

1. 3-D İşlem Nedir?

Geliştirilmesi VISA tarafından yapılan ve MasterCard tarafından da kabul edilmiş olan 3D Secure protokolü, üye işyeri-banka-kart sahibi arasındaki sorumlulukları düzenleyen bir modeldir.

3D Secure protokolü, kartın işlem yapan kişiye ait olduğunu doğrulamak amacı ile geliştirilmiştir. Kart kullanıcısı tarafından ek bilgiler girilerek kontrolü sağlanır.

2. 3-D İşlem Neden Gerekli?

İşlem güvenliğinin sağlanması ve kart sahibinin teyidi için 3D işlem olanağı sağlamak, kart sahibi doğrulayacağından dolayı, e-ticarete sıkça karşılaşılan sahtekârlık olaylarını azaltarak kart sahibini ve üye işyerini güvence altına alır. 3D işlem yapabilmek için VISA ve MasterCard 3D üye işyeri

olunması gerekmektedir. Bu üyelik bankaya başvurunuz sonrasında otomatik olarak sağlamaktadır.

2.1. Kart sahipleri için faydaları

- İnternet üzerinden yapılan alışverişler de kart sahibi güvenin artması
- Kullanım için ekstra bir yazılıma ihtiyaç duyulmaması
- Kullanımının kolay olması
- Online alışverişlerde kart üzerinde kontrol sağlaması

2.2 Üye işyerleri faydaları

- Mağaza tarafından kullanılan e-ticaret yazılımlarına kolayca entegre edilebilmesi.
- Sahtekarlık riskini büyük oranda azaltması
- Müşteri ile mağaza arasındaki etkileşimi minimuma indirmesi
- Geri ödemelerde sorumluluğu mağazalardan bankalara geçirmesi

3. 3DHOST Model

Üye işyerinin SSL sertifikası bulunmuyorsa veya bu sertifika banka tarafından kabul edilmemişse ya da üye işyeri kart bilgilerini kendi sisteminde almak istemiyorsa bankanın sağladığı bir sayfa üzerinden 3-D işlem yapılır ve işlem gerçekleştirildikten sonra üye işyerine dönüş yapılır.

3D Host entegrasyon modelini ,diğer modeller olan 3D ve 3D Pay modellerinden en büyük farkı üye işyerinin kart sahibinin bilgilerini almasına gerek yoktur. Sistem tarafından ödeme işleminin gerçekleştirileceği kartı bilgilerinin alınacağı sayfa harici olarak açılmaktadır.Üye işyeri kendi bilgilerini ve alışveriş bilgilerini post etmesi yeterlidir.

Payfor sanalpos sistemine 3DHOST yapısını kullanarak dahil olmak isteyen üye işyerlerimizi,aşağıdaki parametreler üzerinden kart doğrulaması yapılabilir.

Detaylı bilgi için kod örneklerimiz içerisinde yer alan **Payfor3Dhost & Payfor3DHostPayment** specleri kontrol edilmelidir.

MbrId = "" /Kurum Kodu
MerchantID = "" /Language_MerchantID (Vpos test ekibi tarafından paylaşılacaktır.)
MerchantPass = "" /Language_MerchantPass (Vpos test ekibi tarafından paylaşılacaktır.)
UserCode = "" /Kullanici Kodu(Vpos test ekibi tarafından paylaşılacaktır.)
UserPass = "" /Kullanici Sifre(Vpos test ekibi tarafından paylaşılacaktır.)
SecureType = "3Host" /Language_SecureType
TxnType = "Auth" /Islem Tipi
InstallmentCount = "0" /Taksit Sayisi
CurrencyCode = "{CurrencyCode}" /Para BirimiCode
OkUrl = "" /Language_OkUrl(Başarılı işlemin yönlendirilmesini istediğini web sayfanın adresi)
FailUrl = "" /Language_FailUrl(Başarısız işlemin yönlendirilmesini istediğini web sayfanın adresi)
OrderId = "" /Siparis Numarasi
PurchAmount = "1" /Tutar
Lang = "TR" /Language_Lang

Üye işyeri tarafından güvenlik kontrolü amacı ile bir hash değeri oluşturulması gerekmektedir.

Bu hash değerinin aşağıdaki sıra ile sha1 formatında üretilmesi gerekmektedir.

String hash = MbrId + OrderId + PurchAmount + OkUrl + FailUrl + TxnType + InstallmentCount + Rnd + MerchantPassword;

Örnek Hidden Yapısı

```
<input type="hidden" name="MbrId" value="<%=MbrId%>">
```

```
<input type="hidden" name="MerchantID" value="<%=MerchantID%>">
```

```
<input type="hidden" name="UserCode" value="<%=UserCode%>">
```

```
<input type="hidden" name="UserPass" value="<%=UserPass%>">
```

```
<input type="hidden" name="SecureType" value="<%=SecureType%>">
```

```
<input type="hidden" name="TxnType" value="<%=TxnType%>">
```

```
<input type="hidden" name="InstallmentCount" value="<%=InstallmentCount%>">
```

```
<input type="hidden" name="Currency" value="<%=Currency%>">
```

```
<input type="hidden" name="OkUrl" value="<%=OkUrl%>">
```

```
<input type="hidden" name="FailUrl" value="<%=FailUrl%>">
```

```
<input type="hidden" name="OrderId" value="<%=OrderId%>">
```

```
<input type="hidden" name="PurchAmount" value="<%=PurchAmount%>">
```

```
<input type="hidden" name="Lang" value="<%=Lang%>">
```

```
<input type="hidden" name="Rnd" value="<%=rnd%>">
```

```
<input type="hidden" name="Hash" value="<%=hash%>">
```

4. 3D Secure Response Hash kontrolü edilmesi !!!

Ödeme işlemi sonrasında EndPoint kontrolü için MerchantPass değeri ve diğer parametreler belirli bir sırada olacak şekilde yeni bir hash hesaplanmaktadır ve Finansbank sanalpos sistemi tarafından iletilen response hash değeri ile karşılaştırma yapılarak cevabın VPOS'tan geldiği doğrulanmaktadır.

MerchantPass değeri bildiğiniz üzere istek mesajında yer almamaktadır.

Merchantpass değerinin saklanması ve korunması üye işyerinin sorumluluğundadır.

Sonuç sayfası betiğinde EndPoint kontrolü gerçekleştirebilmek için kullandığımız ResponseHash aşağıda yer almaktadır.

Response Hash hesaplama parametreleri

- MerchantID
- MerchantPass
- MrcOrderId
- AuthCode
- ProcReturnCode
- 3DStatus
- ResponseRnd
- UserCode

String str = MerchantID + MerchantPass + OrderId + AuthCode + ProcReturnCode + 3DStatus+ResponseRnd+UserCode ;

```
System.Security.Cryptography.SHA1 sha = new System.Security.Cryptography.SHA1CryptoServiceProvider();  
byte[] bytes = System.Text.Encoding.UTF8.GetBytes(str);  
byte[] hashingbytes = sha.ComputeHash(bytes);  
String ResponseHash = Convert.ToBase64String(hashingbytes);
```

ResponseRnd parametresi yanıt mesajında yer alacaktır. Üye işyerleri response hash hesaplaması için bu değeri ve MerchantPass (storekey) değerini kullanmalıdır.

Üye işyeri oluşturduğu responsehash değerinin doğruluğunu dönüş parametreleri arasında yer alan ResponseHash parametresinin değeri ile kontrol etmelidir.

5. 3D Host Model Adres Fatura Adres Gönderimi

Sanal pos üye işyeri 3D Host modelinde son kullanıcıya ait fatura ve alışveriş adreslerini güvenli ödeme sayfasına gönderebilmektedir.

Bu işlem için **TemplateType** parametresi kullanılmaktadır. Bu parametrenin alabileceği değerler aşağıda paylaşılmıştır.

TemplateType Parametresinin alabileceği değerler

- **TemplateType = "1"**
- **TemplateType = "2"**

Parametre kullanımına ait kod örneklerine **Payfor3DHostDetails1** & **Payfor3DHostDetails2** isimli dosyalar içerisinde yer almaktadır.

Kod içerisinde ilgili değer **TemplateType = "1"** olarak ödeme sistemine gönderildiğine son kullanıcı ekranı aşağıda yer aldığı gibi gösterilecektir.

QNB FINANSBANK

FinansWebPOS
Güvenli Ödeme Sayfası

QNB FINANSBANK

VISA troy mastercard

Kart Sahibinin Adı

Kart Numarası

Son Kullanma Tarihi Ay Yıl

CVV2 CVV2 Nedir

İşlem Tutarı 1 TL


Fatura Adresi Kerem ERCAN, kerem.ercan@cardtek.com, 00901112223344, 12345678909, Cardtek Payment Solutions, Istanbul, 1234567890, ITU KoruYolu Ayazaga Maslak, Sariyer, Istanbul, 34333, Turkey

Teslimat Adresi Kerem ERCAN, kerem.ercan@cardtek.com, 00901112223344, 12345678909, Cardtek Payment Solutions, Istanbul, 1234567890, ITU KoruYolu Ayazaga Maslak, Sariyer, Istanbul, 34333, Turkey




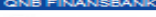
Gönder

Herkes finansçı lazım
qnbfinansbank.com 0850 222 1 900

Kod içerisinde ilgili değer **TemplateType = "2"** olarak ödeme sistemine gönderildiğine son kullanıcı ekranı aşağıda yer aldığı gibi gösterilecektir.



FinansWebPOS
Güvenli Ödeme Sayfası



Kart Sahibinin Adı

Kart Numarası

Son Kullanma Tarihi

Ay

Yıl

CVV2

CVV2 Nedir

İşlem Tutarı

1 TL

↑ ADRES BİLGİSİ

TESLİMAT ADRESİ

AD SOYAD

Vatandaşlık No

Firma Adı

Vergi Dairesi

Vergi No

Email

Telefon

Adres

ilçe

Şehir

Posta Kodu

Ülke

Teslimat Adresi ile aynı bilgileri kullan

FATURA ADRESİ

AD SOYAD

Vatandaşlık No

Firma Adı

Vergi Dairesi

Vergi No

Email

Telefon

Adres

ilçe

Şehir

Posta Kodu

Ülke

Gönder

Herkese finansçı lazım

qnbfinansbank.com 0850 222 1 900

