

FORSKRIFTER FOR SALG MOT BETALING MED KONTOKORT

SALG I BUTIKK (Card Present)

(Oktober 2015)

Disse forskriftene, "Butikkforskriftene", gjelder for salg mot betaling med Kontokort med bruk av Terminal.

Butikkforskriftene utgjør et tillegg til de Generelle vilkårene for innløsning av kontokorttransaksjoner ("Hoveddokumentet") som er inngått mellom Salgsforetaket og Bambora. Ved eventuelle konflikter mellom Hoveddokumentet og Butikkforskriftene skal Butikkforskriftene ha fortrinnsrett. Ord som skrives med stor forbokstav, er ord som har fått særlig betydning/definisjon i Hoveddokumentet, og som i disse Butikkforskriftene skal ha samme betydning som de har i Hoveddokumentet.

1. Kontroller

Salgsforetaket skal i forbindelse med betaling utføre kontrollene angitt nedenfor.

1.1 Kontokortet

I tilfeller der 1) informasjonen på Kontokortet avleses uten medvirkning fra Salgsforetaket, og 2) Kortinnehaveren kvitterer for Transaksjonen med PIN-kode, er det ikke nødvendig å utføre kontrollene angitt i punkt 1.1 nedenfor. Det samme gjelder dersom informasjonen på Kontokortet avleses uten medvirkning fra Salgsforetaket og typen Kontokort ikke krever noen ytterligere tiltak/kvittering for Transaksjonen enn selve avlesningen av informasjonen.

Salgsforetaket skal gjennom visuell kontroll sikre at:

- Kontokortet er utstyrt med Kortinnehaverens signatur,
- Kontokortet ikke bærer spor av endringer,
- Gyldighetsperioden angitt på Kontokortet ikke er utløpt,
- Kontokortet er utstyrt med et varemerke, jf. punkt 1 ("Kontokort") i Hoveddokumentet, som omfattes av Avtalen.

Dersom ovennevnte krav ikke er oppfylt, skal Kontokortet ikke godtas som betalingsmiddel.

1.2 Signatur

Salgsforetaket behøver ikke å kontrollere signatur, fordi Kortinnehaveren kvitterer for transaksjonen med PIN-kode (se punkt 3 under).

Salgsforetaket skal sammenligne Kortinnehaverens underskrift på signaturkvitteringen med signaturen på Kontokortet. Hvis disse ikke stemmer overens, skal Kontokortet ikke godtas som betalingsmiddel.

1.3 Autorisering og sperrekontroll

Autorisering skal alltid skje i betalings situasjonen, uansett kjøpsbeløp. Dersom autorisering og sperrekontroll ikke skjer elektronisk i Terminal, må Salgsforetaket gjennom telefonsamtale til Bambora innhente samtykke til at kjøpstransaksjonen kan gjennomføres. Godkjennelse gis av Bambora med angivelse av et kontrollnummer som skal noteres på signaturkvitteringen. Kontokort uten preget navn og/eller nummer (for eksempel Kontokort med varemerkene Maestro og Electron) krever imidlertid alltid at autorisering skjer elektronisk. Transaksjoner kan ikke gjennomføres hvis verken magnetstripen eller Kontokortets chip av en eller annen grunn kan avleses. Dersom Salgsforetaket ved autoriseringen får beskjed om at Kontokortet

er sperret, eller det blir tydelig at Kontokortet brukes av uvedkommende, skal Salgsforetaket om mulig ta hånd om kortet. Salgsforetaket skal deretter klippe i stykker Kontokortet og sende det inn til Bambora.

Ved kontroll av status på Kortinnehaverens Kontokort (kontroll av kortstatus) skal det alltid brukes en såkalt "nullverdi-autorisasjon".

1.4 Chip og Pin-terminaler

Terminaler som brukes til å gjennomføre transaksjoner med Kontokort, skal støtte teknologi for både magnetsporavlesning og EMV-chip. MasterCard og 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.

1.5 Terminaler med støtte for kontaktløse transaksjoner

F.o.m. 1. januar 2016 skal alle nyinstallerte terminaler hos salgsforetak som tidligere ikke har godtatt Kontokort, 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.

2. Kvitteringer

2.1 Signaturkvitteringens innhold

Salgsforetakets eksemplar av signaturkvitteringen skal inneholde følgende opplysninger:

- Salgsforetakets navn, sted og organisasjonsnummer,
- Salgsforetakets kundenummer hos Bambora,
- Dato og klokkeslett for Transaksjonen,
- Kontokortets nummer (forutsatt at Terminalen støtter dette, skal dette skje i trunkert form),
- Transaksjonstype (betaling eller retur/kreditering) i klartekst,
- Kontrollnummer (bekreftet ved autorisering),
- Valuta og beløp,
- Opplysning om merverdiavgift,
- Teksten: "Godkjennes for debitering av min konto i henhold til ovennevnte" (dette gjelder ikke ved bruk av PIN-kode),
- Plass til signatur (dette gjelder ikke ved bruk av PIN-kode),
- Referanse/gjenfinningsnummer (unik identitet for Transaksjonen).

2.2 Kortinnehaverens kopi

Kortinnehaveren skal motta en kvittering som skal inneholde samme opplysninger som Salgsforetakets eksemplar av signaturkvitteringen. Følgende unntak gjelder imidlertid for Kortinnehaverens kopi:

- Kontokortets nummer skal angis i trunkert form,
- Teksten "kortbetaling" behøver ikke angis (dette kreves bare dersom kopien av signaturkvitteringen består av en komplett kassekvittering),
- Teksten "personlig kode" behøver ikke å angis (dette kreves bare ved bruk av PIN-kode),
- Teksten "Godkjennes for debitering av min konto i henhold til ovennevnte" behøver ikke angis.
- Salgsforetakets kundenummer hos Bambora skal ikke angis

2.3 Lagring

Salgsforetaket skal i minst atten (18) måneder arkivere signaturkvitteringer og PIN-kodejournal 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.

3. Bruk av PIN

Beløpet skal være kjent for Kortinnehaveren når PIN-koden angis. Inntastingen av PIN-koden utgjør Kortinnehaverens godkjenning av at kjøpstransaksjonen kan belastes hans/hennes konto. I visse miljøer kan Bambora etter særskilt avtale godkjenne at andre rutiner gjelder.

Kortinnehaveren skal gis tre (3) forsøk på å angi riktig PIN-kode. Kortinnehaveren skal ha mulighet til å avbryte en Transaksjon i stedet for å gjøre flere forsøk med PIN-kode. I manuelt betjent miljø skal Kortinnehaveren ha rett til å avstå fra å bruke PIN-kode og i stedet undertegne en signaturkvittering (forutsatt at godkjenning av kjøpstransaksjonen med PIN-kode ikke er obligatorisk for det aktuelle Kontokortet).

I situasjonene angitt nedenfor skal signaturkvitteringer underskrives, og derfor skal ikke Kortinnehaveren oppfordres til å angi PIN-kode:

- Autorisering kan ikke skje elektronisk,
- Bruk av PIN-kode er ifølge Bamboras instruksjoner ikke tillatt for det aktuelle Kontokortet,
- Kortnummeret er registrert manuelt, dvs. at det ikke har vært mulig å lese Kontokortet maskinelt, eller
- Ved returer/krediteringer.

4. Transaksjonsinnsamling

4.1 Generelt om innsamling

Innsamling av kjøpstransaksjoner med Kontokort skal bare skje ved hjelp av Terminal.

4.2 Terminal

I Terminal skal Kontokortet leses maskinelt. Dersom dette ikke er mulig på grunn av feil på Kontokortet, kan Bambora gi særskilt tillatelse til å registrere Kontokortets nummer og gyldighetstid manuelt. Salgsforetaket skal i en slik situasjon, for eksempel gjennom avtrykk av Kontokortet eller fotokopiering av fremsiden, kunne bekrefte at Kontokortet var til stede i betalingssituasjonen. Fotokopien e.l. skal oppbevares sammen med den tilhørende signaturkvitteringen på en måte som er i samsvar med PCI-regelverket. Manuell registrering er imidlertid aldri tillatt for Kontokort der navn og/eller nummer ikke er preget (for eksempel Kontokort med varemerkene Maestro og Electron).

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. For miljøer som for eksempel hoteller, der det skjer en såkalt forhåndsautorisasjon, skal kjøpstransaksjonen være mottatt av Bambora innen tretti (30) dager.

5.2 PIN-kodejournal

Salgsforetaket skal føre en særskilt journal over samtlige Transaksjoner der PIN-kode 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),
- Betalingsmåte (se punkt 1.1 ovenfor),
- Transaksjonstype (betaling eller retur/kreditering) i klartekst,
- Kasseidentitet,
- Kontrollnummer som bevis på autorisering,
- Valuta og beløp,
- Referanse/gjenfinningsnummer, og
- Svarkode.

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 Kortnettverket 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 Payment Service Providers

Bruker Salgsforetaket en tredjepart (såkalt 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 tilkoblet til Bambora eller annen innsamler av Transaksjoner som fungerer på oppdrag fra Salgsforetaket innenfor rammene for 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.

6.6 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 såkalt 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 på Transaksjoner, som 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.