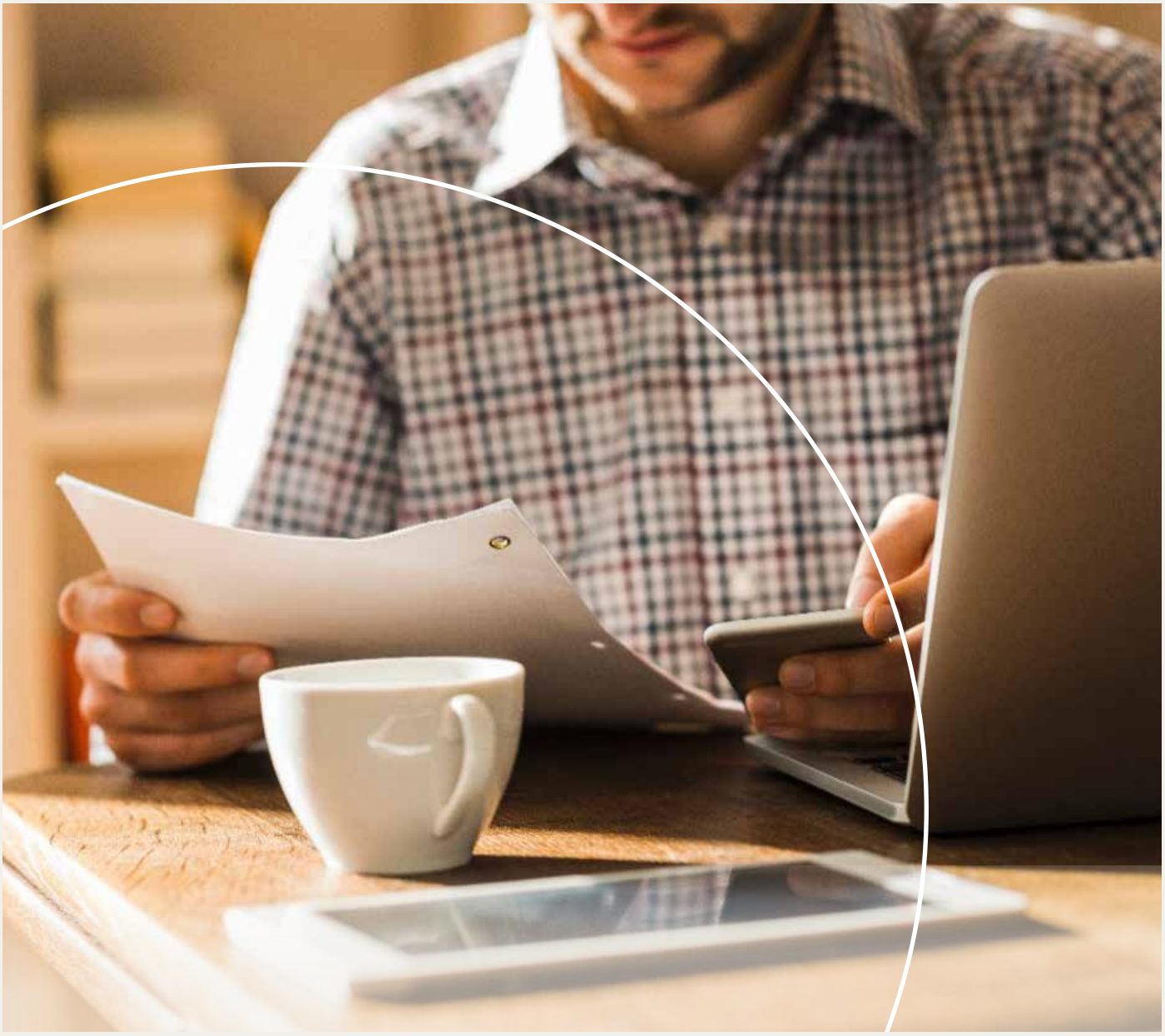


Fra 14. september 2019 vil betaling via nett ifølge loven kreve tofaktorautentisering. Er dere klare?

Her kan du lese vanlige spørsmål fra og tiltak for salgssteder med Mastercard® Identity Check™/EMV 3-D Secure. Målet er å gi deg oversikt over og bedre forståelse av de forandringene og mulighetene det medfører for Europa når direktivet om sterk kundeautentisering (Strong Customer Authentication, SCA) trer i kraft 14. september 2019.

mastercard

Juni 2019

Reduser svindel og feilaktig avviste betalinger – samtidig som du gir kundene en bedre opplevelse.

EUs andre betalingstjenestedirektiv (PSD2 RTS) har som mål å redusere svindel og innføre en bedre og sikrere standard for betaling via nett.

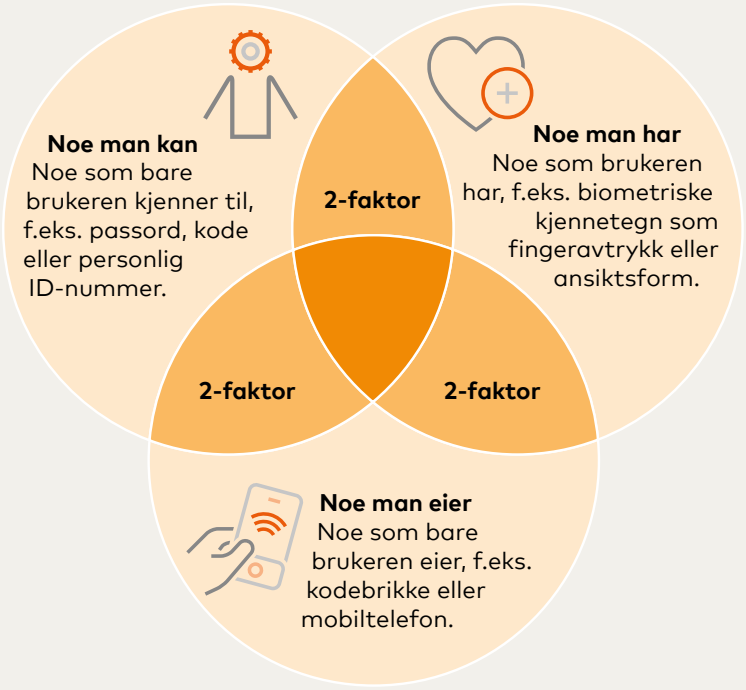
SCA innebærer at fra og med 14. september 2019 må tofaktorautentisering (F2A) brukes ved all betaling via nett, såfremt kortutstedende banker eller innløsere ikke benytter seg av unntak, som også reguleres av direktivet.

Salgssteder må sende autentiseringsforespørsler ved å bruke den nye EMV 3DS-standarden – ellers kan den kortutstedende banken måtte avvise transaksjonen, siden de ikke har nok informasjon til å påvise sterk kundeautentisering, som loven krever.

Tofaktorautentisering er et grunnleggende prinsipp i det andre betalingstjenestedirektivet (PSD2).

Det overordnede målet er å oppnå økt sikkerhet ved digitale betalinger.

Sterk kundeautentisering innebærer at to av følgende faktorer må inngå i identifiseringen:



Dessuten må faktorene være uavhengige av hverandre, slik at brudd mot én faktor ikke påvirker eller gir tilgang til de andre. I tillegg bør minst én av faktorene ikke kunne gjenbrukes eller kopieres (bortsett fra noe man har), og ikke kunne stjeles via Internett. En kundeautentisering anses ikke som sterk hvis man bare kan påvise to elementer av én og samme faktor.

mastercard

Rutiner for sterk kundeautentisering blir obligatoriske og skal gjelde ved all betaling via Internett samt ved håndtering av sensitive opplysninger om betalinger.

Direktivet om sterk kundeautentisering (SCA) gjelder hvis både den kortutstedende banken og innløseren er hjemmehørende i EØS-land (two-leg transactions).

Det andre betalingstjenestedirektivet (Regulary Technical Standard, RTS) gir den kortutstedende banken og innløseren anledning til å benytte seg av flere spesifikke unntak (exemptions). Disse unntakene gir mulighet til å ikke kreve tofaktorautentisering for f.eks. beløp som er under/lik 30 euro, faste betalinger / abonnementsbetalinger (av samme beløp) og transaksjoner til kjente mottakere (såkalt whitelisting). Obs! Den kortutstedende banken eller innløseren er ikke forpliktet til å benytte seg av unntakene. Kortutstedende bank er alltid endelig beslutningsmyndighet.

Derfor bør dere agere allerede nå
- Uten sterk kundeautentisering kan antall avviste transaksjoner øke, noe som kan føre til redusert kundetilfredshet og redusert salg.
- Når direktivet er implementert, kan man få fordeler ved å tilby økt betalingssikkerhet, friksjons-fri betaling via nett og økt kundetilfredshet.

Spørsmål og svar

Hva er EMV 3DS? Og hvorfor må vi oppdatere til en ny standard?

EMV 3DS er en ny bransjestandard som er utviklet globalt av EMVCo (en bransjeorganisasjon etablert av Europay, Mastercard og VISA).

EMV 3DS etterfølger dagens autentiseringsgrensesnitt, 3D Secure 1.0, som ble lansert i 2002. Med rask teknologiutvikling og stadig økende svindel har EMVCo sett at det er et globalt behov for en ny sikkerhetsstandard som kan takle de raske teknologiendringene og sikkerhetsutfordringene vi står overfor.

Formålet med EMV 3DS er å gjøre betalinger sikrere og kjøpsopplevelsen enklere. Standarden omfatter:

- en økt strøm av transaksjons- og forbrukerdata (f.eks. enhetsdata, leverings- og faktureringsadresse), slik at banker kan gjøre unntak fra SCA og å forbedre beslutningene rundt autoriserte transaksjoner
- støtte for nye betalingsbehov, f.eks. betaling i app og mobilbetalinger
- støtte for flere bruksområder, f.eks. lagrede kontoopplysninger (Credentials on File)
- digitale lommebøker, f.eks. Google Wallet, Samsung Pay og Apple Pay
- tokenisering: et token (en krypteringsnøkkel) som erstatter det lagrede kortnummeret

mastercard

* Finanstilsynet må oppgi tilsvarende verdi i norske kroner (NOK).

Hva innebærer EMV 3DS for kortinnehavere?

Med EMV 3DS får kortinnehaveren en enhetlig og enkel betalingsopplevelse på alle enheter, samtidig som sikkerheten blir enda bedre.

Hvordan støtter økt utveksling av autentiseringsdata risikobasert autentisering (RBA)?

EMV 3DS støtter økt datautveksling mellom salgssteder og kortutstedende banker, blant annet bransjekode (MCC), risikoindikatorer som viktige adresser (f.eks. leverings-, fakturerings- og e-postadresse), enheter, geografisk plassering og atferdsmønster. Ved hjelp av en bredere data-strøm og mulighet til å kunne avlese atferds- og transaksjonsinformasjon kan mistenkt svindel identifiseres gjennom bruk av en såkalt risikomotor (fraud monitoring tool).

Transaksjoner som anses å være sikre (lav risiko), kan godkjennes i bakgrunnen. Ved transaksjoner med høy risiko oppfordrer systemet deg derimot til aktiv verifisering med sterk kundeautentisering (tofaktor).

Målet med RBA er:
- at færre transaksjoner avbrytes før kjøpet er gjennomført
- å redusere antall transaksjoner som krever aktiv sterk kundeautentisering
- en bedre kjøpsopplevelse for kortinnehaveren gjennom hele betalingsprosessen

mastercard

Hvilke fordeler gir Mastercard® Identity Check™?

Mastercard Identity Check er et globalt autentiseringsprogram og varemerke som bygger på det tidligere programmet Mastercard SecureCode®. Det nye programmet er basert på EMV 3DS-standarden. Ved at autentiseringsopplevelsen forbedres for både kortinnehaver og salgssted, vil flere korttransaksjoner bli godkjent. Formålet med programmet er å oppnå best mulig kundetilfredshet i betalingsprosessen ved å redusere svindel og tilby smidigere autentisering.

Mastercards Identity Check-program krever bl.a. fra og med april 2019 (i Norden og Baltikum) at europeiske kortutstedere skal tilby kortinnehaverne biometriske autentiseringsløsninger via smarttelefon – der man ser færrest avbrutte kjøp og minst svindel, og dermed høyest kjøpskonvertering.

MasterCard. SecureCode. → mastercard. ID Check.

Hvordan representerer EMV 3DS og Mastercard® Identity Check™ en mulighet for salgssteder?

Med EMV 3DS og Mastercard Identity Check vil salgssteder kunne oppnå samme nivå av sikkerhet som fysiske butikkmiljøer med:

- i gjennomsnitt 10 % høyere godkjenningsgrad
- opptil 50 % færre tilfeller av svindel
- rundt 50 % reduksjon i avbrutte kjøp

mastercard.

Disse resultatene kan oppnås ved å tillate at kortutstedende banker bruker sterk kundeautentisering ved hvert kjøp via nett. De får relevante data om transaksjonen, slik at de kan gjøre unntak. På den måten kan alle kjøp gjennomføres med minimal friksjon for kortinnehaveren.

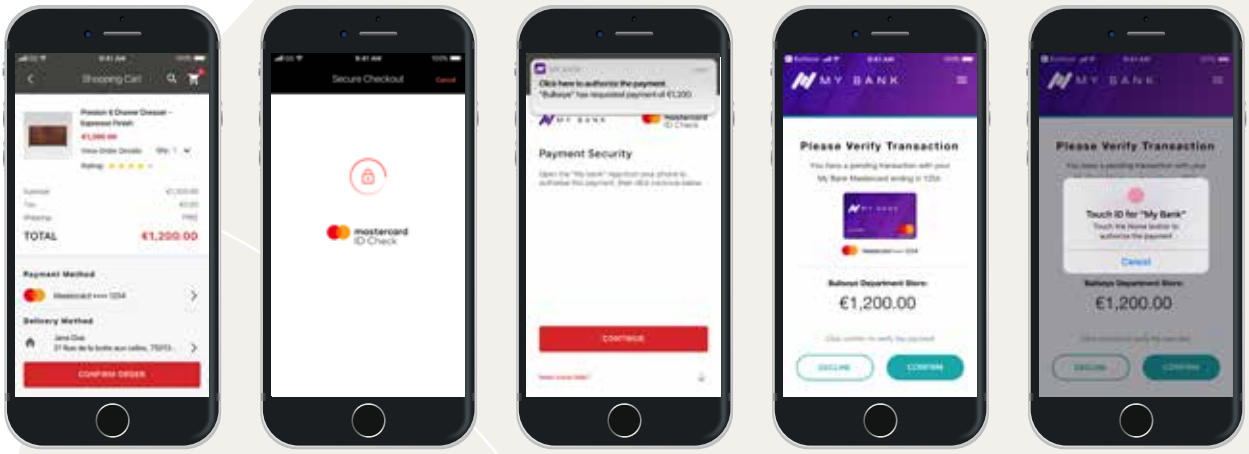
Med Mastercard® Identity Check™ kan kortutstedende banker og salgssteder:

- tilby kortinnehaveren en digital betalingsopplevelse av høyeste kvalitet
- eliminere statiske passord og sikkerhetsspørsmål som kan utnyttes av svindlere
- bruke risikobaserte transaksjoner (bare høyrisikotransaksjoner må verifiseres, andre transaksjoner behandles uten at kortinnehaveren berøres)
- redusere antall avbrutte kjøp og øke nivået av gjennomførte transaksjoner på nett
- øke antall godkjente transaksjoner
- utvide autentiseringen til mobile enheter, som sannsynligvis vil dominere e-handelens fremtid

Hvordan fungerer Mastercard® Identity Check™?

Mastercard Identity Check følger nye regler og fremmer en optimal betalingsopplevelse:

Kortinnehaver – salgssted – Mastercard – bank/ACS-leverandør



1. Betaling initieres fra kassen hos salgsstedet (kortinnehaver).
2. Forespørsel om autentisering sendes via deres 3DS-serverleverandør (salgssted).
3. Forespørsel sendes videre til utstedende bank via autentiseringsnettverket (Mastercard).
4. Forespørsel mottas, og risikobasert autentisering foretas (finansieringsinstitusjon /ACS-leverandør).
5. Hvis risikoen anses å være under den forhåndsdefinerte grensen for risikobasert autentisering, er den videre prosessen friksjonsfri. Hvis risikoen anses å være høyere, verifiseres kortinnehaveren med sterk autentisering (finansieringsinstitusjon/ACS-leverandør).
6. Svar mottas, og autentisering godkjennes (salgssted).

mastercard

Erstatter Mastercard® Identity Check™ salgsstedets behov for å autentisere og verifisere kundens identitet?

Nei, Mastercard Identity Check oppfyller Mastercards visjon om å flytte betalingsautentisering fra hva forbrukerne kan (f.eks. passord), til hva de eier (f.eks. mobiltelefoner), og hva de har (dvs. biometri, eksempelvis fingeravtrykk), for å gjøre kjøpsopplevelsen sikrere og enklere.

Hvordan foregår implementeringen av Mastercard® Identity Check™ på overordnet nivå (koding, systemendringer osv.)?

Mastercard Identity Check inneholder veiledning og spesifikke krav til salgssteder og kortutstedende banker. Kortutstedende banker må tilby kortinnehaveren en av de verifiseringsmetodene som programmet krever, for eksempel dynamisk passord, biometrisk identifikasjon eller lignende metoder for å øke sikkerheten og skape en brukervennlig opplevelse.

Til salgssteder og PSP-er stilles det spesifikke krav, for eksempel at de må oppgi en Accountholder Authentication Value (AAV) for hver transaksjon.

Kortutstedende banker og salgssteder må også følge programmets nøkkelindikasjoner, blant annet følgende:

- et årlig tak på autentiserte transaksjoner som er utsatt for svindel.
- at løsningen deres har et laveste nivå for godkjente transaksjoner.
- krav til deling av autentiseringsdata.

Hvis du vil ha mer informasjon, kan du gå til Mastercard Connect og lese Mastercards "Global Operation Bulletin" og "Program Guide".

Hvilke transaksjoner påvirkes av Mastercard® Identity Check™?

Mastercard Identity Check er utformet for å støtte alle Mastercards varemerker (Mastercard, Maestro osv.) innenfor samtlige segmenter (privat og bedrift) og produkter (kredittkort, debetkort og forhåndsbetalte (pre-paid) kort).

Skjer det endringer som påvirker ansvar (liability shift) og interchange-kostnader?

Samtlige innløsere som driver virksomhet i Europa, har ansvaret for transaksjoner der det gjøres unntak fra SCA. Dette gjelder uansett om salgsstedet sender med EMV 3DS-data i transaksjonen eller ikke.

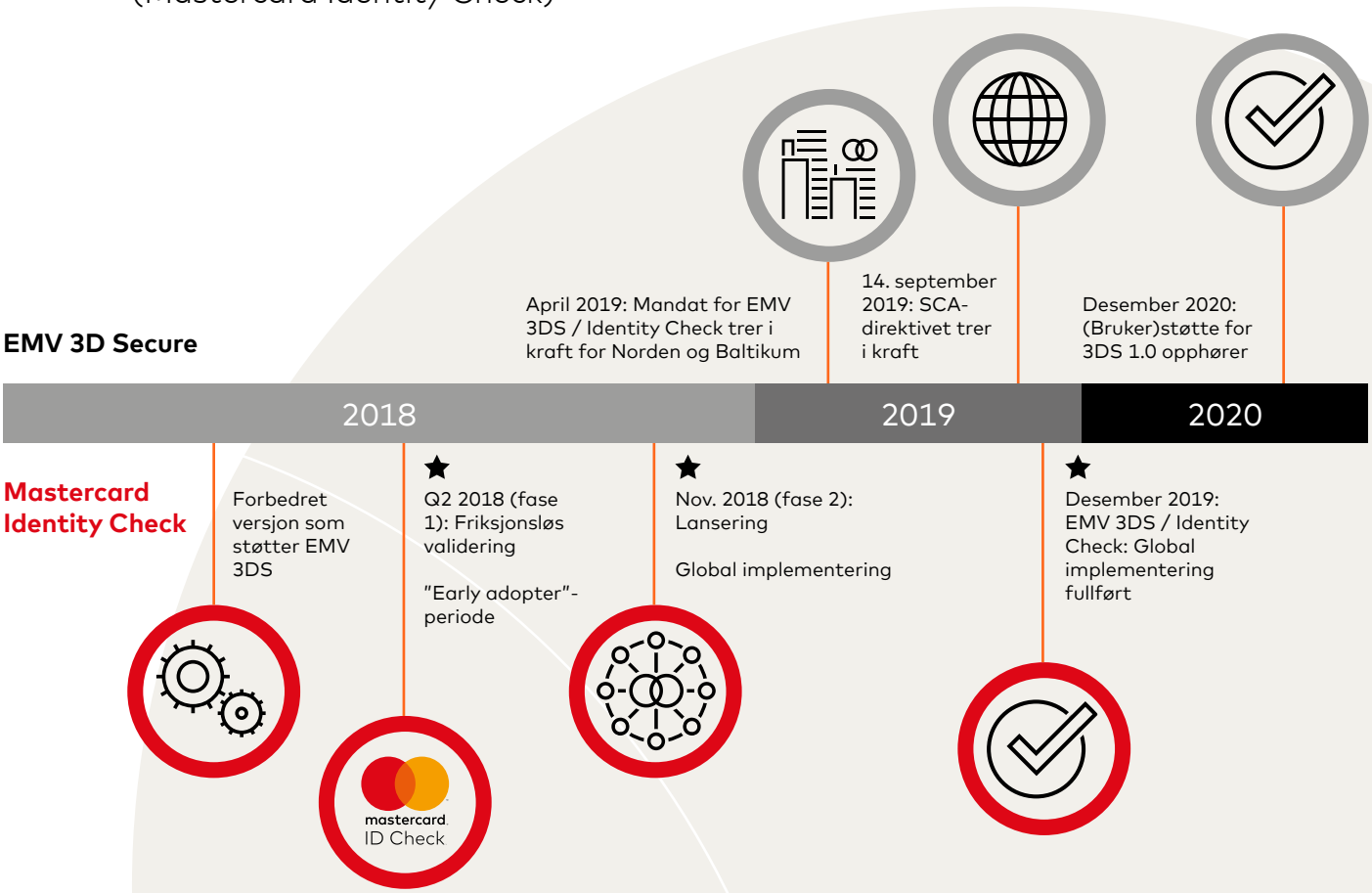
mastercard

Hvordan ser tidslinjen ut for kortutstedende banker, salgssteder og innløsere?

For at overgangen skal bli smidigst mulig, vil den nye standarden, EMV 3DS, i starten gjelde parallelt med 3DS 1.0. På denne måten kan kortutstedende bankers ACS-leverandører håndtere transaksjoner både fra salgssteder som bruker den gamle versjonen (3DS 1.0), og fra salgssteder som bruker den nye versjonen (EMV 3DS). Takket være dette kan kortutstedende banker og salgssteder skreddersy sine løsninger til egne forretningsmål og tidsplaner.

Mastercard vil fortsette å jobbe med samtlige aktører og tjenesteleverandører på det globale markedet for å gi best mulig støtte i overgangen. Hensikten med tidsplanen nedenfor er å hjelpe ulike aktører med å planlegge implementeringen av EMV 3DS.

Tidslinje: Overgang fra 3DS 1.0 (SecureCode) til EMV 3DS (Mastercard Identity Check)



For å sikre funksjonaliteten mellom 3DS 1.0 og EMV 3DS må 3DS-servere og ACS-leverandører støtte både 3DS 1.0 og EMV 3DS inntil (bruker)støtte for 3DS 1.0 (SecureCode) opphører.

- 3DS-servere (tidligere kjent som MPI) skal bygges slik at de kan støtte både 3DS 1.0 og EMV 3DS for salgssteder.
- ACS-leverandører må bygge støtte for både 3DS 1.0 og EMV 3DS for kortutstedende banker.
- Kortutstedende banker må støtte 3DS 1.0 og EMV 3DS for alle kortmodeller (kredittkort, debetkort og forhåndsbetalte kort).

mastercard

Unntak fra SCA: Når og hvordan gjelder disse?

RTS tillater at kortutstedende banker og innløsere kan gjøre følgende unntak for betaling via nett:

- For transaksjoner der summen er 30 euro* eller mindre. Dette unntaket krever imidlertid SCA for hver sjette transaksjon eller hvis den samlede summen er over 100 euro* siden forrige SCA-transaksjon.
- Ved faste transaksjoner (abonnementsbetalinger) der beløpet og forbrukeren er den samme. SCA kreves alltid når en forbruker registrerer kortet sitt for faste transaksjoner (første transaksjon). De etterfølgende transaksjonene skal alltid inneholde en referanse til den første betalingen, men krever ingen SCA.
- Når kortutstedende bank foretar en risikoanalyse. Dette kan gjøres på transaksjoner som samsvarer med summen og svindelnivået som er definert i RTS. Et eksempel på ovennevnte er når en kortinnehaver uten tidligere påvist svindelrisiko gjennomfører en betaling fra en enhet vedkommende har brukt før, der beløpet er under 100 euro*, og der innløserens svindelnivå ikke overstiger 13 rentepunkter (basis points).
- For transaksjoner hos salgssteder som kortinnehaveren stoler på og har satt på en "whitelist", kreves SCA bare ved oppretting og endring av "whitelist". Det er bare kortutstedende banker som kan gjøre slike unntak. Hvis ikke innløseren gjør unntak fra SCA, er den kortutstedende banken ansvarlig for eventuell svindel hvis en autorisasjon er godkjent, forutsatt at salgsstedet har sendt en autentiseringsforespørsel for transaksjonen.

Fra og med 14. september bør salgssteder bruke EMV 3DS-autentisering, hvis ikke innløseren har gjort unntak. Hvis et salgssted / en innløser benytter seg av et unntak som godkjennes av kortutstedende bank, berøres ikke kortinnehaveren (dvs. kortinnehaveren trenger ikke å autentisere seg ytterligere ved betaling via nett).

Autoriserte transaksjoner uten autentisering er tillatt ifølge PSD2 RTS hvis innløseren har gjort et unntak. Disse har imidlertid ofte lavere godkjenningsgrad.

Hva er de viktigste tiltakene salgsstedet må gjennomføre?

1. PSP-en (Payment Service Provider / betalingstjenesteyter) som salgsstedet har valgt, må implementere og håndtere grensesnittet mot salgsstedet for autentisering gjennom EMV 3DS og 3DS 1.0 (som "fall-back" hvis den kortutstedende banken ennå ikke bruker EMV 3DS).
2. Salgsstedet må være forberedt på å håndtere en større mengde transaksjons- og forbrukerdata (adresse, e-post, mobilnummer eller enhets-ID) og sende dem videre til sin PSP. Det kan kreve koding av et nytt API eller lignende, som leveres av PSP. Salgsstedet må forsikre seg om at deres kundevilkår er i samsvar med GDPR når det gjelder oppbevaring og deling av opplysninger.
3. Salgsstedet må, i overensstemmelse med valgt PSP og innløser, implementere en autentiseringspolicy som støtter RTS og unntaksreglene i direktivet. Spesielt når det gjelder TRA-unntak (Transaction Risk Analysis) og tilhørende svindelnivåer.
4. Salgsstedet må sikre at innløseren registrerer dem for EMV 3DS hos kortselskapene.

mastercard

* Finanstilsynet må oppgi tilsvarende verdi i norske kroner (NOK).

5. Salgsstedet må gjøre oppdateringer på nettstedet sitt for å støtte EMV 3DS, RTS og Mastercard® Identity Check™. En av disse oppdateringene består av å legge inn Mastercards logo for Mastercard Identity Check.
6. Hvis et salgssted via innløseren ber om unntak fra SCA uten autentisering, og transaksjonen avvises av den kortutstedende banken (særlig ved andre årsaker enn finansielle eller tekniske avbrudd), må det finnes en automatisert løsning for å foreta autentisering via EMV 3DS. Hvis transaksjonen godkjennes, må det foretas nok en autorisering. Tilsvarende gjelder hvis kortutstederen ennå ikke støtter EMV 3DS. Da må salgsstedet bruke 3DS 1.0 som "fall-back".
7. Salgsstedet en må sikre at firmanavnet deres er unikt, og at det brukes konsekvent i transaksjonsprosessen med innløser og PSP. På denne måten får de best mulighet til å benytte seg av innløserens unntak fra SCA.
8. Vi anbefaler at salgsstedet alltid ber om autentisering, spesielt for kortutstedende banker som avviser transaksjoner der det ikke er gjennomført autentisering tidligere.
9. Integrer funksjoner fra EMV 3DS for å tilby en optimal kundeopplevelse i appen i forbindelse med autentisering, og for å beholde samme brukergrensesnitt under hele betalingsprosessen.
10. Salgsstedet må sende en autentiseringsforespørsel i samsvar med SCA for den første transaksjonen i forbindelse med at kunden registrerer kortet for abonnementsbetalinger (recurring payments). For at abonnementsbetalinger skal kunne godkjennes uten at kunden må autentisere seg, må salgsstedet sende en forespørsel til kortutstederen i henhold til EMV 3DS. Denne må inneholde en henvisning til den første, SCA-godkjente transaksjonen.
11. I forbindelse med abonnementsbetalinger der beløpene kan variere i størrelse, eller betalinger der det endelige beløpet er ukjent, må salgsstedet tydelig forklare kortinnehaveren hvorfor det opprinnelig autentiserte beløpet kan avvike fra det endelige.

For ytterligere informasjon, vennligst ta kontakt med deres PSP eller innløser.

mastercard

Ordliste:

Accountholder Authentication Value (AAV) – Et kryptogram / en kvittering som beviser at en betaling via nett er autentisert.

ACS-leverandør – Access Control Server. Tredjepartsleverandør av EMV 3DS-løsninger.

Betaling i app – Betaling som skjer uten at kjøperen behøver å forlate salgsstedets mobilapp.

Credentials on File (CoF) – Teknologi som innebærer at kortinnehaveren ikke trenger å oppgi betalingsopplysninger ved hvert kjøp. I stedet lagres de hos salgsstedet/PSP-en.

EMV 3DS – EMVCos standard, som er utviklet for å øke sikkerheten ved betaling via nett. Mastercard® Identity Check™ bygger på denne protokollen.

EMVCo – Bransjeorganisasjon som kontrollerer aksept av sikre betalingstransaksjoner.

PSD2 RTS – EUs andre betalingstjenestedirektiv, som trådte i kraft i begynnelsen av 2018. Forkortelsen står for "Payment Services Directive 2 Regulatory Technical Standards".

PSP – Payment Service Provider, også kalt betalingstjenesteyter, er et selskap som formidler betalingstjenester.

RBA – Risk Based Authentication – Risikobasert autentisering er et autentiseringssystem hos kortutstedende bank som tar hensyn til kortinnehaverens transaksjonshistorikk ved fastsetting av transaksjonens risikoprofil.

SCA – Strong Costumer Authentication eller "stark kundautentisering".

Tokenisering – Teknologi som tillater betaling uten å avsløre kortopplysninger. I stedet for at kortnummeret brukes, opprettes det et unikt digitalt nummer som bare kan brukes med en bestemt enhet eller hos et bestemt salgssted.

Whitelist – En liste over salgssteder som kortinnehaveren stoler på, og som derfor ikke krever like streng autentiseringskontroll.

mastercard