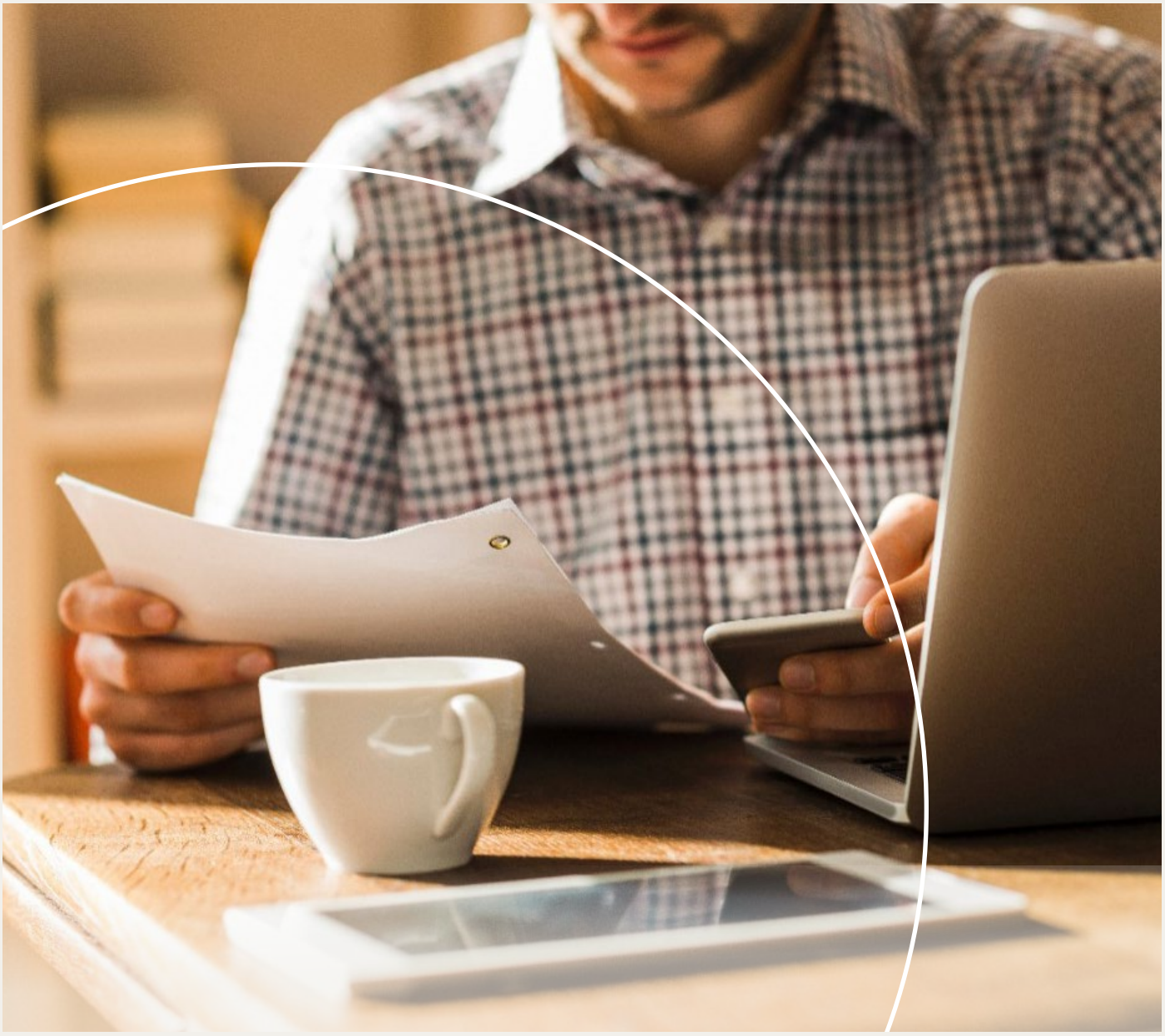


Från den 14 september 2019 kommer online-betalningar kräva tvåfaktorautentisering enligt lag. Är ni redo?

Här kan du ta del av alla vanliga frågor och åtgärder för handlare med Mastercard® Identity Check™/EMV 3-D Secure. Målet är att ge dig en överblick och skapa en bättre förståelse för de förändringar och möjligheter som kommer att ske i Europa då det starka kundautentiserings direktivet Strong Customer Authentication (SCA) träder i kraft den 14 september 2019.

mastercard

Juni 2019

Minska bedrägerier och felaktigt nekade online-betalningar – samtidigt som kundupplevelsen förbättras.

EU:s andra betaltjänstdirektiv (PSD2 RTS) har som målsättning att minska bedrägerier och att införa en förbättrad och säkrare standard för online-betalningar.

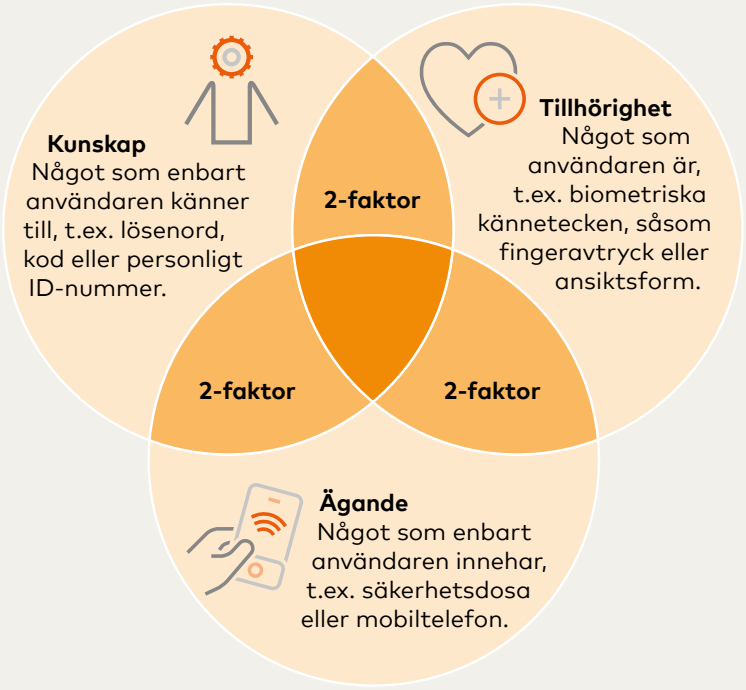
SCA innebär att en tvåfaktorsautentisering (F2A) måste användas för alla online-betalningar från och med den 14 september 2019, såvida kortutgivande banker eller inlösare inte använder sig av ett möjligt undantag, som finns reglerat av direktivet.

Handlare måste skicka autentiseringsförfrågningar genom att använda sig av den nya EMV 3DS standarden – annars kan kortutgivande bank komma att behöva neka transaktionen, då de inte har tillräcklig med information för att påvisa stark kundautentisering, vilket lagen kräver.

Tvåfaktorsautentisering är en grundläggande princip i det andra betaltjänstdirektivet (PSD2).

Det övergripande målet är att åstadkomma en förbättrad säkerhet för digitala betalningar.

En stark kundautentisering bygger på användning av två av följande faktorer som ska ingå i identifieringen:



Dessutom måste faktorerna vara oberoende av varandra, så att brott mot en faktor inte påverkar eller ger tillgång till de andra. Minst en av faktorerna bör också vara icke-återanvändbar och icke-replikerbar (utom för tillhörighet), och inte kunna bli stulen via internet. En kundautentisering anses inte vara stark om man endast kan påvisa två element av en och samma faktor.

mastercard

Rutiner för stark kundautentisering blir obligatoriska och ska tillämpas vid alla internet-betalningar, samt vid hantering av känsliga uppgifter om betalningar.

SCA – Lagen om stark kundautentisering tillämpas där både kortutgivande bank och inlösaren är hemmahörande i EES länder (two–leg).

Det andra betaltjänst direktivet Regulary Technical Standard (RTS) tillåter att kortutgivande bank och inlösaren kan använda sig av ett antal specifika undantag (exemptions). Dessa undantag ger möjlighet att inte kräva tvåfaktorsautentisering, t.ex. för belopp som är mindre än/lika med 30 euro*, återkommande/löpande betalningar (för samma belopp) och transaktioner till kända mottagare (s.k. whitelisting). Värt att notera: Det är inte ett krav för kort-utgivande bank eller inlösaren att använda sig av undantagen. Kortutgivande bank har alltid slutgiltig bestämmanderätt.

Därför ska ni agera redan nu
- Utan stark kundautentisering kan andelen nekade transaktioner öka vilket i sin tur kan resultera i minskad kundnöjdhet och minskad försäljning.
- Vid väl genomförd implementering av direktivet så kan man få en fördel i att erbjuda ökad betalsäkerhet, friktionsfria online-betalningar och ökad kundnöjdhet.

Frågor och svar

Vad är EMV 3DS? Och varför ska man uppdatera till en ny standard?

EMV 3DS är en ny industristandard som har utvecklats globalt av EMVCo (en branschorganisation bildad av Europay, Mastercard, VISA).

EMV 3DS efterföljer det aktuella autentiseringsgränssnittet 3D – Secure 1.0 som lanserades 2002. Med en snabbt växande teknologiutveckling och en ständig ökning av bedrägerier så har EMVCo identifierat ett globalt behov av en ny säkerhetsstandard som kan möta de snabba teknologi-förändringar samt säkerhetsutmaningar vi alla ställs inför.

EMV 3DS syftar till att göra betalningar säkrare och köpresan enklare och kommer med:

- Ett ökat flöde av transaktions- och konsumentdata (t.ex. enhetsdata, frakt- och fakturerings-adress), så att banker kan tillämpa SCA-undantag och förbättra beslutsfattandet kring aukto-riserade transaktioner.
- Stöd för nya betalningsbehov, såsom betalningar "In-app" och mobila-betalningar.
- Stöd för ytterligare användningsområden, såsom lagrade kontouppgifter – (Credentials on File)
- Digitala plånböcker, t.ex. Google -, Samsung- , Apple Pay, etc.
- Tokenisering: en token (krypteringsnyckel) som ersätter kortnumret som lagrats.

mastercard

* Finansinspektionen har som uppgift att meddela motsvarande värde i svenska kronor (SEK).

Vad innebär EMV 3DS för kortinnehavare?

Med EMV 3DS får kortinnehavaren en enhetlig och enkel betalningsupplevelse på alla enheter, samtidigt som säkerheten blir ännu bättre.

Hur stödjer ett utökat datautbyte av autentiseringsdata, Riskbaserad Autentisering (RBA)?

EMV 3DS stödjer ett ökat datautbyte mellan handlare och kortutgivande banker, däribland handelskategorikoden (MCC), handlarens riskindikatorer såsom nyckeladresser (t.ex. frakt, fakturering, e-post, etc.), enheter, platspositioner och beteendemönster. Genom ett bredare dataflöde och möjligheten att kunna avläsa beteende- och transaktionsinformation kan misstänkta bedrägerifall identifieras genom användningen av en s.k. riskmotor (fraud monitoring tool).

Transaktioner som anses vara säkra (lågrisk) kan godkännas i bakgrunden, medan högrisktransaktioner uppmanas, genom systemet, att aktivt verifieras med en stark kundautentisering (tvåfaktor).

Målet med RBA är:
- att färre transaktioner avbryts innan köpet är genomfört.
- att minska antalet transaktioner som kräver aktiv stark kundautentisering.
- en förbättrad shoppingupplevelse för kortinnehavaren genom hela betalningsflödet.

mastercard

Vilka fördelar ger Mastercard® Identity Check™?

Mastercard Identity Check är ett globalt autentiseringsprogram och varumärke som bygger på det tidigare programmet Mastercard SecureCode®. Det nya programmet är baserat på EMV 3DS-standarden. Genom att förbättra autentiseringsupplevelsen för både kortinnehavare och handlare inom e-handeln, kommer fler korttransaktioner att bli godkända. Programmet syftar till att minska bedrägerier och att erbjuda en smidigare autentisering för att uppnå bästa möjliga kundnöjdhet under betalningsprocessen.

Mastercards Identity Check program kräver bl.a. från och med april 2019 (i Norden och Baltikum) att europeiska kortutgivare skall erbjuda sina kortinnehavare biometriska autentiseringslösningar via smartphones – där man ser minst mängd av avbrutna köp och bedrägerier och därav driver högst köpkonvertering.

MasterCard SecureCode → mastercard ID Check

Hur blir EMV 3DS och Mastercard® Identity Check™ en möjlighet för handlare?

Med EMV 3DS och Mastercard Identity Check kommer e-handlare kunna uppnå samma nivå av säkerhet som i en fysisk butiksmiljö med:

- i genomsnitt 10 % högre godkännandegrad.
- upp till 50 % färre fall av bedrägeri.
- runt 50 % färre köp som avbryts.

mastercard

Dessa resultat kan uppnås genom att tillåta kortutgivande banker att använda stark kundautentisering vid varje online-köp. De förses med relevant data för transaktionen, för att kunna tillhandahålla undantag. På så vis kan alla köp genomföras med minimal friktion för kortinnehavaren.

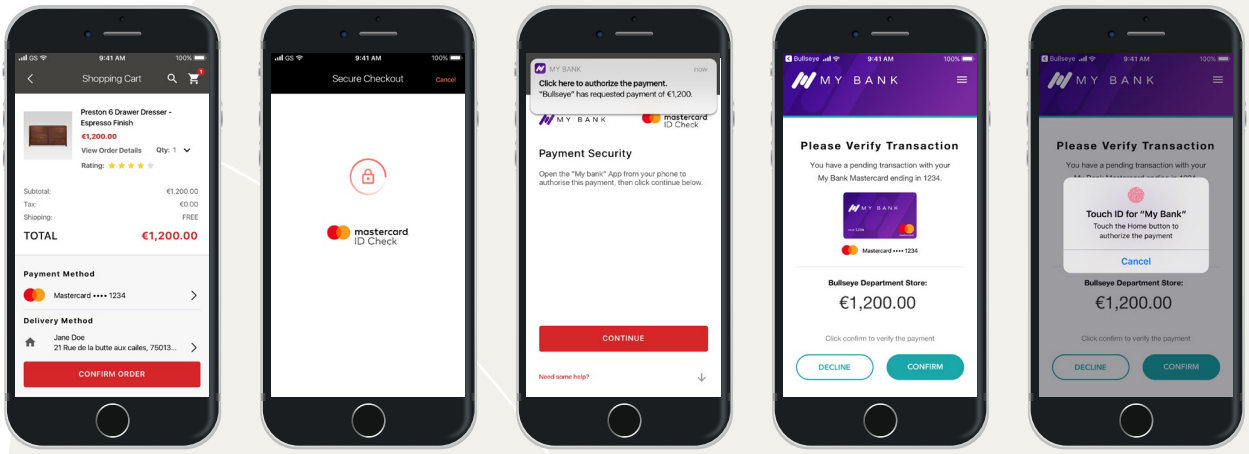
Med Mastercard® Identity Check™ kan kortutgivande banker och handlare:

- erbjuda en digital betalningsupplevelse av högsta kvalitet för kortinnehavaren.
- eliminera statiska lösenord och säkerhetsfrågor som kan utnyttjas av bedragare.
- använda riskbaserade transaktioner – endast högrisktransaktioner behöver verifieras medan övriga transaktioner behandlas utan att kortinnehavaren berörs.
- minska antalet avbrutna köp och öka nivån av genomförda transaktioner online.
- öka antalet godkända transaktioner.
- utöka autentiseringen till mobila enheter, vilka sannolikt kommer att dominera framtiden för e-handel.

Hur fungerar Mastercard® Identity Check™?

Mastercard Identity Check tillämpar nya regler och främjar en optimal betalningsupplevelse:

Kortinnehavare – Handlare – Mastercard – Bank/ACS-leverantör



1. Betalningen initieras från handlarens check-out (Kortinnehavare).
2. Förfrågan för autentisering sker – via deras 3DS-serverleverantör (Handlare).
3. Förfrågan skickas vidare till respektive utgivande bank via autentiseringsnätverket (Mastercard).
4. Tar emot begäran och utför riskbaserad autentisering (Finansinstitut/ACS Provider).
5. Om risken bedöms vara under den förbestämda gränsen för riskbaserad autentisering, sker ett friktionsfritt flöde. Om risken bedöms vara högre, verifieras kortinnehavaren med stark autentisering (Finansinstitut/ACS Provider).
6. Mottager svaret och godkänner autentisering (Handlare).

mastercard

Ersätter Mastercard® Identity Check™ handlarens behov av att autentisera och verifiera kundens identitet?

Nej, Mastercard Identity Check uppfyller Mastercards vision av att flytta betalnings-autentisering uteslutande från vad konsumenterna vet (dvs. lösenord) – till vad de har (t.ex. mobiltelefoner) och vem de är (dvs. biometri, exempelvis fingeravtryck) för att göra shopping-upplevelsen säkrare och enklare.

Hur sker implementering av Mastercard® Identity Check™ på övergripande nivå (som kodning, systemändringar etc.)?

Mastercard Identity Check innehåller vägledning och specifika krav för handlare och kortutgivande banker. Kortutgivande banker måste tillhandahålla kortinnehavaren med en av de verifikationsmetoder som krävs av programmet – såsom dynamiskt lösenord, biometrisk identifikation eller liknande metoder för att höja säkerheten och uppnå en användarvänlig upplevelse.

På handlare och PSP:er ställs specifika krav, såsom att alltid tillhandahålla ett Accountholder Authentication Value (AAV) för varje transaktion.

Kortutgivande banker och handlare måste även följa programmets nyckelindikationer som bland annat omfattas av:

- Ett årligt tak för autentiserade transaktioner som utsatts för bedrägeri.
- Att deras lösning har en lägsta nivå för godkända transaktioner.
- Krav på delning av autentiseringsdata.

För mer information, besök Mastercard Connect och läs Mastercards 'Global Operation Bulletin' och 'Program Guide'.

Vilka transaktioner påverkas av Mastercard® Identity Check™?

Mastercard Identity Check är utformat för att stödja alla Mastercards varumärken (Mastercard, Maestro, etc.) inom samtliga segment (konsument och kommersiellt) och produkter (kreditkort, debitkort och pre-paid-kort).

Förekommer det några förändringar gällande ansvar (Liability Shift) och interchange-kostnader?

Samtliga inlösare som är verksamma inom Europa bär ansvar för transaktioner där undantag från SCA tillämpats. Detta är oavsett om en handlare skickar med EMV 3DS-data i transaktionen eller inte.

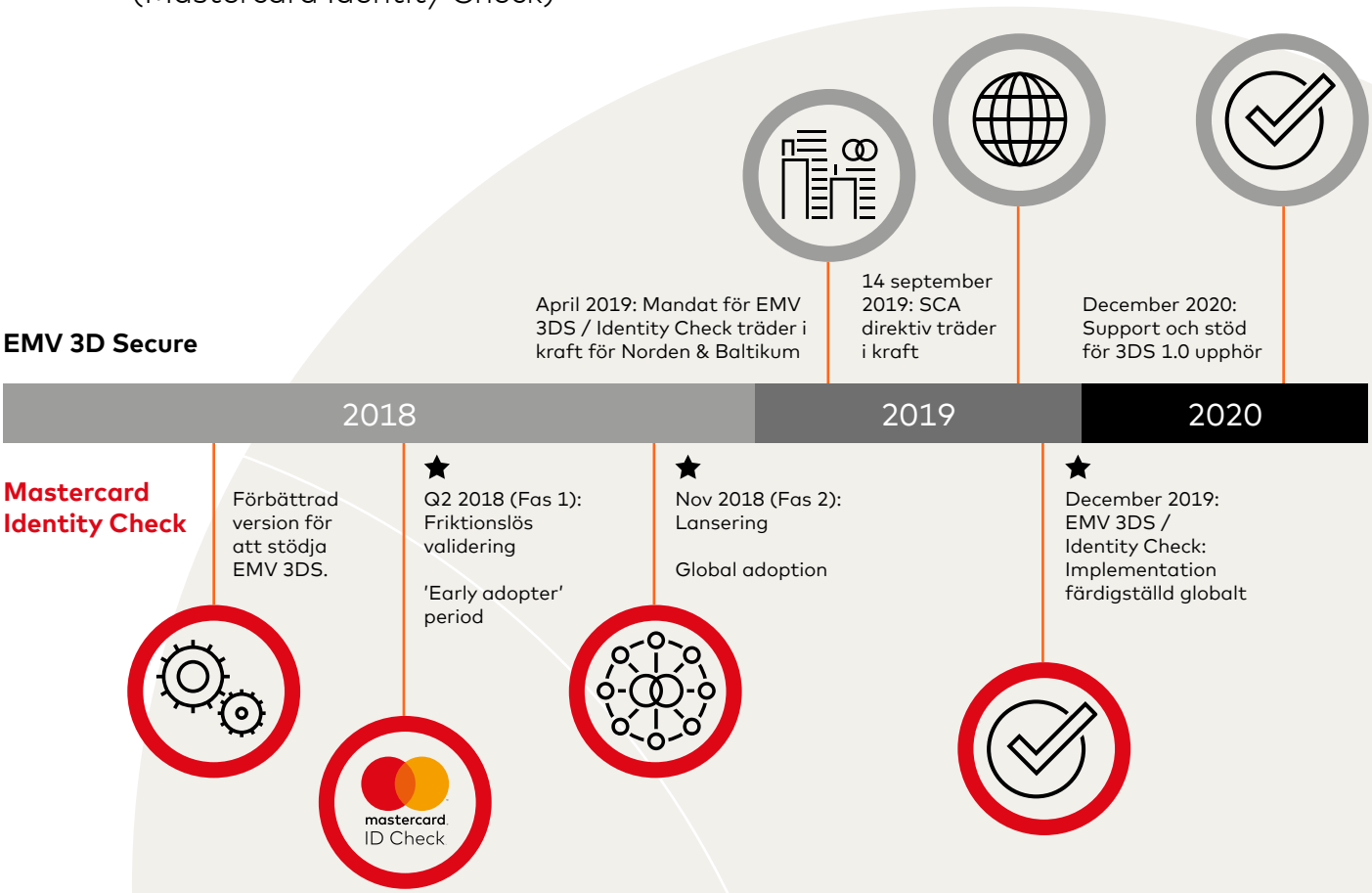
mastercard

Hur ser tidslinjen ut för kortutgivande banker, handlare och inlösare?

Den nya standarden, EMV 3DS, kommer initialt användas samtidigt som 3DS 1.0 för att göra övergången så smidig som möjligt. På detta sätt kan kortutgivande bankers ACS-leverantörer både hantera transaktioner från handlare som använder den gamla versionen (3DS 1.0) och handlare som använder den nya versionen (EMV 3DS). Tack vare detta, kan kortutgivande banker och handlare skräddarsy sin lösning efter egna affärsmål och tidsplaner.

Mastercard kommer att fortsätta jobba med samtliga aktörer och tjänsteleverantörer på den globala marknaden för att stödja övergången på bästa sätt. Tidsplanen här nedan syftar till att hjälpa olika aktörer planera sin utrullning av EMV 3DS.

Tidslinje: Övergång från 3DS 1.0 (SecureCode) till EMV 3DS (Mastercard Identity Check)



För att säkerställa funktionaliteten mellan 3DS 1.0 och EMV 3DS, krävs det att 3DS-servrar och ACS-leverantörer supporterar både 3DS 1.0 och EMV 3DS tills support och stöd för 3DS 1.0 (SecureCode) upphört.

- 3DS-servrar (tidigare känt som MPI) ska byggas så att de kan supportera både 3DS 1.0 och EMV 3DS för handlare.
- ACS-leverantörer ska bygga stöd för både 3DS 1.0 och EMV 3DS för kortutgivande banker.
- Kortutgivande banker ska supportera 3DS 1.0 och EMV 3DS för alla kortmodeller (kreditkort, debitkort och pre-paid-kort).

mastercard

Undantag för SCA: När och hur kan dessa tillämpas?

RTS tillåter kortutgivande banker och inlösare att tillämpa följande undantag för betalningar online:

- För transaktioner där summan är 30 euro* eller mindre. Detta undantag kräver dock SCA för var sjätte transaktion eller om den kumulativa summan är högre än 100 euro* sedan den senaste SCA-transaktionen.
- Vid återkommande transaktioner där beloppet och konsumenten är densamma. SCA krävs alltid när en konsument registrerar sitt kort för återkommande transaktioner (första transaktionen). Efterföljande transaktioner ska alltid innehålla en referens till den första betalningen men kräver ingen SCA.
- När kortutgivande bank tillämpar en riskanalys. Detta kan göras på transaktioner som överensstämmer med den summa och bedrägerinivå som definierats av RTS. Ett exempel på ovan är när en betalning genomförs av en kortinnehavare som inte påvisat tidigare bedrägeririsk, genomför transaktionen från en enhet som använts tidigare, för ett belopp som är under 100 euro* och där inlösarens bedrägerinivå inte överstiger 13 räntepunkter (basis points).
- För transaktioner hos handlare som kortinnehavaren satt på en "whitelist" som en betrodd handlare, krävs endast SCA vid skapande och ändringar av denna "whitelist". Det är bara kortutgivande banker som kan tillämpa detta undantag. Om inte inlösaren tillämpar ett undantag för SCA är den kortutgivande banken ansvarig för ev. bedrägerier om en auktorisation godkänts, förutsatt att handlaren skickat en autentiseringsförfrågan för transaktionen.

Från och med den 14 september bör handlare använda EMV 3DS autentisering, såvida inte undantag från inlösare gäller. Om en handlare/inlösare använder sig av ett undantag som godkänns av kortutgivande bank, berörs inte kortinnehavaren (dvs. kortinnehavaren behöver inte autentisera sig ytterligare vid online-betalning).

Auktoriserade transaktioner utan att autentisering är tillåtna enligt PSD2 RTS i de fall ett undantag från inlösare tillämpas, dock har dessa ofta en lägre godkännandegrad.

Vilka är de främsta åtgärderna som handlaren måste genomföra?

1. Den av handlaren valda PSP (Payment Service Provider/betalväxel) ska implementera och hantera gränssnittet, åt handlaren, för autentisering genom EMV 3DS och 3DS 1.0 (som 'fallback' om den kortutgivande banken ännu inte tillämpar EMV 3DS).
2. Handlaren behöver förbereda sig på att hantera en ökad mängd transaktions- och konsumentdata (adress, e-mail, mobilnummer eller enhets ID) och skicka det vidare till sin PSP. Det kan kräva kodning av ett nytt API eller liknande som förses av PSP. Handlaren ska försäkra sig om att deras kundvillkor stämmer överens med exempelvis GDPR kring lagring och delning av data.
3. Handlaren måste implementera en autentiseringspolicy, i linje med vald PSP och inlösare, som stödjer RTS och dess undantagsregler. Speciellt kring TRA-undantag (Transaction Risk Analysis) och motsvarande tillämpade bedrägerinivåer.
4. Handlaren måste säkerställa att deras inlösare registrerar dem för EMV 3DS hos kortbolagen.

5. Handlaren måste göra uppdateringar på hemsidan för att stödja EMV 3DS, RTS och Mastercard® Identity Check™. En av dessa uppdateringar är att lägga in Mastercards logotyp för Mastercard Identity Check.
6. Om en handlare begär undantag för SCA, via inlösaren, utan autentisering och transaktionen nekas av den kortutgivande banken (särskilt vid andra orsaker än finansiella eller tekniska avbrott), ska det finnas en automatiserad lösning för att en autentisering via EMV 3DS tillämpas. Om den godkänns ska ytterligare en auktorisation genomföras. Liknande gäller om kortutgivaren ännu inte stödjer EMV 3DS, då skall handlaren använda 3DS 1.0 som 'fall back'.
7. Handlaren måste säkerställa att deras företagsnamn är unikt och att det används konsekvent i transaktionsflödet med inlösare och PSP. Genom detta får de bäst möjlighet att använda sig av inlösarens undantag från SCA.
8. Handlaren rekommenderas att alltid begära en autentisering, speciellt för kortutgivande banker som avvisar transaktioner där en autentisering tidigare inte genomförts.
9. Integrera funktioner från EMV 3DS för att erbjuda en optimal, in-app, kundupplevelse i samband med autentisering, och för att behålla samma användargränssnitt under hela betalningsflödet.
10. Handlaren skall skicka autentiseringsförfrågan i enlighet med SCA för den initiala transaktionen i samband med att kunden kopplar kortet till återkommande betalningar (recurring payments). För att återkommande betalningar skall godkännas utan att kunden behöver autentisera sig, skall handlaren skicka en förfrågan till kortutgivaren enligt EMV 3DS med hänvisning till den initiala SCA-godkända transaktionen.
11. I samband med återkommande betalningar där beloppen kan variera i storlek, eller för en betalning där det slutgiltiga beloppet är okänt, skall handlaren tydligt kommunicera samt förklara anledningen för kortinnehavaren, till varför det initiala autentiserade beloppet kan skilja sig från det slutgiltiga.

För mer information, vänligen kontakta er PSP eller inlösare.

mastercard

Ordlista:

Accountholder Authentication Value (AAV) – är ett cryptogram/kvitto som bevisar att en online-betalning har blivit autentiserad.

ACS Provider – Access Control Server. Tredjepartsleverantör av EMV 3DS lösningar.

Credential-on-file (COF) – Teknik som innebär att kortinnehavaren inte behöver ange sina betalningsuppgifter vid varje köp, istället sparas de hos handlaren/PSP.

EMV 3DS – EMVCo:s standard som har tagits fram för att öka säkerheten vid online-betalningar. Mastercard® Identity Check™ bygger på detta protokoll.

EMVCo – branschorganisation som säkerställer acceptans av säkra betaltransaktioner.

In-app-betalning – Betalning som sker utan att köparen behöver lämna handlarens mobila applikation.

PSD2 RTS – EU:s andra betaltjänstdirektiv som utkom i början av 2018. Begreppet står för "Payment Services Directive 2 Regulatory Technical Standards".

PSP – Payment Service Provider, även kallad betalväxel och är företag som förmedlar betaltjänster.

RBA – Risk Based Authentication – Riskbaserad autentisering är ett autentiseringssystem hos kortutgivande bank som tar hänsyn till kortinnehavarens transaktionshistorik för att bestämma riskprofilen som är associerad med transaktionen.

SCA – Strong Costumer Authentication eller "stark kundautentisering".

Tokenisering – Teknik som tillåter betalningar utan att avslöja kortuppgifterna. I stället för att kortnumret används, skapas ett unikt digitalt nummer som bara kan användas med en viss enhet eller hos en viss handlare.

Whitelist – En lista över de handlare som är betrodda av kortinnehavaren och som därför inte kräver lika hög autentiseringskontroll.

mastercard