor 14 dage fra modtagelse (medmindre kortholder har fraskrevet sig fortrydelsesret ved bestilling),"	Espen Jürgensen
	(tabel)	Årsagskode 4554: Ændret til også at omfatte fysisk handel, såfremt der er skriftligt aftalt bestilling	Espen Jürgensen
31.08.2023	(tabel)	Præciseret at ved "3. mandsmisbrug fysisk handel" skal årsagskode 4714 som udgangspunkt anvendes. Tilføjet "3. mandsmisbrug øvrig" med årsagskode 4720, som kun benyttes hvis der er fx systemmæssige årsager til, at 4714 ikke kan anvendes.	Espen Jürgensen
31.01.2023	Bilagsnavn	Navn på bilag ændret for at tydeliggøre, at det er tale om regler, ikke kun en guide.	Espen Jürgensen
	(tabel)	Årsagskode 4714 (3. mandsmisbrug fysisk handel) ændret til at omfatte betaling med stærk autentifikation, så fx biometri er inkluderet tillige med PIN. Årsagskode 4720 (3. mandsmisbrug fysisk handel) ændret fra signatur til at omfatte betalinger uden stærk autentifikation, og indløsers betalingsgaranti ændret til 8000 dkk. Oprydning af beskrivelse af årsagskoder, så de kun indeholder beskrivelser. Betalingsgaranti fremgår nu entydigt af kolonnerene "Udsteder betalingsgaranti" og "Indløser betalingsgaranti".	Espen Jürgensen
18.08.2022	Indledning	Nyt afsnit 'Indledning' tilføjet (indhold fra tidligere indledning i bilag A.X.4 (oversat fra engelsk) integreret i A.X.5)	Anna Gissel
	Kategorier	Kategorien Betalingsgaranti er opdelt i hhv. Udsteders og Indløsers betalingsgaranti	Anna Gissel
	Ændret hæftelse ved chargeback med årsagskoder 4711, 4714, 4718	Ved indsigelser med årsagskode 4711, 4714 eller 4718 gælder følgende betalingsgarantier: Udsteders betalingsgaranti: 2.000 kr. Indløsers betalingsgaranti: 6.000 kr. Ændringerne gælder for følgende kategorier: • Manglende dækning/beløb over betalingsgaranti	Anna Gissel

		• 3.mandsmisbrug i fysisk handel (PIN-terminal) • 3.mandsmisbrug fjernsalg	
	Undtagelse til bestemmelser om betalingsgarantier generelt	Tilføjelse: Ovennævnte betalingsgarantier gælder i øvrigt ikke, hvis virksomheden driver inkassovirksomhed, eller hvis virksomheden inddriver skat, moms eller told.	Anna Gissel
31.03.2022	Udsteders indsigelser Underkategori: Manglende dækning/beløb over betalingsgaranti	Tidsfrist ændret fra 1 til 3 bankdage	Anna Gissel
	Udsteders indsigelser Underkategori: Manglende dækning (for sent afregnet)	Tidsfrist ændret fra 1 til 3 bankdage	Anna Gissel
	Udsteders indsigelser – Indløsers rettigheder Dokumentation	Rettelse/tilføjelse i sætning: *Dokumentation der beviser, at ~~en af ovenstående betingelser er gældende~~ udsteders chargeback er ugyldig.*	Anna Gissel
	Kortholders indsigelser (relateret til misbrug) – Indløsers rettigheder Underkategori: Overordnet	Tilføjelse/rettelse: *Hvis indløser har efterspurgt dokumentation fra udsteder, og denne ikke leveres, har indløser ret til at tilbagekalde indsigelsen.* Sletning: Indløser kan bede udsteder sende kortholders tro og love erklæring. Hvis udsteder ikke kan levere denne, har indløser ret til at tilbagekalde indsigelsen.	Anna Gissel
	Kortholders indsigelser øvrige (ej relateret til misbrug) – Indløsers rettigheder	Tilføjelse: [Indløser kan tilbagekalde en indsigelse, hvis det kan dokumenteres, at udsteders chargeback er ugyldig]*, herunder hvis udsteders chargeback er modtaget for sent.* *Dokumentation der beviser, at udsteders chargeback er ugyldig.*	Anna Gissel

Indledning

Compliance og tvister. Hvis en chargebacksag ikke kan løses i henhold til nærværende gældende schemeregler, skal sagen eskaleres til Dankort scheme, som vil afgøre det retlige ansvar i den pågældende indsigelsessag.

Udsteder og/eller indløser kan indsende eventuelle tvister til Dankort scheme, hvis:

- der ikke eksisterer en relevant årsagskode til den pågældende tvist
- en schemeregel ikke er blevet efterlevet
- der kan dokumenteres et økonomisk tab som direkte følge af den manglende efterlevelse af schemereglerne

Dankort scheme kan opkræve et behandlingsgebyr fra den part, som findes ansvarlig i den pågældende sag.

Rettigheder og forpligtelser: Rights and obligations:

- En udsteder kan ikke gennemføre mere end én chargeback per transaktion indenfor den givne tidsramme, som gælder for den pågældende indsigelseskode. Udsteder kan lave chargeback for hele transaktionsbeløbet eller for dele af det samlede beløb.
- Indløser må ikke processere en ny tilbagekaldelse af den samme transaktion efter at have modtaget en chargeback.
- Refundering for den samme transaktion må kun modtages én gang af hhv. udsteder, indløser, forretning eller kortholder. Udsteder og indløser er ansvarlig for at undersøge og identificere refunderinger forud for hver indsigelsesproces..
    - Eksempel: når en udsteder har bogført en betalingstransaktion på kortholders konto, og derefter vælger at udnytte sin indsigelsesret, skal udsteder kreditere kortholder for det beløb, som der gennemføres chargeback for. Udsteder skal sikre, at kortholder ikke bliver dobbeltkrediteret som følge af en gennemført chargeback og en refundering gennemført af forretningen.
    - Eksempel: hvis en kortholder dobbeltkrediteres (som følge af både en gennemført chargeback samt en refundering initieret af forretningen), skal indløser i tide gennemføre samt dokumentere en tilbagekaldelse af transaktionen. Hvis tidsfristen for tilbagekaldelse er overskredet, skal sagen afgøres udenfor den almindelige indsigelsesproces – fx ved at indsende en tro og love-erklæring.
- Det er ikke tilladt for udsteder vedvarende at gennemføre indsigelser med årsagskode 4711 (manglende dækning) for den samme kortholder for et beløb over betalingsgarantien. Efter 3 indsigelser på samme kort grundet manglende dækning modtaget indenfor en periode på 3 måneder (hvor hver indsigelse kan dække over flere transaktioner), hæfter udsteder for efterfølgende indsigelser. Hver indsigelsessag defineres som transaktioner med samme posteringsdato.

Udsteders indsigelser

Indsigelser i denne kategori er initieret af udsteder og ikke på baggrund af en indsigelse fra kortholder. Årsagen til at udsteder rejser sagen, er overtræk på kortholders konto og dermed manglende dækning for køb. Udsteder har pligt til at underrette kortholder om alle køb, der tilbageføres under denne kategori.

Underkategori	Beskrivelse	Chargeback årsagskode	Udsteders betalingsgaranti	Indløsers betalingsgaranti	Dokumentation	Tidsfrist
Overordnet	Indsigelser i denne kategori er initieret af udsteder og ikke på baggrund af en indsigelse fra kortholder. Årsagen til at udsteder rejser sagen, er overtræk på kortholders konto og dermed manglende dækning for køb. Udsteder har pligt til at underrette kortholder om alle køb, der tilbageføres under denne kategori.					
Manglende dækning/beløb over betalingsgaranti	Hvis der ikke er dækning for beløbet på kortholders konto.	4711	Fysisk handel: 2.000 kr.* Internethandel: Ingen* * kun beløbet over garantien, der ikke er dækning for, må tilbageføres	Fysisk handel: 6.000 kr. Internethandel: 8.000 kr.	Ingen	3 bankdage fra postering til kortholders konto
Manglende dækning For sent afregnet	Hvis en transaktion er afregnet mere end 7 hverdage fra købsdato, og der ikke er dækning på kortholders konto.	4712	Ingen	Ingen	Ingen	3 bankdage fra postering til kortholders konto
Kort spærret eller kortstatus ukendt på købsdato (offline transaktion)	Hvis kortet var spærret eller status ukendt på købsdato, og købet er gennemført offline uden kontrol af kortstatus.	4715	Ingen	Ingen	Ingen	120 kalenderdage fra købsdato
Indløsers rettigheder	Indløser kan tilbagekalde alle indsigelser i denne kategori, hvis én af nedenstående betingelser er opfyldt: • Chargeback er modtaget for sent • Kortet var ikke spærret, da der blev lavet chargeback • 3 chargebacks grundet manglende dækning på samme kort er modtaget inden for en periode på 3 måneder • Indløser kan dokumentere, at transaktionen var sendt til udsteder inden for 7 hverdage fra købsdato • Indløser kan dokumentere, at kortet ikke var spærret på købstidspunktet				Dokumentation der beviser at udsteders chargeback er ugyldig.	10 kalenderdage fra modtagelse af chargeback

Kortholders indsigelser (relateret til misbrug)
Indsigelser fra kortholder relateret til 3.mandsmisbrug på tabte eller stjålne kort. Under denne kategori skal kortholder underskrive tro og love -erklæring indeholdende alle de transaktioner, som kortholder ikke kan vedkende sig.
Kortet skal spærres før der kan laves chargeback, og alle ej vedkendte transaktioner skal misbrugsrapporteres, inklusiv eventuelle transaktioner, der ikke kan tilbageføres.

Underkategori	Beskrivelse	Chargeback årsagskode	Udsteders betalingsgaranti	Indløsers betalingsgaranti	Dokumentation	Tidsfrist
3.mandsmisbrug fysisk handel	Hvis kortholder ikke vedkender sig køb, og kortet er enten tabt eller stjålet på købstidspunktet.	4714	2.000 kr. (0 kr. hvis uden stærk autentifikation)	6.000 kr. (8.000 kr. hvis uden stærk autentifikation)	Tro og love-erklæring underskrevet af kortholder skal leveres til indløser på forlangende	120 kalenderdage fra købsdato
3. mandsmisbrug fjernsalg	Hvis kortholder ikke vedkender sig køb foretaget på internettet.	4718	Ingen	8.000 kr.	Tro og love-erklæring underskrevet af kortholder skal leveres til indløser på forlangende	120 kalenderdage fra købsdato
3. mandsmisbrug For sent afregnet	Hvis kortholder ikke vedkender sig køb, og transaktionen er afregnet senere end 7 dage fra købsdato.	4713	Ingen	Ingen	Tro og love-erklæring underskrevet af kortholder skal leveres til indløser på forlangende	120 kalenderdage fra købsdato
3. mandsmisbrug øvrig	(benyttes kun i visse situationer hvor 4714 ikke kan anvendes af systemmæssige årsager)	4720	Ingen	8.000 kr.	Tro og love-erklæring underskrevet af kortholder skal leveres til indløser på forlangende	120 kalenderdage fra købsdato
Indløsers rettigheder	Indløser kan tilbagekalde en indsigelse, hvis det kan dokumenteres, at udsteders chargeback er ugyldig, herunder hvis udsteders chargeback er modtaget for sent. Hvis indløser har efterspurgt dokumentation fra udsteder, og denne ikke leveres, har indløser ret til at tilbagekalde indsigelsen.				Dokumentation der beviser, at udsteders chargeback er ugyldig.	45 kalenderdage fra modtagelse af chargeback

Kortholders indsigelser øvrige (ej relateret til misbrug)
Øvrige kortholderindsigelser omfatter transaktioner, hvor kortholder selv har deltaget i købet. Inden udsteder sender chargeback til indløser, skal udsteder sikre sig at kortholder forinden har forsøgt at løse sagen direkte med forretningen. Udsteder skal modtage dokumentation fra kortholder, der beviser at kortholder har kontaktet forretningen i et forsøg på at løse sagen.

Underkategori	Beskrivelse	Chargeback årsagskode	Udsteders betalingsgaranti	Indløsers betalingsgaranti	Dokumentation	Tidsfrist
Dobbelt debitering	Kortholder mener at været debiteret to eller flere gange for det samme køb. Debiteringerne skal være sket til samme kort, samme beløb i DKK, fra samme forretning og på samme købsdato.	4351	Ingen	Ingen	Ingen	120 kalenderdage fra købsdato
Abonnement opsagt/uoplyst	*Køb fra og med 1. marts 2024:* Kortholder mener at have opsagt et abonnement (tilbagevendende betaling), hvorefter forretningen fortsætter med at debitere kortholder. Kan også anvendes, hvis kortholder er trukket for et abonnement, som forretningen ikke tydeligt havde oplyst om. Kortholder skal have opsagt abonnement i henhold til forretningens vilkår for opsigelse. Forretningen skal gives 30 dage fra kortholder har kontaktet denne, for at give mulighed for tilbagebetaling af det omtvistede beløb til kortholder. *Køb før 1. marts 2024:* Kortholder mener at have opsagt et abonnement (tilbagevendende betaling),	4544	Ingen	Ingen	Kopi af forretningens vilkår for abonnement og kortholders opsigelse af samme inkl. dato og tidspunkt for opsigelse. Udsteder skal levere dokumentationen til indløser på forlangende.	120 kalenderdage fra købsdato

	hvorefter forretningen fortsætter med at debitere kortholder. Kortholder skal have opsagt abonnement i henhold til forretningens vilkår for opsigelse. Forretningen skal gives 30 dage fra kortholder har kontaktet denne, for at give mulighed for tilbagebetaling af det omtvistede beløb til kortholder.					
Fortrydelsesret udnyttet	*Køb fra og med 1. marts 2024:* Denne årsag kan kun anvendes ved internet- og MOTO-transaktioner. For at kunne anvende denne årsag skal kortholder have nægtet modtagelse eller sendt varen retur i samme stand indenfor 14 dage fra modtagelse (medmindre kortholder har fraskrevet sig fortrydelsesret ved bestilling), og kortholder skal have informeret forretningen om udnyttelse af fortrydelsesret. Forretningen skal gives 30 dage fra kortholder har kontaktet denne, for at give mulighed for tilbagebetaling af det omtvistede beløb. *Køb før 1. marts 2024:* Denne årsag kan kun anvendes ved internet- og MOTO-transaktioner. For at kunne anvende denne årsag, må varer ikke have været i kortholderes besiddelse, og kortholder skal have informeret forretningen om udnyttelse af fortrydelsesret. Forretningen skal gives 30 dage fra kortholder har kontaktet denne, for at give mulighed for tilbagebetaling af det omtvistede beløb.	4717	Ingen	Ingen	Dokumentation for at kortholder rettidigt har kontaktet forretningen for udnyttelse af fortrydelsesret, samt at pakke er nægtet modtaget/ikke afhentet af kortholder eller er sendt tilbage indenfor fristen. Udsteder skal levere dokumentationen til indløser på forlangende.	120 kalenderdage fra købsdato
Kortholder godkender ikke det fulde beløb	Denne årsag kan kun anvendes ved internet- og MOTO-transaktioner.	4719	Ingen*	Ingen	Dokumentation for at kortholder har	120 kalenderdage fra købsdato

	Den kan bruges, hvis kortholder ikke har godkendt det beløb der er trukket, eller beløbet er større end hvad kortholder har godkendt.		* kun beløbet over det godkendte må tilbageføres		kontaktet forretningen i forsøg på at løse sagen samt ordrebekræftelse, der indeholder det beløb, kortholder har godkendt, skal leveres til indløser på forlangende.	
Varer/serviceydelse ikke leveret	*Køb fra og med 1. marts 2024:* Kan anvendes, hvor kortholder ikke har modtaget bestilte varer eller serviceydelser. Gælder alene ved skriftligt aftalt bestilling til fremtidig levering. Ved aftale om forudbetaling må der ikke laves tilbageførsel før forventet leveringsdato, medmindre det kan dokumenteres, at forretningen ikke vil levere. Årsagskoden kan ikke anvendes for varer/ydelser købt via en formidler, eller hvis manglende levering skyldes, at forretningen er erklæret konkurs, medmindre forretningen har trukket beløbet inden varen er afsendt, og der IKKE er indgået aftale om forudbetaling. *Køb før 1. marts 2024:* Denne årsag kan kun anvendes ved internet- og MOTO-transaktioner, hvor kortholder ikke har modtaget varer eller serviceydelser. Forretningen må ikke trække beløbet fra kortholder, før varer eller serviceydelser sendes, medmindre der er aftalt forudbetaling. Ved aftale om forudbetaling må der ikke laves chargeback før forventet	4554	Ingen	Ingen	Dokumentation for at kortholder har kontaktet forretningen i forsøg på at løse sagen skal leveres til indløser på forlangende.	120 kalenderdage fra *køb*sdato <u>Ved forudbetaling</u>: 120 kalenderdage fra forventet *levering*sdato

	leveringsdato, medmindre det kan dokumenteres, at forretningen ikke vil levere. Årsagskoden kan ikke anvendes for varer/ydelser købt via en formidler, eller hvis manglende levering skyldes, at forretningen er erklæret konkurs, medmindre forretningen har trukket beløbet inden varen er afsendt, og der IKKE er indgået aftale om forudbetaling.					
Indløsers rettigheder	Indløser kan tilbagekalde en indsigelse, hvis det kan dokumenteres, at udsteders chargeback er ugyldig, herunder hvis udsteders chargeback er modtaget for sent. Hvis indløser har efterspurgt dokumentation fra udsteder, og denne ikke leveres, har indløser ret til at tilbagekalde indsigelsen.				Dokumentation der beviser, at udsteders chargeback er ugyldig.	45 kalenderdage fra modtagelse af chargeback

Ovennævnte betalingsgarantier gælder i øvrigt ikke, hvis virksomheden driver inkassovirksomhed, eller hvis virksomheden inddriver skat, moms eller told.

Misbrugsrapportering

Udsteder skal misbrugsrapportere alle transaktioner, hvor der er tale om 3.mandsmisbrug. Ved 3.mandsmisbrug skal kortet spærres og transaktionerne misbrugsrapporteres, inden der kan gennemføres chargeback via Dankort chargeback system.

ATM-transaktioner skal også misbrugsrapporteres til scheme via Dankort chargeback system.

Misbrugsårsag	**Anvendes ved**
Tabt kort	tabt kort, hvor der er transaktioner, som er misbrug af 3.mand
Stjålet kort	stjålet kort, hvor der er transaktioner, som er misbrug af 3.mand
Kort afsendt, ej modtaget af kortholder	ej modtaget kort, hvor der er transaktioner, som er misbrug af 3.mand
Kontoovertagelse	fx identitetstyveri, hvor 3.mand har overtaget kontrol over kortholders konto
Modifikation af data	situationer, hvor data for kortbetaling er modificeret af 3.mand under købsproces (gælder kun fjernsalg)
Manipulation af kortholder	kortholder er blevet narret til at oplyse personlige koder for at 3.mand kan gennemføre køb
Fjernsalg/internet	kortnummer misbrugt af 3.mand til at gennemføre køb (gælder kun fjernsalg)
Andet	3.mandsmisbrug hvor ingen af de øvrige årsager kan anvendes

A.X.6 Behandling af Dankort ind-sigelser

Januar 2024

Indholdsfortegnelse

Ændringslog

Dato	Ændring	Forfatter
31.01.2024	Første udgave baseret på "Vejledning Nets' opgaver vedr. Dankort (februar 2018)"	Espen Jürgensen

Om dette dokument

Dette dokument beskriver roller, ansvar og arbejdsgange i forbindelse med behandling af indsigelser og tilbageførsler for Dankort. Målgruppen er medarbejdere, der enten som indløser, scheme, udsteder (eller serviceleverandør til denne) arbejder med indsigelser og tilbageførsler.

Rollefordeling

Kortudsteders opgaver/ansvar

Kortudsteder har det fulde ansvar for indsigelsesbehandling over for kortholder, herunder:

- kontakt til, og kommunikation med kortholder
- vurdering af indsigelserne
- bestilling af evt. nota hos indløser
- vurdering af kortholders ansvar
- træk af evt. selvrisiko
- kreditering af kortholders konto
- oprettelse/indsendelse af indsigelsen til kortindløser.

Kortudsteder skal dække transaktioner op til betalingsgarantien, jf. Dankort schemeregler A.X.5.

Hvis en forretning har spørgsmål om Dankort-indløsning henvises til indløser. Indløser kan dog i tilfælde af sager, hvor en forretning er debiteret på baggrund af manglende dækning, henvise til udstedende pengeinstitut. Indløser må ikke udlevere informationer om kortholder til forretningen. Det er kortudsteder, der vurderer om information kan/må videregives.

Kortudsteder kan anvende en serviceleverandør til at udføre udsteders opgaver i forbindelse med indsigelser/tilbageførsler og til rådgivning om regler og processer.

Kortindløsers opgaver/ansvar

Kortindløser varetager forretningernes interesser i forbindelse med indsigelser, og har det fulde ansvar over for denne. Det vil sige:

- kontakt til, og kommunikationen med forretningen
- vurdering af indsigelserne
- vurdering af forretningens ansvar
- evt. træk på forretningens konto
- kreditering af kortudsteder

- bestilling af nota hos forretningen.

Kortindløser skal endvidere besvare spørgsmål fra udstedere vedrørende indsigelsessager, som udsteder har indsendt. Til dette formål skal kortindløser stille en webformular til rådighed på sin hjemmeside.

Dankort schemes opgaver/ansvar

Dankort scheme vedligeholder regler for indsigelser og tilbageførsler. Gældende regler fremgår af nærværende schemeregler, som er tilgængelige på https://infonet.nets.eu.

Dankort scheme skal besvare spørgsmål fra indløser og udsteder (herunder udsteders evt. serviceleverandør) til Dankorts regler for indsigelser og tilbageførsler.

Dankort scheme behandler alene indsigelsessager, men hvis der i forbindelse med en sag opstår tvist mellem indløser og udsteder. I så fald skal udsteder eskalere til scheme, som træffer afgørelse.

Henvendelser til Dankort scheme sker til dankortscheme@nets.eu.

Modtagelse og behandling af indsigelser

Nets Clara giver kortudsteder adgang til at se Dankort-transaktioner, samt indsende misbrugsrapportering, indsigelser og notarekvisitioner. Indsigelser og notarekvisitioner kan alternativt indsendes via blanket DK203.

Når kortudsteder anvender portalen

Adgang til portalen sker i henhold til kortudsteders egne forretningsgange. Følg nedenstående trin i forbindelse med en indsigelse:

Trin	Handling
1.	På portalen indtastes kortoplysninger og periode. Herefter vises en liste over kortets transaktioner i den valgte periode.
2.	Kortudsteder vælger de transaktioner, som efter kortudsteders vurdering skal tilbageføres.
3.	Årsag til indsigelse vælges.
4.	Systemet validerer i forhold til de gældende regler, og giver svar tilbage om, hvorvidt tilbageførsel er mulig. Webportalen viser en liste over de transaktioner, som er omfattet af indsigelsen.
5.	Hvis det maksimale beløb som angivet i skærmbilledet skal returneres, skal kortudsteder ikke foretage yderligere. Hvis et mindre beløb skal returneres, skal kortudsteder indtaste det beløb, der ønskes returneret.
6.	Webportalen viser en liste over de transaktioner, som kan tilbageføres.
7.	Der oprettes en sag i systemet.

	En kvittering på skærmen viser de transaktioner, der tilbageføres, og som vil blive krediteret kortudsteder. Kvitteringen er en liste over de transaktioner, der er tilbageført, og som vil blive krediteret kortudsteder. Det unikke sagsnummer fremgår af kvitteringen til kortudsteder. Kortudsteder kan vælge at udskrive kvitteringen. For status på sagen i øvrigt kan kortudsteder søge på kortnummer eller sagsnummer i systemet.
8.	Eventuel dokumentation arkiveres hos kortudsteder. Normalt vil en sag herefter være afsluttet for kortudsteders vedkommende.

Spørgsmål ved anvendelse af portalen kan rettes til Nets via www.nets.eu.

Når kortudsteder anvender blanketten

Hvis kortudsteder ikke anvender webportalen skal indsigelsesblanket DK203 benyttes. Blanketten findes på https://infonet.nets.eu. Indløser kan opkræve et gebyr pr. transaktion, når blanketløsning benyttes.

Når indløser modtager indsigelsen, sker følgende:

- Indløser indtaster indsigelsen i webportalen senest 10 bankdage efter modtagelsen.
- Indløser udskriver en liste over transaktionerne med angivelse af, hvorvidt de kan returneres eller ej
- Listen sendes til kortudsteder

Kreditering af indsigelsesbeløb

Indløser anvender faktureringssystemet FS i forbindelse med kreditering af Dankort-indsigelser. Kortudsteder vil sædvanligvis modtage kreditering via clearing 2 bankdage efter indtastning af indsigelsen i webportalen.

På kortudsteders konto vil fremgå en postering pr. kreditnota og en postering pr. faktura. Af posteringen vil fremgå det nummer på den faktura eller kreditnota, som indeholder specifikation af beløbet.

Gendebitering

Hvis forretningen gør indsigelse mod den foretagne tilbageførsel vil indløser behandle sagen på ny. Dette kan resultere i, at indløser fastholder tilbageførslen eller vurderer, at forretningens indsigelse er berettiget.

Hvis indløser vurderer, at forretningens indsigelse er berettiget (forretningen kan f.eks. komme med yderligere dokumentation), vil indløser gendebitere kortudsteders konto samt fremsende information herom til kortudsteder

Accepteres gendebiteringen af kortudsteder, er sagen slut. Hvis ikke det er tilfældet, kontakter udsteder indløser med anmodning om revurdering.

Ved fortsat uenighed mellem indløser og udsteder kan udsteder eskalere til Dankort scheme dan-kortscheme@nets.eu, som træffer endelig afgørelse. Henvendelse skal ske senest 45 kalenderdage efter gendebitering.

Advisering

Specifikationen (faktura eller kreditnota) indeholder en adviseringslinje pr. transaktion, som er tilbageført. Af adviseringsteksten fremgår kortnummer, sagsnummer og indsigelsesbeløb.

Hvilken konto anvendes til kreditering

Når en indsigelse er accepteret, vil indløser kreditere kortudsteders konto. Kortudsteder er ansvarlig for kreditering af kortholders konto.

Hvis kortudsteder benytter webportalen til indsendelse af indsigelser, kan kortudsteder vælge, hvilke konti, der skal benyttes til kreditering i forbindelse med indsigelser.

Kortudsteder har mulighed for at vælge konto afhængig af årsag til tilbageførsel:

- Konto til brug for kreditering som følge af manglende dækning (overtræk på kortholders konto).
- Konto til brug for kreditering som følge af øvrige indsigelser (tredjemandsmisbrug mv.).

Kontoen kan være på h-reg. niveau (f.eks. ved centraliseret behandling af indsigelser) eller på filialniveau.

Kortudsteder vælger i forbindelse med opsætning af adgange til webportalen, hvilke brugere der har adgang til at oprette og ændre kontonumre.

Hvis kortudsteder ikke benytter webportalen til indsendelse af indsigelser, kan kortudsteder ikke vælge krediteringskonto. Indløser vil benytte kortudsteders sædvanlige Dankort-kontonummer, som er registreret i FS.

Indsigelsesblanket/rekvisition af nota Dankort

A.

Dato:

Reg. nr.

Kortudsteders navn:

Kontaktperson hos udsteder:

Adresse:

Postnummer og by:

Direkte tlf. nummer:

E-mail:

B. Udfyld enten kortnummer eller Pan ID:

Kortnummer (16 cifre)

Pan ID (op til 32 cifre)

C. Henvendelsen vedrører følgende transaktioner:

Forretningsnummer	Ordre/nota nummer	Købsdato	Notabeløb (kr.)	Indsigelsesbeløb (kr.)

D. Indsigelsesårsag – kun ét kryds

- ☐ Varen/ydelsen ikke leveret (fjernsalg hvor transaktion ikke længere findes i Clara)
- ☐ Serietransaktioner*
- ☐ Notabestilling
- ☐ Manglende dækning (KUN ved Clara driftsproblemer)**
- ☐ Beløb ikke udbetalt i ATM ***

* *Ved serietransaktioner, hvor der er tale om 3.mands misbrug, skal kortholders tro & love erklæring medsendes.*
** *Ved manglende dækning skal sagen modtages hos indløser (Nets) senest klokken 12:00 på dagen for tilbageførsel for at være rettidig.*
*** *Ikke relevant for transaktioner, der er omfattet af den bilaterale aftale, pengeinstitutterne har indgået i Finans Danmark.*

E. Underskrift og stempel fra kortudsteder

Kortudsteder indestår for at der ved manglende dækning, ikke er dækning for beløbet når transaktionen posteres på kortholders konto.

Dato

Kortudsteders underskrift og stempel

Blanket indsendes via vores kontaktformular på www.nets.eu/kontakt
DK203

Bohemian, Version DK 06.2023

B.X.6 Card parameters and features
Updated: 31.01.2023

Table of contents

1 Change log

Version	Change	Author
31.01.2023	Changed name of document to be more generic. Added section 2.4 and preface in 3 regarding virtual cards. Added header 2.2 for information on physical Visa/Dankort Changed version requirements (with italics): "EMV 2011 version 4.3 *with subsequent bulletins* and. The card must be approved by Visa according to minimum VIS 1.6.*3* (VISA Integrated Circuit Card Specification) and VCPS 2.2.*4*"	ejurg
31.01.2022	Referenced version numbers of Visa and Mastercard chip specifications made "minimum" to allow for future versions.	ejurg

	Changes to document formatting and headings. Added table of contents and change log. Parameters for Visa and Mastercard side of co-badged cards are not referred to as requirements, but as examples. Removed obsolete references to previously issued cards. Removed option to issue cards with old (short) keys. Consolidation of AUC-tables for Dankort, Visa/Dankort and Mastercard Dankort. Entire document translated to English. Language order changed to "da-en-sv-no" to match how current applications are configured.	

2 General requirements

If the card is co-badged, then the Dankort application (AID) must not have a lower priority than the card's other applications unless the cardholder specifically has requested this.

The Dankort application must not share data elements with other applications unless the Dankort rules in this document and the other payment network's rules allow them to have the same value.

2.1 Physical Dankort

For a physical Dankort, one application with two interfaces (contact, CT, and contactless, CTL) must be implemented on the chip:

- Dankort application, A000000121 1010

2.2 Physical Visa/Dankort

For a physical Visa/Dankort, two applications, each with two interfaces (contact, CT and contactless, CTL), must be implemented on the chip:

- a Visa application, e.g. A000000003 1010
- a Dankort application, A000000121 4711

Solutions, where this is one application that can be used via the two AIDs, are allowed.

Data such as card number, transaction counter and offline accumulators of amount and transactions can be shared between the applications.

The chip must conform to EMV 2011 version 4.3 with subsequent bulletins. The card must be approved by Visa according to minimum VIS 1.6.3 (VISA Integrated Circuit Card Specification) and VCPS 2.2.4.

2.3 Physical Mastercard Dankort

For a physical Mastercard Dankort, two applications, each with two interfaces (contact, CT and contactless, CTL), must be implemented on the chip:

- a Mastercard application, e.g. A000000004 1010
- a Dankort application, A000000121 4713

The card numbers may be different for the two applications, e.g. 5019xxxx… for Dankort and 5xxxxxxx… for Mastercard.

Data such as card number, transaction counter and offline accumulators of amount and transactions can be shared between the applications.

The chip must conform to EMV 2011 version 4.3 (minimum). The card must be approved by Mastercard according to M/Chip Advance 1.2.x (minimum).

2.4 Virtual Dankort (all types)

For a virtual Dankort (a card virtualised to a mobile device using tokenisation) the following application must be used for the Dankort part, independently of whether the card is co-badged or not:

- a Dankort application, A000000121 4712

3 Card parameters

The following parameters are for physical cards only. Parameters for virtual cards are available in a separate document on request.

3.1 Functional chip requirements

Function	Implementation	Description
	Generation 4	
General chip setup		
Application Selection (CT)	PSE	
Application Selection (CTL)	PPSE	
Language list	da-en-sv-no	Default language preference. Issuer may choose another order.
Chip Application type	VIS 1.6.2 (min) / M/Chip Advance 1.2.x (min)	
Service Code	201	International usage, unrestricted
CVM methods: (only for CT)		
Priority 1	Online PIN if unatt. Cash / Fail	
Priority 2	Online PIN if Cashback / Go Next	
Priority 3	Enciphered offline PIN if Cashback. / Go next	
Priority 4	Plaintext offline PIN if Cashback / Fail	
Priority 5	Enciphered offline PIN if supported. / Go next	

Priority 6	Plaintext offline PIN if supported / Go next	
Priority 7	Online PIN if supported / Go Next	
Priority 8	Signature if supported / Fail	
Priority 9	No CVM if supported / Fail CVM	

Function	**Implementation**	**Description**
	Generation 4	
CAM	DDA and CDA(CT) / fDDA(CTL)	Dankort and Visa/Dankort
	DDA and CDA(CT) / CDA(CTL)	Mastercard Dankort
Offline Risk Management		
Terminal Risk Management	For CT: The terminal executes Floor limit check and Random transaction selection. The card executes velocity checking. For CTL: The terminal executes Floor limit check and CVM limit check. The card executes velocity checking.	The card executes Card Risk Management. For CTL it is Upper Limit.
Currency table	DKK/EUR-SEK-NOK-GBP-USD	Visa/Dankort and Mastercard Dankort, known currencies
	DKK/DKK	Dankort, known currencies
Consecutive Transaction Counter Limit CTCL	0	Above this limit the card will try to send the transaction online
Consecutive Transaction Counter Upper Limit CTCUL	15	Above this limit the card will require the transaction to be sent online
Consecutive Transaction Counter International Limit CTCIL	0	Above this limit the card will try to send the transaction online (unknown currencies)
Consecutive Transaction International Upper Limit CTIUL	0	Above this limit the card will require the transaction to be sent online (unknown currencies)
Cumulative Total Transaction Amount Limit CTTAL	0	Above this limit the card will try to send the transaction online
Cumulative Total Transaction Amount Upper Limit CTTAUL	20.000	Above this limit the card will require the transaction to be sent online

Funktion	**Dankort and Visa/Dankort implementation**	**Note**
	Generation 4	
Accumulated amount limit - VLP Funds Limit	800	Card must go online (CTL) when the accumulated amount exceeds this limit
Offline PIN try limit	3	
PIN Action if above offline try limit	Go online / if not possible decline	

Issuer-to-Card script processing	Optional (CT)	

3.2 Dankort - Application Usage Control (AUC)

These card parameters tell the terminal which types of transactions the card may perform (code 1 = Yes, 0= No).

Service	**Dankort and Visa/Dankort**		**Mastercard Dankort**	
	CT	CTL	CT	CTL
Valid for domestic cash transactions	1	1	1	1
Valid for international cash transactions	1	1	1	1
Valid for domestic goods	1	n/a	1	1
Valid for international goods	1	n/a	1	1
Valid for domestic services	1	n/a	1	1
Valid for international services	1	n/a	1	1
Valid for ATMs	1	n/a	1	1
Valid for terminals other than ATMs	1	n/a	1	1
Domestic cashback allowed	1	1	1	1
International cashback allowed	1	1	1	1

3.3 Data elements in ARQC/AAC/TC

Input data for validation by the processing system.

Data elements in ARQC/AAC/TC	**Dankort and Visa/Dankort**		**Mastercard Dankort**	
	Data from terminal	Data from card	Data from terminal	Data from card
Amount, Authorised (numeric)	X		X	
Amount Other (numeric)	X		X	
Terminal Country Code	X		X	
Terminal Verification Results	X		X	
Transaction Currency Code	X		X	
Transaction Date	X		X	
Transaction Type	X		X	
Unpredictable Number	X		X	
Application Interchange Profile		X		X
Application Transaction Counter		X		X
Card Verification Results		X		X
Issuer Application Data		X		X
Last Online ATC		n/a		X

3.4 Issuer Action Codes (IAC)

Each condition (bit) has the following possible codes:

- Ignore Denial=0, Online =0, Default=0
- Try online Denial=0, Online =1, Default=0
- Require online Denial=0, Online =1, Default=1
- Decline Denial=1, Online =0, Default=0

Card Verification Results, CVR: Internal card register which stores information about a transaction risk assessment.

Issuer Action Codes, IAC: Card parameters that sets the issuer's preferences with regard to offline transactions and sending transactions online after the terminal has made risk assessment.

Card Verification Results (CVR)	**Issuer Action Codes (IAC)**	**Note**
	Generation 4	
Data Authentication was not performed	Require online	
ICC Data missing	Require online	
Card appears on terminal exception file	Require online	Terminals do not have exception files
DDA failed	Require online	Terminal could not determine card authenticity
CDA failed	Require online	Terminal could not determine card authenticity
Chip card and terminal have different application versions	Ignore	
Expired application	Require online	
Requested service not allowed for card product	Require online	
New card	Ignore	Card will automatically go online at first use
Transaction exceeds floor limit	Require online	
Lower consecutive offline limit exceeded	Ignore	
Upper consecutive offline limit exceeded	Ignore	
Transaction selected randomly for online processing	Try online	
Merchant forced transaction online	Try online	Determined by merchant as it is per merchant request
Default TDOL used	Ignore	Default TDOL not used
Issuer authentication was unsuccessful	Ignore	Not necessary since the card will request ARPC in CDOL2 ('9108') and will fail if the ARPC cannot be verified (with the exception of 8 x 00h which means that there was no ARPC from the host, which will cause an approved transaction since the card is configured for "partial grade").

Script processing failed before final Generate AC	Ignore	Script is no longer critical for current transaction
Script processing failed after final Generate AC	Ignore	Script is no longer critical for current transaction

3.5 Dankort Public Key

Dankort PROD	**CA_{PK} Index 3 - 1984 bit**
Key ID	SIGRSAP1.CADK.5019.P1984003
RID	A000000121
Service Identifier	10100000
CA Public Key Index	3
Expiration (YYMM)	1228
CA Public Key Modulus	B8 26 DC A2 1E 3F 79 1D D8 A1 62 AC 1B 55 14 31 38 2A C1 BB C1 B0 15 B4 30 8C 2A A6 D5 4E 66 BC 38 5E DD C8 D5 B8 7F 08 0C 56 2F 8D 2D 8F DB 13 EA 16 8F EE 1A 7A E0 23 4B C4 CC 10 53 5B 81 FF 68 97 4A 9D 12 CA C2 AE 64 AB 8C EF F1 DD FB 44 3A F4 31 AC E3 DB B8 17 E4 59 52 47 29 87 87 23 9C DF 5B E4 1E AB A4 7D C2 65 A9 DD 56 63 0C F6 E3 EA 4A 8C C3 9D A3 84 A7 73 47 36 BB 97 C7 0F 7E 9A D8 FA 35 36 4E 99 F9 71 E7 D9 5C 49 1C A2 7C CC E8 1A A8 DD ED 01 14 02 B1 4F 66 45 A7 52 8F CE 55 69 4E 1C 63 59 BE 66 CC 73 04 7C EF 53 C9 E7 B5 29 D5 37 BD 42 E3 E7 02 8D 9B 68 8B 59 26 97 6E 4F FA DF 26 BA E1 CA 50 21 FA 40 F7 DD 02 38 7D F0 2E D6 8C B0 07 40 DA 3B DC CC F5 48 72 E6 E4 3D 24 60 EC 56 34 1F FC F3 07 63 A8 C7 AD C7 77 C9 BB 77 19 55
CA Public Key Exponent	3
CA Public Key Check Sum (SHA-1 Hash)	CE EA 8B 63 58 5F 25 60 00 91 F5 D8 F1 22 A1 71 9F F0 B1 32

D.X.1 Terminal parameters and features

Updated: 31.01.2024

This appendix specifies how the terminal should handle the Dankort application on the card, e.g. on a Visa/Dankort or a Mastercard Dankort. The handling of Visa and Mastercard applications is out of scope of this document. Please refer to the scheme rules from Visa and Mastercard.

Table of contents

1 Revision history

Version	Section	Change	Author
31.01.2024	7	Removed "in effect" date, since date is passed	ejurg
	7.2	Added a single tap alternative method of offering cardholder application selection	ejurg
31.08.2023	2.1.1	Update of table with listing of device types and AIDs	ejurg
	3 and 4	BIN lists replaced with a reference to BIN lists on the TRG portal	ejurg
	3.1	Added that Mastercard Dankort cannot be used for Dankort magstripe transactions	ejurg
28.04.2023	2.1.2 and 5.1.2	Prod key with idx 1 removed (expired). Expiry for key with idx 2 changed 2023-12-31 -> 2024-12-31, and key with idx 3 changed 2030-12-31 -> 2031-12-31.	ejurg
	6.1	Removed paragraph regarding double tap for mobile payments, not relevant any more.	ejurg
31.01.2023	2.1.1 and 2.2.x	AID x4712 also used by single badge Dankort and for cards (i.e. non-mobile). Added section 2.2.2 with parameters for this AID.	ejurg
	2.3.2	Added application version (03 00)	ejurg
	6.1	Removed table 1 in section 6.1 (specific to ISO and is documented in that spec), incl. references	ejurg
	7	Added new section with requirements for contactless application selection	ejurg
31.03.2022	2.3.2	TAC – Denial, TAC – Online and TAC – Default for AID 4712 were incorrectly specified. Corrected values are set to match other AIDs.	ejurg
31.01.2022		Add revision history Add table of contents Modify introductory text	ejurg
		Correct "CA Public Key Check Sum" for test key with index 6	tjhan
		Remove section in "Strong Customer Authentication (SCA) Request" about "new SCA rules" (the rules are no longer new) Remove "Action when cashback" and "Action when manual cash" from contact (special rules no longer relevant)	ejurg

2 Chip-based Transactions

2.1 Common Data for Contact and Contactless Transactions

2.1.1 Application Identifiers (AIDs)

A terminal accepting contact and contactless chip transactions for Dankort must support the following AIDs:

- A000000121 1010
- A000000121 4711
- A000000121 4712
- A000000121 4713

Device type	Interface	Card Product		
		Dankort	Visa/Dankort	Mastercard Dankort
Physical card	Contact and Contactless	A000000121 1010 A000000121 4712	A000000121 4711 A000000121 4712	A000000121 4713
Mobile	Contactless	A000000121 4712	A000000121 4712	A000000121 4712

Parameters and functionality defined per AID is given below.

2.1.2 Certification Authority Public Keys (CA Public Keys)

An offline-capable terminal must support the following CA Public Keys:

Environment	CAPK Index	Key length	Expiry Date	Remarks
TEST	3	1152	Expiration of CA Public Keys not enforced in the TEST environment	
	4	1152		
	5	1408		
	6	1984		
PROD				
	2	1408	2024-12-31	May be extended
	3	1986	2031-12-31	May be extended

Key values are listed in section 5.

2.2 Contact Transactions

2.2.1 Miscellaneous (AID = A000000121 1010 and A000000121 4711)

AID	Parameter	Value	Remarks
A000000121 1010 -OR- A000000121 4711	General		
	Application Version	00 8C (or higher)	140 decimal (VIS 1.4.0)
	Default DDOL	9F3704	
	Terminal Action Codes		
	TAC – Denial	00 10 00 00 00	See section 5.2
	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	
	Limits		
	Floor Limit	DKK 0.00	
	Transaction limit	DKK 100,000.00	
	Random Transaction Selection		

	Threshold Value for Biased Random	DKK 0.00	
	Target Percentage for Random Selection	0	
	Maximum Target Percentage for Random Selection	0	
	Special Transactions		
	Action when fallback	Online	

2.2.2 Miscellaneous (AID = A000000121 4712)

AID	Parameter	Value	Remarks
A000000121 4712	General		
	Application Version	03 00	
	Default DDOL	9F3704	
	Terminal Action Codes		
	TAC – Denial	00 10 00 00 00	See section 5.2
	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	
	Limits		
	Floor Limit	DKK 0.00	
	Transaction limit	DKK 100,000.00	
	Random Transaction Selection		
	Threshold Value for Biased Random	DKK 0.00	
	Target Percentage for Random Selection	0	
	Maximum Target Percentage for Random Selection	0	
	Special Transactions		
	Action when fallback	Online	

2.2.3 Miscellaneous (AID = A000000121 4713)

AID	Parameter	Value	Remarks
A000000121 4713	General		
	Application Version	00 02	
	Default DDOL	9F3704	
	Terminal Action Codes		
	TAC – Denial	00 10 00 00 00	See section 5.2

	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	
	Limits		
	Floor Limit	DKK 0.00	
	Transaction limit	DKK 100,000.00	
	Random Transaction Selection		
	Threshold Value for Biased Random	DKK 0.00	
	Target Percentage for Random Selection	0	
	Maximum Target Per-centage for Random Selection	0	
	Special Transactions		
	Action when fallback	Online	

2.3 Contactless Transactions

2.3.1 Miscellaneous (AID = A000000121 1010 and A000000121 4711)

AID	Parameter	Value	Remarks
A000000121 1010 -OR- A000000121 4711	General		
	Application Version	00 8C (or higher)	140 decimal (VIS 1.4.0)
	Default Kernel ID	03	
	Default TTQ	36 20 40 00	Certain positions depend on the actual terminal type
	Limits		
	Floor Limit	DKK 0.00	
	CVM Limit	DKK 350.00	
	Transaction limit	DKK 100,000.00	
	Late Amount Transactions		
	Action at decreased amount	Online	Amount confirmation optional
	Action at increased amount	Online + Confirm	
	Dynamic Currency Conversion (DCC)	Not allowed	

2.3.2 Miscellaneous (AID = A000000121 4712)

AID	Parameter	Value	Remarks
A000000121 4712	General		
	Application Version	03 00	

	Default Kernel ID	05	
	Terminal Action Codes		
	TAC – Denial	00 10 00 00 00	See section 5.2
	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	
	Limits		
	Floor Limit	DKK 0.00	
	CVM Limit	DKK 350.00	
	Transaction limit	DKK 100,000.00	
	Late Amount Transactions		
	Action at decreased amount	Online	Amount confirmation optional
	Action at increased amount	Online + Confirm	
	Dynamic Currency Conversion (DCC)	Not allowed	

2.3.3 Miscellaneous (AID = A000000121 4713)

AID	Parameter	Value	Remarks
A000000121 4713	General		
	Application Version	00 02	
	Default Kernel ID	02	
	Terminal Action Codes		
	TAC – Denial	00 10 00 00 00	See section 5.2
	TAC – Online	FC 40 BC F8 00	
	TAC - Default	FC 40 A4 A8 00	
	Limits		
	Floor Limit	DKK 0.00	
	CVM Limit	DKK 350.00	
	Transaction limit	DKK 100,000.00	
	Late Amount Transactions		
	Action at decreased amount	Online	Amount confirmation optional
	Action at increased amount	Online + Confirm	
	Dynamic Currency Conversion (DCC)	Not allowed	

3 Magnetic Stripe Transactions

3.1 Magnetic Stripe Lay-out

The following table shows the structure of the magnetic stripe track 2 for Dankort and Visa/Dankort (Start Sentinel, End Sentinel and LRC check character have been omitted). Mastercard Dankort cannot be used for Dankort magstripe transactions.

Position i track 2	Dankort	Visa/Dankort	Remarks
1	'5'	'4'	PAN:Primary Account Number 16 digits
2	'0'	'5'	
3	'1'	'7'	
4	'9'	'1'	
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17	Separator	Separator	
18			4 digits in YYMM
19	Expirydate	Expirydate	
20			
21			
22			3 digits: 601 for Dankort 201 for Visa/Dankort
23	Servicecode	Servicecode	
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			

34			
35	'Korttype'	'Korttype'	2 digit code which may be used in supplementary control of the card
36	'50' - '54'	'40' - '44'	
37			

4 Dankort BIN lists

Dankort BIN lists are available on Nets TRG Portal. To obtain access to the portal, contact trg-portal@nets.eu. The portal will automatically send notifications on updates. Consider registering with a department email, so that notifications are not disrupted by staff changes.

5 Detailed Data Elements

5.1 CA Public Keys

5.1.1 CA Public Keys – TEST Environment

Dankort TEST	CAPK Index 03 - 1152 bit
RID	A000000121
CA Public Key Index	03
CA Public Key Modulus	D5 6A 6C 70 74 82 4A 5A 62 8C 66 33 B1 F1 55 34 44 6D F7 79 06 57 86 75 EE 4D 7A 58 B8 D2 8A 3A 0C 0C 9B CF 04 18 A3 55 B5 54 57 73 2C 0A 52 4E AB 27 2A D1 82 A1 BE B9 46 0D D1 71 3F 9E A5 0E 3E 5C E9 1C 60 AD B0 33 CF 4A D3 20 DD 7D 33 64 97 18 F9 40 D2 04 5B BA 05 0A 93 56 A8 F6 31 C7 95 93 86 75 21 00 4B 55 5D 3B EA B9 36 47 D1 3E 56 84 11 91 4F F7 77 73 45 93 43 8D D1 71 10 8F 74 E4 94 D8 68 1C 93 59 6E 1D 10 11 F0 60 2A 1F
CA Public Key Exponent	3
CA Public Key Check Sum (SHA-1 Hash)	A5 14 6E 81 C8 97 A8 79 40 72 89 F3 2B 00 BD 24 66 8F 20 FF

Dankort TEST	CAPK Index 04 - 1152 bit
RID	A000000121
CA Public Key Index	04
CA Public Key Modulus	A0 1B 29 51 D3 5D A5 83 47 54 CD DD 2C AE 9A 29 96 C9 DA 0A 4D C4 14 B6 D9 CE 90 AC AD 6E 03 2C BD F9 4F 6F 17 DC FA 38 F0 3E 52 49 36 C8 42 8D 6D F5 39 D7 11 4A F1 F6 DA CB A0 84 07 BB 9A BC 4F 96 81 AB B6 93 1F DF E9 FB 71 9A 28 B0 11 1E 69 03 C0 35 1F 2B 50 09 BB F8 EA EE FE 84 8B E8 1F 6A 3C AC 76 D1 F5 B5 3C DE 2B ED 98 D6 6C DB D6 5E 32 78 78 08 36 22 85 27 7E CC 38 2E 6F 7A 26 FB 90 77 3D D5 7E 1F 36 A1 21 4B E9 F0 E6 E3
CA Public Key Exponent	3

CA Public Key Check Sum (SHA-1 Hash)	53 8E 24 72 41 3E BE 6A 49 BB 25 D2 CC 1F E5 55 7A 00 DF CF

Dankort TEST	CAPK Index 05 – 1408 bit
RID	A000000121
CA Public Key Index	05
CA Public Key Modulus	BB 18 15 B0 73 A2 83 DC B8 66 D5 37 3D 35 FF 46 B6 A0 D5 6A 09 EE 97 B8 B0 2D 13 3E 03 87 B1 B1 B5 3C DC 64 3F 4B 5F 60 1B 97 3B 6E C8 2F C9 3C ED C2 7A DC B0 7F 56 20 89 44 52 6B DA 21 7E FC B0 9D C1 09 7A B2 0C 0E 76 18 FC DE E5 2D 24 29 F4 CE 74 84 51 D7 CB 43 7C 1D A5 A9 D9 25 81 09 BD 58 1D B1 4B 21 C4 EE 02 9C 03 1F 68 9B D5 30 55 9C 10 6F 98 85 77 1C DC EB E0 21 5B 16 A6 90 FA 16 6B BA 42 EC 37 8F 4E 74 2B 97 42 CB 0F 2D 4D 6A EC 86 28 0C 79 A0 B0 EE CF 76 74 BC 93 E1 57 83 C9 4F 1E 13 33 7A 93 15 B4 30 FE 5A 8C 43
CA Public Key Exponent	3
CA Public Key Check Sum (SHA-1 Hash)	CC 44 C0 74 74 8B CD 88 64 53 CE C8 DF EC CA 0B AD 27 56 85

Dankort TEST	CAPK Index 06 – 1984 bit
RID	A000000121
CA Public Key Index	06
CA Public Key Modulus	C5 C3 E0 0F E0 96 D3 96 16 E2 CB 39 E9 DB E4 59 FF F1 DF F1 A3 33 DD 37 4B 3F D2 35 1D 49 77 32 8B 8B 14 F1 13 EC B0 65 04 0A 2A CC 28 F2 C4 D1 95 0D 11 4C 4F C3 59 0E C2 F9 33 CE 5C 35 09 AC 0D C7 B2 3F 90 9F C6 38 FA B3 A1 18 3B A6 B7 FD EC 73 14 24 77 D5 3E 42 23 3C 35 D8 2B F7 A4 B5 34 12 E2 50 CF 40 00 28 CB 0F A3 C8 EF E5 E7 3E 46 56 D1 D6 B6 97 E8 C7 B8 05 11 23 56 C3 B4 74 B1 E4 BD 1F 61 4F 03 66 96 84 2A AD C1 51 E3 D5 74 36 47 74 90 23 A3 D8 CF 31 67 6B 2F A1 D4 E0 12 27 E9 4B 7B 92 6C 50 67 36 BD 2A 36 60 48 B1 6E 8D 9B F6 CC 10 CD 03 E1 8B D7 BD CD D0 EC E8 79 38 AD 52 86 28 A9 4F 15 CD 22 F5 37 C1 13 CA 86 6C 19 91 6D 06 4F 2F 4C 3F 62 33 F4 5A 47 D1 5A 55 A6 8F 33 63 22 5E 9D 25 E9 CB 31 D6 43 98 DE BC 16 27 1B 4F 78 E7
CA Public Key Exponent	3
CA Public Key Check Sum (SHA-1 Hash)	BE 32 F4 25 B7 10 78 B7 D3 2D 54 AF CD 02 67 79 14 BC 43 46

5.1.2 CA Public Keys – PRODUCTION Environment

Dankort PROD	CAPK Index 2 - 1408 bit
RID	A000000121
CA Public Key Index	2
CA Public Key Modulus	B1 56 42 E4 6D E9 33 C7 7B 11 A6 CF 9C 10 F1 74 2A BF 20 5B 78 C4 A3 32 E2 04 AB 77 33 48 1B 0D 2A 6E 20 D8 2B 16 F9 26 81 25 C5 6D 85 DB A2 54 7C D3 F4 6E FC 9C 4E 92 3F 35 7A 12 0B A8 F0 17 99 46 74 89 D7 13 35 C6 94 E5 01 3D 36 A0 67 24 C6 58 01 A9 EE 35 BB F3 E6 F7 68 7C 13 B2 40 32 E4 CD 75 A4 C1 84 D5 75 CA 98 86 96 65 19 DB A8 F2 01 5D 2F 80 92 ED 65 C5 04 03 09 6B 88 4A B6 57 6E 6C E5 7D F5 4F 97 F0 79 B2 DF 37 55 AF 84 85 C7 E4 C5 75 10 A3 C7 5C AF 98 AD E5 25 62 5C A7 F1 5F 26 17 DC 17 33 D3 01 BC 73 A1 EC 4B 33
CA Public Key Exponent	3
CA Public Key Check Sum (SHA-1 Hash)	95 94 57 1F 85 11 55 D8 92 22 F4 E1 DE 02 EA D4 84 C4 D4 BC

Dankort PROD	CAPK Index 3 - 1984 bit
RID	A000000121
CA Public Key Index	3
CA Public Key Modulus	B8 26 DC A2 1E 3F 79 1D D8 A1 62 AC 1B 55 14 31 38 2A C1 BB C1 B0 15 B4 30 8C 2A A6 D5 4E 66 BC 38 5E DD C8 D5 B8 7F 08 0C 56 2F 8D 2D 8F DB 13 EA 16 8F EE 1A 7A E0 23 4B C4 CC 10 53 5B 81 FF 68 97 4A 9D 12 CA C2 AE 64 AB 8C EF F1 DD FB 44 3A F4 31 AC E3 DB B8 17 E4 59 52 47 29 87 87 23 9C DF 5B E4 1E AB A4 7D C2 65 A9 DD 56 63 0C F6 E3 EA 4A 8C C3 9D A3 84 A7 73 47 36 BB 97 C7 0F 7E 9A D8 FA 35 36 4E 99 F9 71 E7 D9 5C 49 1C A2 7C CC E8 1A A8 DD ED 01 14 02 B1 4F 66 45 A7 52 8F CE 55 69 4E 1C 63 59 BE 66 CC 73 04 7C EF 53 C9 E7 B5 29 D5 37 BD 42 E3 E7 02 8D 9B 68 8B 59 26 97 6E 4F FA DF 26 BA E1 CA 50 21 FA 40 F7 DD 02 38 7D F0 2E D6 8C B0 07 40 DA 3B DC CC F5 48 72 E6 E4 3D 24 60 EC 56 34 1F FC F3 07 63 A8 C7 AD C7 77 C9 BB 77 19 55
CA Public Key Exponent	3
CA Public Key Check Sum (SHA-1 Hash)	CE EA 8B 63 58 5F 25 60 00 91 F5 D8 F1 22 A1 71 9F F0 B1 32

5.2 Dankort Terminal Action Codes (TAC)

Byte	Bit	Meaning	TAC-Denial	TAC-Online	TAC-Default
1	8	Offline data authentication was not performed	0	1	1
	7	Offline static data authentication (SDA) failed	0	1	1
	6	ICC data missing	0	1	1

Byte	Bit	Meaning	TAC-Denial	TAC-Online	TAC-Default
	5	Card appears on terminal exception file	0	1	1
	4	Offline dynamic data authentication (DDA) failed	0	1	1
	3	Combined DDA/AC Generation (CDA) failed	0	1	1
	2	Static data authentication (SDA) selected	0	0	0
	1	RFU	0	0	0
2	8	ICC and terminal have different application versions	0	0	0
	7	Expired application	0	1	1
	6	Application not yet effective	0	0	0
	5	Requested service not allowed for card product	1	0	0
	4	New card	0	0	0
	3…1	RFU	0	0	0
3	8	Cardholder verification was not successful	0	1	1
	7	Unrecognized CVM	0	0	0
	6	PIN Try Limit exceeded	0	1	1
	5	PIN entry req. and PIN pad not present or not working	0	1	0
	4	PIN entry req., PIN pad present, but PIN was not entered	0	1	0
	3	Online PIN entered	0	1	1
	2…1	RFU	0	0	0
4	8	Transaction exceeds floor limit	0	1	1
	7	Lower consecutive offline limit exceeded	0	1	0
	6	Upper consecutive offline limit exceeded	0	1	1
	5	Transaction selected randomly for online processing	0	1	0
	4	Merchant forced transaction online	0	1	1
	3…1	RFU	0	0	0
5	8	Default TDOL used	0	0	0
	7	Issuer authentication was unsuccessful	0	0	0
	6	Script processing failed before final GENERATE AC	0	0	0
	5	Script processing failed after final GENERATE AC	0	0	0
	4…1	RFU	0	0	0

6 Strong Customer Authentication (SCA) Request

6.1 General

Whether SCA is required or not for an online No CVM transaction is handled by the Nets host for physical cards and in the mobile device for wallets/apps.

If SCA is required, the terminal will (as usual) send an online No CVM Request to the Nets host. The host will return a specific code (Action Code) to the terminal/merchant i.e. SCA is required and this request is therefore declined by the host. A subsequent second request (with PIN) shall then be created using the existing transaction data (including PIN data etc.) according to the SCA requirements.

This will give the following changes in the payment flow:

For CAT terminals without PIN-pad, the terminal must:

- Abort the transaction and start a new transaction – and
- Prompt the customer to use another interface

For CAT-terminals with PIN-pad, the terminal must:

- Prompt the customer to enter PIN and
- Continue the transaction using the existing transaction data from the first transaction, meaning – the card must not be activated again (no new tap or use of the contact interface) and no re-entry of transaction amount is required.
- The existing data from the first transaction are resend to the host with the exception that this transaction is marked as a PIN transaction and includes PIN-data.

For merchant operated terminals (with PIN-pad), the terminal must:

- Prompt the customer to enter PIN and
- Continue the transaction using the existing transaction data from the first transaction, meaning – the card must not be activated again (no new tap or use of the contact interface) and no re-entry of transaction amount is required.
- The existing data from the first transaction are resend to the host with the exception that this transaction is marked as a PIN transaction and includes PIN-data.

For transactions based on use of wallet/apps there are no changes to the payment flow.

The specific impact on contactless transactions is that contactless PIN-retry is possible. In case of an incorrect online PIN during a contactless transaction, the customer is prompted to enter the PIN again (without starting a new transaction and presenting the contactless card again).

For Dankort contactless transactions, the issuer host checks the accumulated amount for No CVM transactions. When the accumulated amount limit is exceeded, the issuer host declines the transaction and sends a response code/Action Code requesting Strong Customer Authentication.

NOTE: The host may, in the future, maintain other counters/conditions that may inhibit/initiate Strong Customer Authentication.

Dankort supports a One-Tap SCA solution. It means that when the host declines the contactless card transaction as described above, the customer shall be prompted on the terminal display to enter the PIN. It shall in general *not* be necessary to present the card again and the same request data shall be resent, except for following updated fields:

- DE11: System Trace Audit Number (STAN)
- DE37: Retrieval Reference Number

and with the following data added to the request:

- DE52: PIN data present

6.2 Terminal Capabilities Indicator

A data element shall be conveyed to the host in *all* contactless requests (Purchase and Original Authorisations) indicating whether Strong Customer Authentication is supported or not for this terminal.

The internal ISO 8583 format will be as follow:

Terminal Capabilities Indicator

Purpose: Used to indicate the host whether the terminal supports e.g. SCA or not.

Format: b1 (1 byte).

Contents: See Table 1.

Remarks: The Terminal Capabilities Indicator may indicate "SCA not supported by the terminal" if the terminal does not support a PIN Entry Device. If the Terminal Capabilities Indicator is not present (e.g. for old terminals), it is interpreted by the host as "SCA not supported by the terminal". Tag C# is defined for this data element. Example: C# 0001 01.

Table 1 – Terminal Capabilities Indicator

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	Strong Customer Authentication (SCA):
-	-	-	-	-	-	-	0	- SCA *not* supported by the terminal
-	-	-	-	-	-	-	1	- SCA supported by the terminal
x	x	x	x	x	x	x	-	RFU
NOTE:								

6.3 SCA - Exceptions

Payment Service Providers shall be allowed *not* to apply to SCA for transport fares and parking fees. The host will differentiate using the Merchant Category Code (MCC).

7 Contactless application selection for co-badged cards

EU regulation requires that cardholders with co-badged cards have the option of selecting which application is used. The regulation also allows merchants to configure preferred payment networks (referred to as "Merchant preferred").

7.1 Merchant preferred

The terminal must allow the merchant to configure either "Dankort" as preferred, or "Domestic methods" or similar general term. Setting either must mean that the terminal selects one of the Dankort AIDs, unless the cardholder chooses to override the choice.

7.2 Cardholder selection

The terminal must offer the cardholder a way of enabling application selection mode prior to tapping the card. This could, for instance, be by pressing the yellow button on the terminal.

What the terminal must do after the card is tapped depends on whether application selection mode is enabled:

Application selection mode	**Step**	**Action**
Disabled	1	The cardholder taps card.
	2	The terminal must select merchant preferred application if set. If not set, the terminal selects application according to EMV rules.
Enabled	1	The terminal displays a list of payment networks that the merchant accepts. *OR*

		The cardholder taps card. The terminal displays a list of the applications on the card (using application labels, if available from the card).
	2	
	2	The cardholder selects an application/network.
	3	The cardholder taps card and the terminal uses the selected application/network.

Bilag D.X.2 CVC requirements for Dankort card-not-present payments

Updated: 31.12.2020

CARDH_PRESENT (pos 5)		POS-data code CARDDATA_INPUT_MODE (pos 7)						
		0	**1**	**6**	**8**	**K**	**L**	**R**
		Unspecified	**Manual, no terminal**	**Key entered**	**PAN entry eCom w. 3DS**	**PAN entry eCom, only SSL**	**PAN entry eCom, no security**	**PAN obtained by wallet**
0	**Cardholder present**					CVC req.	CVC req.	
2	**Cardholder not present, mail order**		CVC req.	CVC req.				
3	**Cardholder not present, telephone**		CVC req.	CVC req.				
4	**Standing order/recur-ring**							
K	**Subsequent trx for stored card**							
L	**First trx for stored card**				CVC req.	CVC req.	CVC req.	