BESTEMMELSER FOR SALG MOD BETALING MED KONTOKORT
I UBEMANDET TERMINAL
(Oktober 2015)

Disse bestemmelser, "Bestemmelser for ubemandet terminal", gælder ved salg mod betaling med Kontokort i ubemandede terminaler som parkeringsautomater, vareautomater og vejbetalingsautomater.

Bestemmelserne udgør et supplement til de Generelle betingelser om indløsning af kontokorttransaktioner , som er indgået mellem Salgsvirksomheden og Bambora. Ved eventuelle uoverensstemmelser mellem Hoveddokumentet og Bestemmelserne skal Bestemmelserne have forrang.

1. Typer af Terminaler til ubemandet miljø

Ved **Type 1** forstås Ubemandet terminal, hvor autorisation altid skal gennemføres 'online' uanset beløbets størrelse, og hvor verificering foretages med PIN-kode, f.eks. en vareautomat.

Ved **Type 2** forstås Ubemandet terminal, hvor autorisation altid skal gennemføres 'online' uanset beløbets størrelse, men som mangler mulighed for verificering med PIN-kode. Transaktioner via parkeringsautomater (MCC 7523) i dette miljø må ikke overstige 50,- EUR*. Transaktioner via vareautomater (se definition nedenfor) i dette miljø må ikke overstige 20,- EUR*. I øvrigt må transaktionsbeløbet aldrig overstige EUR 100,-*.
* Eller tilsvarende i lokal valuta.

Ved **Type 3** Denne løsning er kun tilladt for vejbetalingsautomater (MCC 4784). Hentyder til Ubemandet terminal, som kun er 'offline' og mangler mulighed for verificering med PIN-kode. Transaktioner i dette miljø må ikke overstige EUR 40,- og kortet skal kontrolleres i forhold til spærreliste.

For ubemandet benzinpumpe (MCC 5542) gælder særlige bestemmelser.

2. Chip- og Pin-terminaler

Terminaler, som anvendes til at gennemføre transaktioner med Kontokort, skal understøtte både magnetlæser og EMV-chipteknologi. MasterCard/VISA kan komme ud for at skulle påføre Bambora et gebyr i tilfælde af, at Salgsvirksomheden ikke overholder ovenstående. Salgsvirksomheden er i dette tilfælde iht. Hoveddokumentet forpligtet til at godtgøre Bambora sådanne gebyrer.

Fra og med 1. januar 2016 skal alle nyinstallerede terminaler, uanset type, hos salgsvirksomheder, der tidligere ikke har accepteret Kortbetalinger understøtte kontaktløse transaktioner også kaldet 'Contactless'. Dette gælder også salgsvirksomheder, der udskifter samtlige kortlæsere. Fra og med 1. januar 2020 skal samtlige terminaler understøtte kontaktløse transaktioner.

3. Kundekvittering

Kundekvittering skal altid udleveres og indeholde følgende informationer:

- Salgsvirksomhedens navn, by og CVR-nummer
- Dato

- Kontokortets nummer skal angives i trunkeret form dvs. (kun de (4) sidste cifre udskrives, indledende positioner trunkeres med '*')
- Beløb
- Oplysninger om moms
- Reference/søgenummer (unik identitet på Transaktionen).

4. Anvendelse af PIN

Hvis Terminalen håndterer PIN, skal kortindehaveren have tre (3) forsøg på at identificere sig ved hjælp af PIN-kode. Hvis der indtastes forkert PIN-kode tre (3) gange i træk, skal udstyret om muligt beholde kortet. Disse kort sendes ituklippet til den pågældende kortudsteder. Kortindehaveren skal have mulighed for at afbryde en transaktion i stedet for at foretage yderligere forsøg med en PIN-kode.

Hvis PIN ikke er tilladt for denne korttype, kan kortet ikke anvendes i selvbetjeningsudstyr med PIN-verificering.

Med transaktioner via vareautomater hentydes til varer og tjenester, som kan sælges ved en ubemandet terminal med undtagelse af:

- Parkeringspladser, parkeringsautomater og garage (MCC 7523)
- Vejbetalingsautomater (MCC 4784)
- Benzinpumper (MCC 5542)
- Alle varer og tjenester som iht. loven har en aldersgrænse ved salg (f.eks. spil, tobaksvarer og alkohol)
- Alle varer og tjenester, som iht. andre regler eller bestemmelser er underlagt visse restriktioner ved salg, og kræver en form for kunde- eller kortindehaververificering ved f.eks. lægemidler).

4. Transaktionsindsamling

Indsamling af købstransaktioner med Kontokort, hvorpå der ikke er præget navn og/eller nummer (f.eks. Kontokort med varemærkerne Maestro og Electron) må kun foregå i Terminal af Type 1 og for parkeringsautomater (MCC 7523) af Type 2.

5. Rapportering

5.1 Indsendelse af købstransaktioner
Elektronisk indsamlede købstransaktioner skal senest inden for to (2) dage fra betalingsdagen overføres til Bambora. Ved "betalingsdagen" forstås dagen for autorisationen.

5.2 Transaktionsjournal
Salgsvirksomheden skal føre en særlig journal over samtlige Transaktioner, hvor der er anvendt Kontokort, dvs. både gennemførte og afbrudte Transaktioner. Denne journal skal vise:

- På hvilken måde Transaktionen er gennemført,
- Salgsvirksomhedens navn (firma), by og CVR-nummer,
- dato og klokkeslæt,

- kontokortets nummer (forudsat, at Terminalen understøtter dette, skal ske i trunkeret form),
- transaktionstype (betaling eller returnering/kreditering) i klartekst,
- kasseidentitet,
- kontrolnummer som bevis på autorisation,
- beløb der skal debiteres,
- reference/søgenummer og
- svarkode.

5.3 Arkivering
Salgsvirksomheden skal i mindst (18) måneder arkivere Transaktionsjournalen iht. de gældende regler for PCI DSS (se punkt 6.1 nedenfor). På Bamboras anmodning skal Salgsvirksomheden inden for fem (5) dage fremlægge en kvittering vedrørende en enkelt Transaktion. Dette gælder også, hvis Salgsvirksomhedens indløsningsaftale med Bambora i øvrigt er ophørt.

6. Sikkerhed

6.1 Håndtering af kontokortinformationer
Med henblik på dels at bevare et højt sikkerhedsniveau i de globale kortbetalingssystemer, dels at styrke tilliden til Kontokort som betalingsmiddel, er det af yderste vigtighed, at alle, som håndterer Kontokortinformationer, gør det på en sikker måde. Med "Kontokortinformationer" forstås sådanne informationer, som er præget eller trykt på Kontokortets for- og bagside, inklusive informationer som er lagret i Kontokortets magnetspor og chip. Derfor har kortindustrien vedtaget en fælles standard for håndtering af Kontokortinformationer. Standarden kaldes Payment Card Industry (PCI) Data Security Standard (DSS) og er udviklet af de internationale kortnetværk Visa og MasterCard.

Salgsvirksomheden forpligter sig til at overholde standarden PCI DSS i den udformning, der til enhver tid er offentliggjort www.pcisecuritystandards.org.

6.2 Godkendelse af systemer
Terminaler, som leverer Transaktioner til Bambora, skal være godkendt af Bambora eller anden tredjepart, som Bambora anviser. Bambora kan stille krav til særlig kontrol af komponenter, der er følsomme ud fra et sikkerhedsmæssigt synspunkt.

6.3 Specielt vedrørende såkaldte Nodes og Payment Service Providers
Hvis Salgsvirksomheden anvender en tredjepart (såkaldt node eller Service Provider) som en del af sin betalingsløsning til håndtering af Transaktioner, skal Salgsvirksomheden sikre, at denne opfylder alle krav iht. PCI DSS.

6.4 Ændring i udstyr m.m.
Salgsvirksomheden skal informere Bambora om enhver form for installation, flytning eller afvikling af udstyr, som er teknisk tilsluttet til Bambora eller en anden indsamler af Transaktioner, der arbejder efter ordre fra Salgsvirksomheden inden for rammerne af denne aftale.

Ændringer i Terminaler, som påvirker de gældende forudsætninger på tidspunktet for godkendelsen, må ikke gennemføres uden Bamboras godkendelse.

Salgsvirksomheden skal, inden Transaktioner må overføres til Bambora, gennemføre en af Bambora anvist test af opkoblingen til Bamboras modtagelsessystem.

6.5 Særligt om kassesystemer med integreret kortlæser/Sikkerhedsanvisninger
Salgsvirksomheder, som anvender kassesystemer med integrerede kortlæsere, skal også sikre, at de af Bambora til enhver tid separat meddelte Sikkerhedsanvisninger følges.

6.6 Dataangreb og IT-forensisk undersøgelse
Hvis Bambora har mistanke om, at Salgsvirksomhedens kassesystemer, it-systemer eller lignende har været udsat for angreb, manipulation eller lignende, som efter Bamboras mening på nogen måde berører Parternes samarbejde iht. denne Aftale, har Bambora ret til at foretage en såkaldt IT-forensisk undersøgelse af det pågældende udstyr. Undersøgelsen skal foretages af Bambora eller af en IT-forensisk virksomhed, der er engageret af Bambora.

Tidspunkt og dermed relaterede spørgsmål/rutiner, som kan henføres til Undersøgelsens gennemførelse, skal, hvis Bambora ikke vurderer dette som ubelejliget, om muligt aftales mellem Parterne. Bambora må dog også, hvis det efter Bamboras mening er mest formålstjenligt, besøge Salgsvirksomheden og gennemføre Undersøgelsen, uden at Salgsvirksomheden underrettes herom på forhånd.

Det påhviler Salgsvirksomheden i rimeligt omfang at medvirke ved Undersøgelsen og lette gennemførelsen, således at formålet med Undersøgelsen, dvs. at konstatere hvorvidt der har været angreb/manipulation, kan opnås.

I tilfælde af, at det ved Undersøgelsen konstateres, at Salgsvirksomhedens kassesystemer, it-systemer eller lignende, har været udsat for angreb, manipulation eller lignende, påhviler det Salgsvirksomheden på Bamboras anmodning at godtgøre Bambora omkostninger til Undersøgelsen.

7. Liability Shift

Bambora anvender såkaldt Liability Shift. Dette indebærer, at Salgsvirksomheden i forholdet til Bambora iht. Aftalen, bærer risikoen for samtlige tab, som kan henføres til magnetlæste Transaktioner foretaget med uautoriseret fremstillede kort, hvor det korrekte Kontokort, dvs. det af en autoriseret/licenseret kortudsteder udstedte Kontokort med samme kortnummer som det uautoriseret fremstillede, er forsynet med en såkaldt EMV-chip.