

.....

Eenvoudig veiliger betalen

Een korte inleiding over de
nieuwe Europese richtlijn voor
sterke klantauthenticatie

Worldline

Samenvatting

In het jaar 2020 zal e-commerce in Europa voorgoed veranderen. Vanaf die dag zijn banken namelijk wettelijk verplicht om sterke klantauthenticatie (Strong Customer Authentication - SCA) te ondersteunen bij het verwerken van e-commerce-betalingen in heel Europa.

Op grond van de tweede richtlijn inzake betalingsdiensten (PSD2¹) moeten banken nu meer informatie van consumenten verzamelen dan uitsluitend hun naam, kaartnummer en kaartvalidatie code (CVC, CVV).

Organisaties en hun Payment Service Providers (PSP's) moeten bij kaartbetalingen in staat zijn om de identiteit van klanten te controleren op basis van het 3DS2.0-protocol (3-D Secure) dat een reeks technologieën ondersteunt variërend van eenmalige, tijdelijke wachtwoorden tot vingerafdrukken en gezichtsherkenning. Indien SCA en 3DS2.0 niet door de PSP van een onderneming worden ondersteund, kunnen transacties door de bank van een klant geweigerd worden.

Slim, simpel en soepel

Het is begrijpelijk dat veel bedrijven zich zorgen maken over het mogelijke effect van deze eisen op hun conversies. Deze nieuwe regels verkleinen echter niet alleen het risico op online-fraude, maar maken het voor klanten eenvoudiger om online-aankopen te doen. Dankzij de technische EU-normen² voor de implementatie van PSD2 beschikken online-shoppers over een veiligere en meer gebruiksvriendelijke omgeving, met name wanneer zij gebruik maken van hun smartphones. Overigens hoeven veel transacties met een lage waarde en periodieke betalingen niet aan de nieuwe eisen te voldoen. De aanvullende verificaties zijn bijvoorbeeld voor de meeste online-transacties onder de € 30,- niet vereist. Een intelligente, op risico's gebaseerde authenticatie leidt daarnaast tot

minder verstoringen in het betalingsverkeer. Wanneer kaarthouders het verzoek krijgen om hun identiteit aan te tonen, worden zij niet langer naar een andere website doorgelinkt om hun gegevens in een nieuw betaalfenster in te voeren. Klanten kunnen hun identiteit nu aantonen als integraal onderdeel van het controleproces waardoor het risico wordt verminderd dat zij de transactie afbreken.

De tijd dringt

De Europese Bankautoriteit heeft de nationale toezichthouders aanbevolen om na 14 september 2019 een overgangperiode in te stellen zodat alle marktpartijen meer tijd hebben om op de nieuwe omgeving over te stappen. Uiteraard heeft een dergelijke overgangperiode altijd een tijdelijk karakter. Organisaties moeten er dan ook nu al voor

zorgen dat hun PSP's aan de authenticatievereisten voldoen. Bovendien moeten organisaties ook hun modellen voor online-betalingen evalueren en hun controleprocedures herzien om niet alleen de stappen te integreren die nodig zijn om 3DS2.0 te ondersteunen, maar ook met het oog op een effectievere authenticatie en een betere klantervaring. De nieuwe regels lijken weliswaar ingrijpend, maar als zij op de juiste manier en met de benodigde expertise worden geïmplementeerd, wordt online-shopping veiliger en gebruikersvriendelijker. Dat kan zowel tot hogere conversiepercentages als grotere e-commercevolumes in heel Europa leiden.

¹ Richtlijn 2015/2366/EU (PSD2)

² Verordening (EU) 2018/389 - Technische reguleringsnormen voor een sterke klantauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden

Veiliger online-shoppen

Veel e-commerce bedrijven in Europa kennen de klantauthenticatie die bekend staat onder de naam 3-D Secure 1.0. Deze procedure, ontwikkeld door de grote betaalkaartmaatschappijen, verwijst kaarthouders naar externe webpagina's. Om hun identiteit aan te tonen, moeten klanten een code of wachtwoord invoeren die gemakkelijk vergeten kan worden.

Dit proces kan leiden tot een hoog aantal klanten die transacties alsnog afbreken en is ook niet echt geschikt voor transacties met smartphones. Dit protocol is dan ook gematigd enthousiast ontvangen door de Europese detailhandel: veel organisaties hebben zelfs besloten om het protocol helemaal niet te implementeren.

Na de inwerkingtreding van de SCA-vereisten van PSD2 kan 3DS echter niet langer door de organisaties genegeerd worden. Kaartuitgevende instanties kunnen online-betalingen die niet middels 3DS zijn gecontroleerd namelijk weigeren. Organisaties die zich zorgen maken over deze ontwikkeling, kunnen echter gerust zijn: er is hulp in aantocht in de vorm van 3DS2.0. Dit is een modern protocol dat volledig aan de nieuwe voorschriften voldoet en afgestemd is op de huidige en toekomstige marktvereisten met het oog op een veiligere en prettige gebruikerservaring.

Geïntegreerde veiligheid

3DS2.0 is specifiek door de betaalkaartmaatschappijen ontworpen om niet alleen de veiligheid van online-betalingen te vergroten, maar om ook de klanttevredenheid te verbeteren, met name bij aankopen via smartphones, via een app of bij het gebruik van digitale portefeuilles. Hierdoor krijgt de authenticatie van kaarthouders een veiliger en duidelijker karakter. Wat die veiligheid betreft, maakt 3DS2.0 in overeenstemming met de SCA-vereisten

gebruik van een authenticatie op basis van twee factoren. Een statisch wachtwoord is niet meer afdoende. Klanten moeten hun identiteit aantonen door middel van twee van de volgende drie elementen:

Kennis



Iets wat de klant weet (bijv. een wachtwoord, pincode of antwoord op geheime vraag)

Bezit



Iets wat de klant bezit (Bijv. een smartphone, token of horloge)

Eigenschap



Iets wat uniek is voor de betreffende klant (bijv. een vingerafdruk, de stem of iris- of gezichtsherkenning)

Een technologie die op dit moment veel gebruikt wordt om authenticatie op basis van twee factoren mogelijk te maken, is het tijdelijke One-Time Password (OTP - eenmalig wachtwoord) dat naar een apparaat van de klant wordt gestuurd, zoals een mobiele telefoon, een veiligheids-ID of een draagbaar iets (zoals een smartwatch). Naar verwachting zal voor een veilige authenticatie in de toekomst op grote schaal gebruik worden gemaakt van identificatie op basis van unieke biometrische eigenschappen. Veel banken in Europa zetten op dit moment vaart achter de ontwikkeling van deze intuïtieve, gebruikersvriendelijke technologieën die

ook ondersteund worden door 3DS2.0 (maar niet door 3DS1.0). Het geavanceerde 3DS2.0 betekent ten opzichte van de vorige versie ook een aanzienlijke verbetering in de gebruikerservaringen. Wanneer een twee-factoren-authenticatie vereist

is, integreert 3DS2.0 het identificatieproces in de checkout-fase van een website of mobiele app van een organisatie zodat het niet meer nodig is om een klant naar een andere site e.d. door te linken. Hoewel 3DS1.0 in de huidige vorm in overeenstemming is met de SCA-vereisten, zal deze versie naar verwachting eind 2020 uitgefaseerd worden. Alle kaartuitgevende instanties en organisaties moeten dan gebruik maken van 3DS2.0. Veel betalingspartijen zijn nu al bezig met de overstap naar de meest recente versie om verstoringen te minimaliseren en de risico's terug te dringen dat kaarthouders hun transacties alsnog afbreken.

Soepele procedure

Een belangrijk uitgangspunt van de nieuwe SCA-eisen is dat kaarthouders uitsluitend hun identiteit hoeven aan te tonen bij online-transacties met een hoger risico op fraude. Op transacties zoals e-mailbestellingen, telefonische bestellingen en transacties buiten de Europese Economische Unie zijn de nieuwe voorschriften niet van toepassing. Betalingen die op initiatief van een bedrijf met toestemming van de kaarthouders geïnd worden (zoals betalingen aan nutsbedrijven) vallen eveneens buiten het toepassingsgebied van de SCA. Daarnaast zullen veel transacties van de nieuwe voorschriften vrijgesteld worden op basis van een analyse van de gegevens die een bedrijf met de kaartuitgevende instantie heeft uitgewisseld.

Transacties met een laag risico kunnen in aanmerking komen voor een breed scala aan vrijstellingen van de twee-factoren-authenticatie. Daartoe behoren o.a.:

- **Transacties met een lage waarde.** Transacties op afstand met een waarde van minder dan € 30,- zijn vrijgesteld, tenzij de totale waarde meer dan € 100,- bedraagt of wanneer er in totaal vijf of meer transacties plaatsvinden.
- **Analyse van het transactierisico.** Er kan een vrijstelling worden verleend op basis van het gemiddelde fraudepercentage van de acquirer (verwerker van de betalingen) en de kaartuitgevende instantie. Naarmate het fraudepercentage lager ligt, kunnen er grotere transacties worden uitgevoerd zonder dat de SCA-eisen van toepassing zijn.
- **'White List' met organisaties en te vertrouwen begunstigen.** Transacties met een organisatie kunnen voor een vrijstelling in aanmerking komen nadat een klant de betreffende organisatie als te vertrouwen aan een 'witte lijst' heeft toegevoegd.
- **Periodieke betalingen, zoals abonnementen.**
- **Betalingen door bedrijven (B2B transacties).**

Met betrekking tot al deze vrijstellingen kunnen organisaties profiteren van de zogeheten 'soepele procedure'. Online-betalingen voor dergelijke transacties worden automatisch goedgekeurd zonder dat de klanten hun identiteit hoeven te bevestigen. 3DS2.0 wordt pas operationeel bij transacties waarop deze vrijstellingen niet van toepassing zijn.

Leveranciers kunnen deze vrijstelling uitsluitend samen met hun PSP en acquirer aanvragen. De kaartuitgevende instantie heeft de eindverantwoordelijkheid wat het al dan niet toekennen van vrijstellingen betreft. Overigens kunnen kaartuitgevende instanties altijd een sterke klant-authenticatie eisen, ook wanneer de verwerker van de betalingen heeft verzocht om een vrijstelling op basis van de analyse van het transactierisico.

De vrijstelling op basis van de analyse van het transactierisico is voor organisaties van belang, omdat hierdoor minder snel aan de SCA-vereisten voldaan hoeft te worden. Daardoor neemt de kans ook af dat klanten transacties bij de controle van de betalingsgegevens afbreken. Bovendien kunnen banken bij lagere fraudepercentages organisaties vaker gebruik laten maken van de soepele procedure, hetgeen voor acquirers een extra argument kan zijn om het niveau van hun online-beveiliging te verbeteren.



Wat wordt er van organisaties verwacht?

Ongeacht de duur van de overgangperiode zoals die door de nationale toezichthouders wordt vastgesteld met het oog op de volledige implementatie van de nieuwe voorschriften, verdient het aanbeveling dat online-ondernemingen zich nu al voorbereiden op de sterke klantauthenticatie en 3DS2.0.

Allereerst moeten organisaties contact opnemen met hun PSP's om te informeren of zij minimaal 3DS1.0 voor SCA ondersteunen en aan de vereisten van deze nieuwe richtlijn voldoen. Indien een PSP SCA niet ondersteunt, is het mogelijk dat een kaartuitgevende instanties transacties van een organisatie weigert die niet geauthenticeerd zijn.

Hoewel 3DS1.0 vooralsnog aan de SCA-vereisten voldoet, dient een PSP ook over een migratieplan te beschikken waardoor organisaties gebruik kunnen maken van 3DS2.0 op het moment dat het verbeterde protocol door banken wordt ondersteund. De PSP's moeten daarnaast toelichten wat de gevolgen van de nieuwe vereisten voor ondernemers zijn en welke maatregelen zij nemen om de SCA-vereisten integraal in acht te nemen.

Daarnaast moeten organisaties ook met hun PSP's en acquirers over de vrijstellingsregels overleggen en afspreken welke vrijstellingen aangevraagd worden om optimaal gebruik te kunnen maken van de soepele procedures. Het beheer van die vrijstellingen is van essentieel belang bij het opnieuw vormgeven van de online-betalingsprocessen en bij het vergroten van het vertrouwen van de kaarthouders.

Indien een acquirer die vrijstellingen niet namens een organisatie aanvraagt, kunnen kaartuitgevende instanties voor alle online-transacties waarop de nieuwe voorschriften van toepassing zijn alsnog een sterke authenticatie verlangen. Dat zou van negatieve invloed kunnen zijn op de conversiepercentages van ondernemers.

Door een nauwe samenwerking met hun PSP's en acquirers kunnen ondernemers het aantal authenticatieverzoeken van kaartuitgevende instanties minimaliseren en zo optimaal gebruik maken van de soepele procedure. Aangezien verschillende markten en banken de voorschriften tijdens de overgangperiode op een andere manier kunnen interpreteren, is het op dit moment voor de ondernemers van belang dat zij een nauwe samenwerking met hun PSP's en acquirers aangaan.



Een nieuwe kijk op betalingen

De ondernemers zelf moeten hun betalingsprocessen en -stromen evalueren om van deze veranderingen te profiteren en de ervaringen van hun gebruikers te verbeteren. Wellicht dat zij nieuwe API's moeten implementeren om optimaal gebruik te maken van 3DS2.0. Indien een bank een sterke authenticatie voor een transactie verlangt, moet een organisatie voorbereid zijn om SCA zo gestroomlijnd mogelijk te ondersteunen om het ongemak voor online-shoppers te minimaliseren.

Daarnaast kunnen ondernemers de kans benutten om hun eindgebruikers op de hoogte te stellen van de voordelen die hen in de toekomst te wachten staan bij het online-betalen.

Alle partijen in het betalingsecosysteem, van banken en PSP's tot ondernemers, moeten ervoor zorgen dat de e-commercemarkt zich zo soepel mogelijk aan de nieuwe voorschriften aanpast.

Op de lange termijn leiden de SCA en 3DS2.0 namelijk tot minder fraude in de e-commerce, een groter vertrouwen van kaarthouders en meer gebruiksgemak. Dankzij een eenvoudiger en veiliger betalingsproces mogen ondernemers na de implementatie van de nieuwe regels op hogere conversiepercentages rekenen.

Worldline: ready to deliver

Worldline was één van de eerste betaalproviders in Europa die 3-D Secure 2-transacties verwerkte.

In het vierde kwartaal van 2018 lanceerden we bij Worldline een samenwerkingsproject met banken, betaalschema's en een selecte groep bedrijven. In mei 2019 startte een testfase waarin reële verrichtingen geauthenticeerd werden met 3-D Secure 2.

Dankzij onze betaaloplossing kunnen we elektronisch transacties beveiligen en beheren en streven we ernaar de voorkeurspartners te zijn voor bedrijven die vrijstellingen willen beheren, een vlotte verwerking zoeken en de online gebruikerservaring willen verbeteren.

Onze experts hebben de afgelopen jaren hun kennis en praktische ervaring op dit gebied gedeeld in een reeks workshops met bedrijven, betaalproviders en banken. Daarin leggen ze uit hoe betaalplatformen effectief 3-D secure 2 kunnen toepassen. We werken al samen met een groeiend aantal bedrijven van allerlei omvang om aan de nieuwe voorschriften te voldoen.

Onze experts staan klaar om alle bedrijven te helpen deze uitdagingen met succes aan te gaan, zodat ze kunnen profiteren van online betaalprocessen die veiliger, slimmer en gemakkelijker in gebruik zijn. Met onze producten bent u voorbereid op de nieuwe vereisten van klantauthenticatie en profiteert u van alle toepasselijke vrijstellingen.

Over Worldline

Met het bieden van de juiste betaalmogelijkheden verhogen ondernemers hun conversie en verkoop. In een snel veranderende markt biedt Worldline oplossingen die klaar zijn voor de toekomst en die meerwaarde bieden aan ondernemers. Door het leveren van innovatieve oplossingen kunnen klanten veilig, gemakkelijk en overal op de door hen gewenste manier betalen. Worldline biedt een compleet aanbod van omnichannel oplossingen, internetkassa's, betaalautomaten, betaalkaartacceptatie, cadeaukaarten en loyalty diensten, kortom een one-stop shop voor uw volledige betalingsverkeer. Met ruim 45 jaar ervaring is Worldline de Europese marktleider in betaaloplossingen en betaalautomaten.