

Değerli İş ortaklarımız,

Ödeme.keas sayfamızda yapılan kredi kartlı çekimlerinizde 3D uygulaması 2018 yılına kadar zorunlu olup 2018 yılının 3. çeyreğinde 3D uygulaması sizlerden gelen talepler neticesinde seçilebilir hale getirilmiştir.

Ancak son zamanlarda yapılan itirazlarda yaşanan kart kopyalama sorunları ile karşılaştığımız için 3D güvenlik kullanımının önemi hakkındaki bilgilendirmemizi sizlerle paylaşmak isteriz.

Bankaya yapılan itirazlarda;

- 3D kullanılmaması durumunda “**haberim olmadan işlem yapıldı**”, “**ben yapmadım**” “**benim onayım olmadan işlem yapılmış**” gibi kart sahibinin bankaya itirazında karta iade işlem süreci sizlere bilgi verilerek başlatılmaktadır.
- Kart sahibi ödeme yapıp hizmet alamıyorsa Tüketici kanunu gereği iade süreci sizlere bilgi verilerek başlatılmaktadır.
- Yukarıda sayılan itiraz nedenlerinde Bankaya belge sunabilmemiz için kart sahibinden **ıslak imzalı ödeme talimat formu, slip, makbuz, fatura vb** belgelerin temin edilmesi gerekmektedir.
- Bu tür itirazlarda sorumluluk Bayilerimize aittir.

Kredi kart çekimlerinizde güvenirliliğinden emin olmadığınız durumlarda 3D şifre kullanmanızı önemle rica ederiz.

3D kullanılsın veya kullanılsın güvenliğiniz için ıslak imzalı fatura, makbuz, talimat formu vb. belgenin temin edilip tarafınızca saklanmasını rica ederiz.

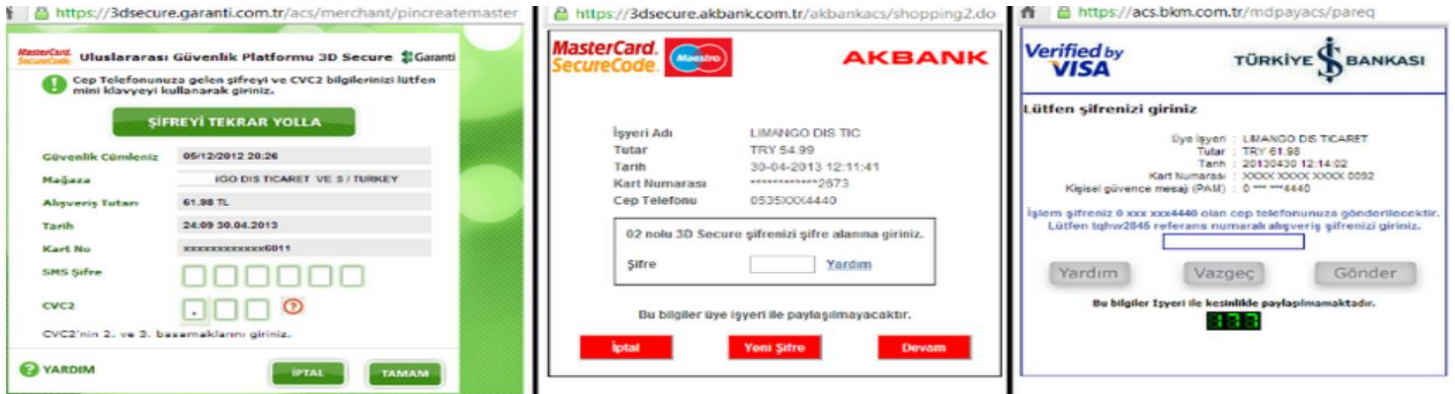
3D Secure (Güvenli Alışveriş) Nedir?

Web siteleri üzerinden, kredi kartı ile yapılan ödemelerde kart sahibinin kart güvenliğini sağlamak amacıyla bankaların firmalar ile yaptığı ortak çalışmaya 3D Secure denir.

3D Secure, çalıntı bir kredi kartı ile yapılacak alışverişleri rahatlıkla önler. Sebebi de kart sahibinin telefonuna onay sms bilgisi gönderilerek ödemenin tamamlanmasıdır.

3D sistemi sayesinde kart, 3. şahısların eline geçse bile sistem mesajı kart sahibinin bankaya bildirdiği cep telefonu numarasına yollayacağı için karttan herhangi bir çekim yapılamayacaktır. Yani bu şifreyi bilmeyen birinin kartı kullanması mümkün değildir.

Aşağıda Örnek 3D Secure Ekranlarını Görebilirsiniz:



The image displays three examples of 3D Secure authentication screens:

- Garanti (Left):** Shows a 'ŞİFREYİ TEKRAR YOLLA' button and a form with fields for 'Güvenlik Cömendizi', 'Mağaza', 'Alışveriş Tutarı', 'Tarih', 'Kart No', 'SMS Şifre', and 'CVC2'. A 'YARDIM' button is at the bottom left.
- Akbank (Middle):** Shows a form with fields for 'İşyeri Adı', 'Tutar', 'Tarih', 'Kart Numarası', and 'Cep Telefonu'. A '02 nolu 3D Secure şifrenizi girfe alanına giriniz.' section has a 'Şifre' input field and a 'Yardım' button. At the bottom are 'İptal', 'Yeni Şifre', and 'Devam' buttons.
- Türkiye İş Bankası (Right):** Shows a 'Lütfen şifrenizi giriniz' section with a form containing 'Üye İşyeri', 'Tutar', 'Tarih', 'Kart Numarası', and 'Kişisel güvence mesajı (PAM)'. A 'İşlem şifrenizi 0 xxx xxx4440 olan cep telefonunuza gönderecektir. Lütfen lghw2845 referans numaralı alışveriş şifrenizi giriniz.' message is present. At the bottom are 'Yardım', 'Vazgeç', and 'Gönder' buttons.

Saygılarımızla.

KEAS