FORSKRIFTER FOR SALG MOT BETALING MED KONTOKORT
I UBEMANNET TERMINAL
(Oktober 2015)

Disse forskrifter, "Forskrifter for ubemannet terminal", gjelder ved salg mot betaling med Kontokort i ubemannede terminaler som parkeringsautomater, vareautomater og veibommer.

Forskriftene utgjør et tillegg til de Generelle vilkårene for innløsning av kontokorttransaksjoner som er inngått mellom Salgsforetaket og Bambora. Ved eventuelle konflikter mellom Hoveddokumentet og Forskriftene skal Forskriftene ha fortrinnsrett.

1. Terminaltyper for ubemannet miljø

Type 1 gjelder Ubemannet terminal der autorisering alltid skal gjennomføres "online", uansett beløpets størrelse, og der verifisering skjer med PIN-kode, for eksempel i vareautomat.

Type 2 gjelder Ubemannet terminal der autorisering alltid skal gjennomføres "online", uansett beløpets størrelse, men som mangler mulighet til verifisering med PIN-kode. Transaksjoner via parkeringsautomater (MCC 7523) i dette miljøet kan ikke overstige 50 EUR*. Transaksjoner via vareautomater (se definisjon under) i dette miljøet kan ikke overstige 20 EUR*. Forøvrig kan transaksjonsbeløpet aldri overstige EUR 100*.
* Eller tilsvarende i lokal valuta.

Type 3 Denne løsningen er bare tillatt for Veibommer (MCC 4784). Gjelder Ubemannet terminal som bare er "offline" og mangler mulighet for verifisering med PIN-kode. Transaksjonene i dette miljøet kan ikke overstige EUR 40, og kortet skal kontrolleres mot sperreregister.

For ubemannet bensinpumpe (MCC 5542) gjelder særskilte forskrifter.

2. Chip og Pin-terminaler

Terminaler som brukes til å gjennomføre transaksjoner med Kontokort, skal støtte teknologi for både magnetsporavlesning og EMV-chip. MasterCard/VISA kan komme til å ilegge Bambora et gebyr dersom Salgsforetaket bryter mot ovennevnte. I dette tilfellet er Salgsforetaket i henhold til Hoveddokumentet forpliktet til å kompensere Bambora for slike gebyrer.

F.o.m. 1. januar 2016 skal alle nyinstallerte terminaler, uansett type, hos salgsforetak som tidligere ikke har godtatt Kortbetalinger, ha støtte for kontaktløse transaksjoner, også kalt "Contactless". Dette gjelder også salgsforetak som bytter ut samtlige av sine kortlesere. F.o.m. 1. januar 2020 skal samtlige terminaler ha støtte for kontaktløse transaksjoner.

3. Kundekvittering

Kundekvittering skal alltid gis og skal inneholde følgende informasjon:

- Salgsforetakets navn, sted og organisasjonsnummer
- Dato
- Kontokortets nummer skal angis i trunkert form (dvs. at bare de (4) siste tallene skrives ut, innledende posisjoner trunkeres med "*").

- Beløp
- Opplysninger om merverdiavgift
- Referanse/gjenfinningsnummer (unik identitet for Transaksjonen)

4. Bruk av PIN

Dersom Terminalen håndterer PIN, skal kortinnehaveren gis tre (3) forsøk på å identifisere seg ved hjelp av PIN-kode. Dersom feil PIN-kode tastes inn tre (3) ganger på rad, skal utstyret om mulig beholde kortet. Disse kortene klippes i stykker og sendes til den aktuelle kortutstederen. Kortinnehaveren skal ha mulighet til å avbryte en transaksjon i stedet for å gjøre flere forsøk med PIN-kode.

Dersom PIN ikke er tillatt for korttypen, kan kortet ikke brukes i selvbetjeningsutstyr med PIN-verifisering.

Med transaksjoner via vareautomater menes varer og tjenester som kan selges ved en ubemannet terminal, bortsett fra:

- Parkeringsplasser, parkeringsautomater og garasje (MCC 7523)
- Veibommer (MCC 4784)
- Bensinpumper (MCC 5542)
- Alle varer eller tjenester som har en lovpålagt aldersgrense for salg (for eksempel spill, tobakksvarer og alkohol)
- Alle varer eller tjenester som i følge andre regler eller forskrifter har visse restriksjoner ved salg, og som ville kreve noen form for verifisering av kunde eller kortinnehaver (for eksempel legemidler).

4. Transaksjonsinnsamling

Innsamling av kjøpstransaksjoner med Kontokort der navn og/eller nummer ikke er preget (for eksempel Kontokort med varemerkene Maestro og Electron), kan bare skje i Terminal type 1 og i parkeringsautomater (MCC 7523) type 2.

5. Rapportering

5.1 Innsending av kjøpstransaksjoner
Elektronisk innsamlede kjøpstransaksjoner skal overføres til Bambora senest innen to (2) dager fra betalingsdatoen. Med "betalingsdatoen" menes datoen for autoriseringen.

5.2 Transaksjonsjournal
Salgsforetaket skal føre en særskilt journal over samtlige Transaksjoner der et Kontokort er brukt, dvs. både gjennomførte og avbrutte Transaksjoner. Denne journalen skal vise:

- På hvilken måte Transaksjonen er gjennomført,
- Salgsforetakets navn (firma), sted og organisasjonsnummer,
- Dato og klokkeslett,
- Kontokortets nummer (forutsatt at Terminalen støtter dette, skal dette skje i trunkert form),

- Transaksjonstype (betaling eller retur/kreditering) i klartekst,
- Kasseidentitet,
- Kontrollnummer som bevis på autorisering,
- Beløp som skal debiteres,
- Referanse/gjenfinningsnummer, og
- Svarkode.

5.3 Lagring
Salgsforetaket skal i minst atten (18) måneder arkivere Transaksjonsjournalen i henhold til gjeldende regler for PCI DSS (se punkt 6.1 nedenfor). På forespørsel fra Bambora skal Salgsforetaket innen fem (5) bankdager kunne legge frem en kvittering som gjelder en enkelt Transaksjon. Dette gjelder selv om Salgsforetakets innløsningsavtale med Bambora ellers har opphørt.

6. Sikkerhet

6.1 Håndtering av Kontokortinformasjon
For dels å beholde et høyt sikkerhetsnivå i de globale kortbetalingssystemene og dels å styrke tilliten til Kontokort som betalingsmiddel er det ytterst viktig at alle som håndterer Kontokortinformasjon, gjør det på en sikker måte. Med "Kontokortinformasjon" menes slik informasjon som er preget eller trykt på Kontokortets frem- og bakside, inkludert informasjon som ligger lagret på Kontokortets magnetspor og chip. Av denne grunn har kortbransjen blitt enige om en felles standard for håndtering av Kontokortinformasjon. Standarden kalles Payment Card Industry (PCI) Data Security Standard (DSS) og er utarbeidet av de internasjonale kortnettverkene Visa og MasterCard.

Salgsforetaket forplikter seg til å følge standarden PCI DSS i den versjonen som til enhver tid finnes publisert på www.pcisecuritystandards.org.

6.2 Godkjenning av system
Terminaler som leverer Transaksjoner til Bambora, skal være godkjent av Bambora eller annen tredjepart som Bambora utpeker. Bambora kan stille krav til særlig kontroll av komponenter som ut fra et sikkerhetssynspunkt er sensitive.

6.3 Særskilt om såkalte Noder og Payment Service Providers
Bruker Salgsforetaket en tredjepart (såkalt node eller Payment Service Provider) som del av sin betalingsløsning for håndtering av Transaksjoner, må Salgsforetaket sikre at denne oppfyller alle krav i henhold til PCI DSS.

6.4 Endringer av utstyr m.m.
Salgsforetaket skal informere Bambora før hver installasjon, omflytting eller avvikling av utstyr som er teknisk koblet til Bambora eller annen innsamler av Transaksjoner som fungerer på oppdrag fra Salgsforetaket innenfor rammene av denne avtalen.

Endringer i Terminaler som påvirker de forutsetningene som gjaldt på tidspunktet for godkjenning, kan ikke gjennomføres uten godkjenning fra Bambora.

Salgsforetaket skal, før Transaksjoner kan overføres til Bambora, gjennomføre en test anvist av Bambora av sin oppkobling mot Bamboras mottakssystem.

6.5 Særskilt om kassesystem med integrert kortleser / Sikkerhetsinstruksjoner
Salgsforetak som bruker kassesystem med integrert kortleser skal også sørge for at særskilte Sikkerhetsinstruksjoner meddelt av Bambora til enhver tid følges.

6.6 Datainnbrudd og IT-rettslige undersøkelser
Dersom Bambora mistenker at Salgsforetakets kassesystem, datasystem e.l. har vært utsatt for innbrudd, manipulasjon e.l. som etter Bamboras vurdering på noen måte angår Partenes samarbeid i henhold til denne Avtalen, har Bambora rett til å gjennomføre en IT-rettslig undersøkelse av det aktuelle utstyret. Undersøkelsen skal gjennomføres av Bambora eller av et IT-rettslig foretak utpekt av Bambora.

Tidspunkt, og spørsmål/rutiner som henger sammen med dette og som kan henføres til gjennomføringen av Undersøkelsen, skal, dersom Bambora ikke vurderer dette som upassende, så langt det er mulig avtales mellom Partene. Bambora kan imidlertid også, dersom dette etter Bamboras mening er det mest formålstjenlige, besøke Salgsforetaket og gjennomføre Undersøkelsen uten at Salgsforetaket har blitt underrettet om dette på forhånd.

Salgsforetaket plikter i rimelig omfang å medvirke ved Undersøkelsen og tilrettelegge for gjennomføringen slik at formålet med Undersøkelsen, dvs. å konstatere om det har forekommet innbrudd/manipulasjon, kan oppnås.

Dersom Undersøkelsen fører til at det konstateres at Salgsforetakets kassesystem, datasystem e.l. har blitt utsatt for innbrudd, manipulasjon e.l., plikter Salgsforetaket på forespørsel fra Bambora å dekke Bamboras kostnader til Undersøkelsen.

7. Liability Shift

Bambora bruker såkalt Liability Shift. Dette innebærer at Salgsforetaket i forholdet til Bambora ifølge Avtalen bærer risikoen for samtlige tap som kan henføres til magnetsporleste Transaksjoner foretatt med uberettiget fremstilte kort, der det korrekte Kontokortet, dvs. Kontokortet utstedt av berettiget/lisensiert kortutsteder med samme kortnummer som det uberettiget fremstilte, er utstyrt med en såkalt EMV-chip.