

E-Ticaret Güvenliđi

Kartlı Ödeme Sistemleri Bakıř Ađısı



M. Korhan Güçođlu
Yazılım Geliřtirme Yöneticisi

16 Mart 2007

E-Ticaret Tanım

- ◆ E-ticaret, işletme faaliyetlerinin elektronik olarak yapılmasıdır. Bu faaliyet metin, ses ve video verilerinin elektronik olarak işlenmesi ve aktarımına dayanmaktadır. E-ticaret bu boyutuyla mal hizmet alımı ödemelerinin dijital olarak yapılmasını kapsamaktadır. Bu faaliyetler hem mamulleri (tüketici malları, spesifik ekipmanları) ve hizmetleri (bilgi hizmeti, finansal ve yasal hizmetler) hem de geleneksel faaliyetleri (sağlık, bakım, eğitim) kapsamaktadır.(*)

***Avrupa Birliği e-ticaret komisyonu tarafından tanımlanmıştır**

E- Ticarete Kartlı Ödeme Sistemleri

- ◆ Kredi kartları, başlangıçta fiziksel dünyada kullanım amacı ile tasarlanmışlardır.
- ◆ Sanal ortama erişim imkanı ve sunulan içerik katlanarak artmıştır.
- ◆ Kredi kartları, E-Ticaret'te ülkemizde ve dünyada en yaygın ve önemli ödeme aracıdır.
- ◆ Müşteri ve işyerlerine büyük kolaylık sağlayan bu imkan sahtekarların ve saldırganların tehdidi altındadır.

B**K**BANKALARARASI
KART MERKEZİ**M**

Yurtiçi E-Ticaret Fraud Durumu

Yıl	İşlem Adet	İşlem Ciro	Fraud Adet	Fraud Ciro(YTL)	Fraud Oran (Adet)	Fraud Oran (Ciro)	Fraud Artış Adet	Fraud Artış Ciro
2002	-	-	187	16.611	-	-	-	-
2003	3.534.678	262.435.219	1.046	304.419	0,03%	0,12%	559,36%	1832,64%
2004	6.726.626	633.761.019	2.341	2.011.113	0,04%	0,32%	223,80%	660,64%
2005	7.448.236	1.038.456.958	5.484	2.514.649	0,07%	0,24%	234,26%	125,04%

B**K**BANKALARARASI
KART MERKEZİ**M**

Yurtiçi Standart

T.C. BAŞBAKANLIK
DEVLET PLANLAMA TEŞKİLATI MÜSTEŞARLIĞI

Bilgi ve İletişim Teknolojilerinin İş Dünyasına Nüfuzu

BİN- 26 – e-Ticaret Güvenlik Altyapısı

1. Proje Sahibi Kuruluş

Türk Standardları Enstitüsü

2. Zamanlama

Başlangıç : Temmuz 2007**Bitiş** : Temmuz 2008**Süre** : 12 ay

3. Proje İle İlgili Kuruluşlar

Kuruluş 1 : Dış Ticaret Müsteşarlığı**Kuruluş 2** : TÜBİTAK (UEKAE)**Kuruluş 3** : Bankacılık Düzenleme ve Denetleme Kurumu**Kuruluş 4** : Türk Akreditasyon Kurumu**Kuruluş 5** : Bankalararası Kart Merkezi**Kuruluş 6** : İlgili Sivil Toplum Kuruluşları

Yurtiçi Standart

- ◆ Sektörel beklentimiz:
 - Global ödeme sistemleri ile entegre
 - Ticari faaliyetleri zorlamayacak / engellemeyecek.
 - Rekabet koşullarına uygun.
 - Girişimciler açısından fırsat eşitliği sağlayan.
 - İşlem hacmi ölçeğinde değişken
 - Uygulanabilir, kontrol edilebilir.
 - Ceza yerine teşvik uygulamaları ile desteklenen
 - Zorunluluk yerine sorumluluk devri koşul ve kurallarını yasal çerçevede tanımlayan, bir çözüm oluşturulmasıdır.

B

K

BANKALARARASI
KART MERKEZİ

M

Kartlı Ödeme Sistemleri Güvenliği

PoS Kullanımı

Çevrimiçi E-Ticaret

Back Office

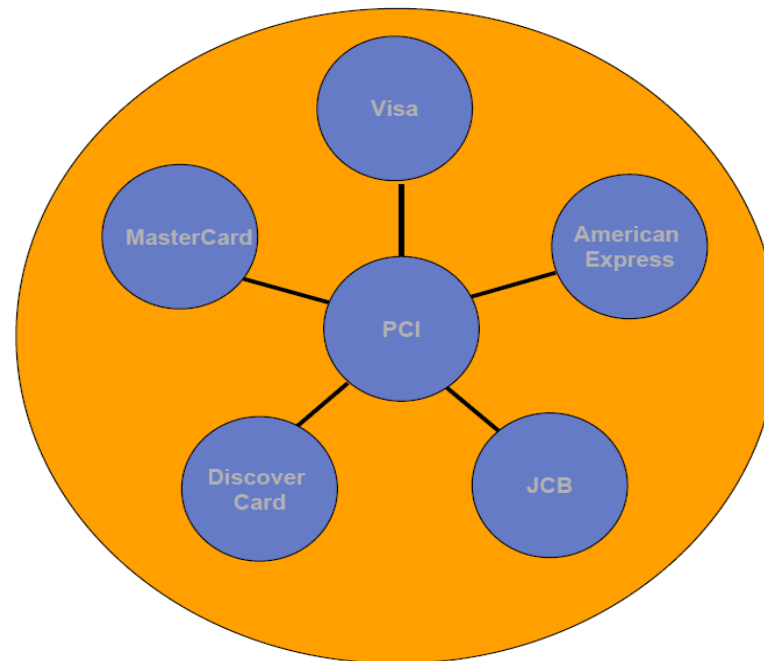
Chip & PIN

3-D Secure Sistemleri

PCI DSS

PCI DSS

- ◆ Payment Card Industry(PCI), Data Security Standards(DDS)



PCI DSS – 6 Başlık 12 Zorunluluk

- **Güvenli iletişim ağının oluşturulması ve idamesi**
 - Güvenlik duvarının kurulumu ve idamesi
 - Üretici tarafından belirlenmiş ön tanımlı kullanıcı kodu/şifrelerin ve güvenlik parametrelerinin kullanılmaması
- **Kart sahibinin bilgilerinin/verilerinin korunması**
 - Depolanan bilginin korunması
 - Paylaşılan ağlarda, kart sahibinin bilgilerinin kriptolanarak gönderilmesi
- **Zafiyet Yönetimi Programının kurulması**
 - Anti-virüs yazılımının kullanılması ve sürekli güncellenmesi
 - Güvenli sistem ve uygulamaların geliştirilmesi ve bakımı
- **Kuvvetli erişim denetimi önlemlerinin uygulanması**
 - Yalnız iş için gerekli olan bilgiye erişim prensibine göre erişimin kısıtlanması
 - Her bilgisayar kullanıcıasına tek bir kullanıcı ID atanması
 - Kart sahibinin verilerine fiziksel erişimin kısıtlanması
- **Düzenli olarak iletişim ağının izlenmesi ve test edilmesi**
 - Ağ kaynaklarına ve kart sahibinin verilerine erişimin takibi ve izlenmesi
 - Güvenlik sistemlerin ve süreçlerin düzenli olarak test edilmesi
- **Bilgi Güvenliği Politikasının işlerliğinin sağlanması**
 - Bilgi güvenliğini adresleyen bir politikanın bulunması

PCI DSS – 1. Zorunluluk

- ◆ Güvenlik duvarının kurulumu ve idamesi
 - Firewall ve Router ayarları standartları
 - Değişiklik kontrol prosedürleri
 - Ağ segmentasyonu ve firewall kuralları
 - NAT / PAT altyapıları
 - Kişisel firewall

PCI DSS – 2. Zorunluluk

- ◆ Üretici tarafından belirlenmiş ön tanımlı kullanıcı kodu/şifrelerin ve güvenlik parametrelerinin kullanılmaması
 - Ön tanımlı kullanıcı kodu/şifrelerini değiştirin ve yönetici erişimini engelleyin
 - Konsol üzerinden olmayan yönetici erişimlerinde kullanıcı kodu/parolaları şifreleyin
 - Sistem konfigürasyon standartlarını ve güvenlik altyapılarını dokümante edin

PCI DSS – 3. Zorunluluk

- ◆ Depolanan bilginin korunması
 - Kart ve kart sahibi verisinin saklanma ihtiyaçlarını en aza indirin
 - Otorizasyonla ilgili hassas bilgileri şifreli olsa dahi saklamayın
 - Kart numaralarını gösterimi gerektiğinde maskeleyin
 - Kart ve kart sahibi verisini okunamaz şekilde saklayın (şifreleme, hashing, silme)

PCI DSS – 4. Zorunluluk

- ◆ Paylaşılan ağlarda, kart sahibinin bilgilerinin kriptolanarak gönderilmesi
 - Güçlü kriptografi ve şifreleme teknikleri kullanın
 - Hiçbir zaman kart ve kart sahibi verisini şifrelenmemiş bir şekilde e-posta ile göndermeyin

PCI DSS – 5. Zorunluluk

- ◆ Anti-virüs yazılımının kullanılması ve sürekli güncellenmesi
 - Virüs etkilenmesine açık tüm sistemleriniz için virüs engelleyici mekanizmalar geliştirin
 - Çalıştıklarını, güncel olduklarını ve denetim iz kaydı ve alarmlar ürettiklerini garanti altına alın

PCI DSS – 6. Zorunluluk

- ◆ Güvenli sistem ve uygulamaların geliştirilmesi ve bakımı
 - En geç 30 gün içinde sistemlere güvenlik güncellemelerini yükleyin
 - Yeni tespit edilmiş güvenlik açıklarını belirleyecek iş akışlarını oluşturun
 - Tüm sistem ve yazılım konfigürasyon değişiklikleri için değişiklik kontrol prosedürleri hazırlayın
 - Yazılım geliştirme süreçlerinizi güvenli kodlama tekniklerine uygun hale getirin

PCI DSS – 7. Zorunluluk

- ◆ Yalnız iş için gerekli olan bilgiye erişim prensibine göre erişimin kısıtlanması
 - Bilgi işlem kaynakları, kart ve kart sahibi verilerine erişim hakkını sadece işi gereği buna ihtiyaç duyan çalışanlarınıza tanıyın
 - Eğer özellikle aksi belirtilmemişse kullanıcılarınıza ilk tanımlamada çok kullanıcılı sistemlere erişim hakkı tanımayın

PCI DSS – 8. Zorunluluk

- ◆ Her bilgisayar kullanıcılarına tek bir kullanıcı ID atanması
 - Kullanıcı adlarını kişilere özelleştirin
 - Sistemdeki bütün doğrulama adımlarında kullanıcı adı ve şifre kullanımını zorunlu hale getirin
 - Uzaktan erişim için "2-factor authentication" uygulayın
 - Şifre profili güvenlik seviyenizi yükseltin(90 günde bir değişen, en az 7 karakter uzunluğunda, son 4 şifrenin unutulmadığı, kilitlenebilir vb..)

PCI DSS – 9. Zorunluluk

- ◆ Kart sahibinin verilerine fiziksel erişimin kısıtlanması
 - Sistem odasına girişi sınırlandırmak için giriş kontrolleri ve izleme altyapısı geliştirin(video kamera(kayıtlar 3 ay saklanacak), ağ araçlarına fiziksel erişimi kısıtlayın) uygulayın
 - Ziyaretçilerinizi kontrol edin, onları çalışanlarınızdan ayırıştırın(yaka kartı)
 - Verimerkezi ziyaretçi kayıtlarını tutun
 - Kağıt ya da elektronik ortamlarda bulunan kart ve kart sahibi verilerinin saklandığı ortamları fiziksel güvenlik altına alın
 - Medya imha prosedürlerini geliştirin, uygulayın (kağıt imha, cd imha, sabit disk silme)

PCI DSS – 10. Zorunluluk

- ◆ Ağ kaynaklarına ve kart sahibinin verilerine erişimin takibi ve izlenmesi
 - Kart ve kart sahibi bilgilerine erişimleri için iz kayıtları oluşturun
 - Erişim için kişiselleştirilmiş kullanıcılar tanımlayın
 - İz kayıtlarının denetimi sürecini güvenli ve merkezileştirilmiş bir şekilde yapın
 - Tüm sistemlerde senkronize sistem saati kullanın
 - Erişim iz kayıtlarını günlük olarak inceleyin
 - Erişim iz kayıtlarını kontrollü ve güvenli bir şekilde silin - imha edin

PCI DSS – 11. Zorunluluk

- ◆ Güvenlik sistemlerin ve süreçlerin düzenli olarak test edilmesi
 - Ağ yapısında açık-zafiyet tespiti amacı ile yapılan harici ve dahili taramaları minimum 3 ayda bir ya da önemli bir ağ yapısı değişikliğini takiben gerçekleştirin
 - Penetrasyon testlerini en az yılda bir ya da ciddi uygulama değişikliklerini takiben uygulayın
 - Sistemlere İzinsiz girişleri tespit eden ve/veya engelleyen sunucu tabanlı sistemler kurun
 - Kritik sistem ve içerik dosyalarında onaysız değişiklikleri tespit amacı ile dosya bütünlüğü izleme araçlarını uygulayın

PCI DSS – 12. Zorunluluk

- ◆ Bilgi güvenliğini adresleyen bir politikanın bulunması
 - Bilgi Güvenliđi Politikanızı oluřturun, dokümente edin, güncelleyin ve yayınlayın
 - Politikanız çerçevesinde güvenlik operasyon prosedürlerinizi oluřturun
 - Bilgi güvenliđi sorumluluklarının net bir şekilde tanımlanıp ilgili personele atamalarının yapıldığından emin olun
 - Proaktif güvenlik programları geliřtirin
 - İnsan kaynaklarının çalıřanlarınıza politika ve prosedürlerinizi aktarmasını/onatmasını sađlayın
 - 3. partilerle çalıřırken sözleşme seviyesinde zorunluluklar tanımlayın
 - Olay reaksiyon planları geliřtirin

B

K

BANKALARARASI
KART MERKEZİ

M

PCI DSS – Kategoriler

- ◆ İşyerleri / Hizmet Sağlayıcılar
- ◆ İşlem sayısı:
 - Geçen VISA, MC işlem sayısı (birbirinden ayrı)
 - Kabul noktası sayısı
- ◆ Acente altyapıları

PCI DSS – Faaliyet Alanı

- ◆ PCI DSS üzerinde kart ve kart sahibi bilgileri saklanan, işlenen ve/veya iletilen tüm sistem ve ağ yapıları, ve bunlara bağlı tüm sistemler için geçerlidir.
- ◆ PCI DSS e uyulduğunu doğrulama süreçlerine ilişkin zorunluluk her zaman bu alanı kapsamaz.
 - Hizmet sağlayıcılar genelde doğrulanır.
 - İşyerleri genelde doğrulanmaz.

PCI DSS – Faaliyet Alanı

- ◆ İşyeri bütün sistemlerinde kurallara uymakla sorumludur, doğrulama süreci genelde otorizasyon ve takas verileri barındıran kurumlar için geçerlidir.
- ◆ PoS donanımları doğrulama süreci dışındadır.

3-D Secure - Tarihçe

- ◆ Kart sahipleri genelde internette alışveriş yaparken, araya birisinin girip kart bilgileri çalmasından korkarlar.
- ◆ Ancak; çoğu e-ticaret sitesinde kullanılan SSL teknolojisi bunu imkansız kılar.
- ◆ Asıl risk alışveriş esnasında girilen kart bilgisinin kart sahibi tarafından girilip girilmediğinin doğrulanamamasından kaynaklanır.
- ◆ Kredi kartları fiziksel dünyada işlem gerçekleştirmek için tasarlanmışlardır.
- ◆ Fiziksel dünyada kart sahibi doğrulaması imza yada geçerli bir kimlik kontrolü ile sağlanabilmektedir.

3-D Secure - Tarihçe

- ◆ Efektif bir kart sahibi doğrulama metodu kullanılmadan gerçekleştirilen e-commerce işlemleri:
 - Müşteri güveninin azalmasına,
 - Daha yüksek işlem maliyetine,
 - İşyerlerinde gelir kaybına,
 - Bankalar için daha yüksek servis giderlerine ve ters ibraz (charge-back) kayıplarına,
 - Kredi kartı firmaları için çok ciddi imaj zedelenmelerine yol açar.
- ◆ Ayrıca; kart sahibi doğrulama metodunun kullanılmaması süreç içerisinde kartlı ödeme sistemleri dışında kalan online ödeme metodu alternatiflerinin pazardan pay kapmalarını sağlar.

3-D Secure - Tarihçe

- ◆ 90'ların başında, VISA, MasterCard ve AMEX Internet alışveriş işlemlerinde kredi kartlarının pazarda dominant bir araç olacağı öngörüsü ile, bu işlemlerde, kart sahibini doğrulama metodları geliştirmenin gerekli olduğunu tespit ettiler.
- ◆ Bu amaçla, Secure Electronic Transaction (SET) adında ortak standartlar kümesini geliştirdiler.
- ◆ SET teknolojik açıdan bir başyapıt olsa da yüksek maliyeti ve karışık implementasyon yapısı genel pazar kabulü görmesine engel oldu.

3-D Secure - Tarihçe

- ◆ Bu arada, kredi kartları kullanılarak gerçekleştirilen e-commerce işlem hacmi yükselmeye devam etti.
- ◆ Buna paralel olarak fraud işlem ve terz ibraz adetleri de artmaya devam etti.
- ◆ 2002 yılında, internetten yapılan kredi kartı işlemleri toplam işlemlerin % 2-4 ü oranına erişmesine rağmen fraud işlem cirosu normal işlemlerin 12 katı seviyelerine ulaşmıştı.
- ◆ E-commerce 2002 yılındaki büyüme hızı ile devam ettiğinde bu bütün kartlı ödeme sistemleri ve sektör için oldukça ciddi bir problem olmaya başlayacağı açıktı.
- ◆ VISA ve MasterCard bu duruma engel olabilmek için 2001 yılında(SET'in açıklanmasından 5 yıl sonra) yeni kart sahibi doğrulama standartları oluşturma çabasına giriştiler.



B

K

BANKALARARASI
KART MERKEZİ

M

Tarihçe

- ◆ Bu sefer MC ve VISA birlikte çalışmak yerine, rekabet edebilecek iki ayrı standart üzerinde çalıştılar.
- ◆ JCB de bu sürece 1-2 yıl sonra katıldı.
- ◆ Verified by VISA, MC Secure Code ve JCB J-Secure
- ◆ Bu standartlar teknik olarak farklı olsalar da, müşterinin işlem esnasında, kullanıcı adı ve şifre girmesi mekaniği ile çalışırlar.
- ◆ Ayrıca; bir şekilde kart numarasını elde eden kötü niyetli bir kişi bu standartlara uyan E-Ticaret sitelerinde işlem gerçekleştiremez.

Sistem Açıklamaları

- ◆ MPI(Merchant Plug In):
 - E-Ticaret sitelerinde kullanılacak yazılım parçası.
 - İşlemin WEB üstünden yönlendirileceği sistem seçimi ve iletişim kanalları yönetimi.
- ◆ ACS(Access Control Server):
 - Aktivasyon sonrasında kart ve kart doğrulama bilgilerinin tutulacağı sunucu sistem.
 - Aktivasyon ve doğrulama süreci WEB üzerinden yapılacağı için kesintisiz Internet çıkışı ihtiyacı var.
- ◆ DS(Directory Server):
 - Kart sahibi doğrulama süreci için ilgili Issuer ACS sistemine yönlendirme yapan sunucu.

3-D Secure

- ◆ 3-D (Three Domain) işlem iş akışında sorumlulukları ilgili partiler için ayrıştırıp tanımlayan bir sistemdir
- ◆ Issuer Domain: Kart sahipleri ve bankaları
- ◆ Acquirer Domain: İş yerleri ve bankaları
- ◆ Interoperability Domain: Issuer ve Acquirer organizasyonları arasında VISA, MC sistemleri ile sağlanan iletişim
- ◆ İşyeri ve kart sahibi açısından katılım esasına göre tasarlanmıştır

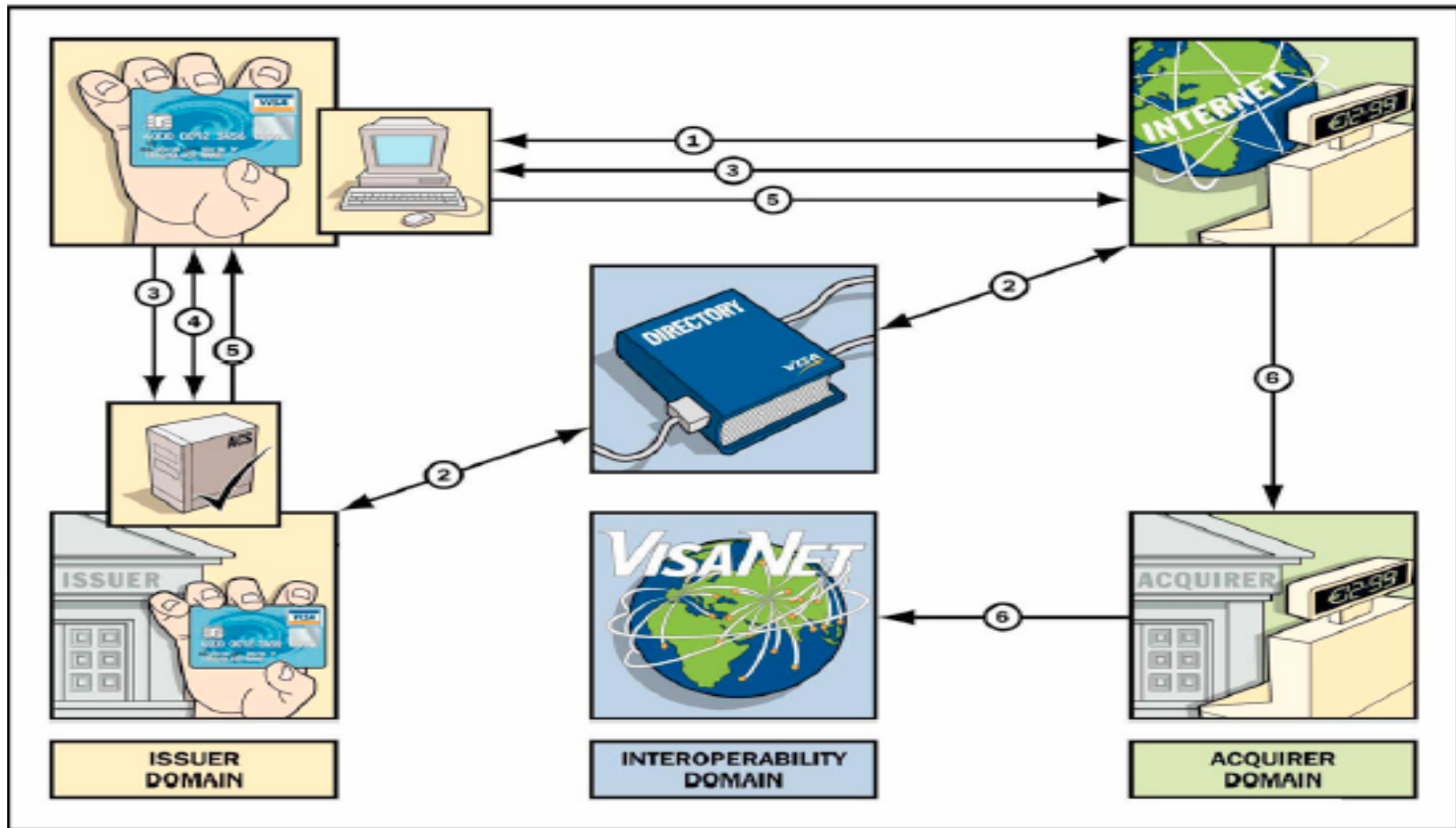
B

K

BANKALARARASI
KART MERKEZI

M

Verified By VISA



B

K

BANKALARARASI
KART MERKEZİ

M

VISA Kart Sahibi Doğrulama Ekranı

TB Test Bank

Test Merchant

Date: 01/12/05


Time: 03:57:18

Amount: \$123.65 USD

Card Number: XXXX-XXXX-XXXX-XXXX

Personal Assurance Message:
I'm sure this is my bank

Visa Password:

 Verified by
GPayments

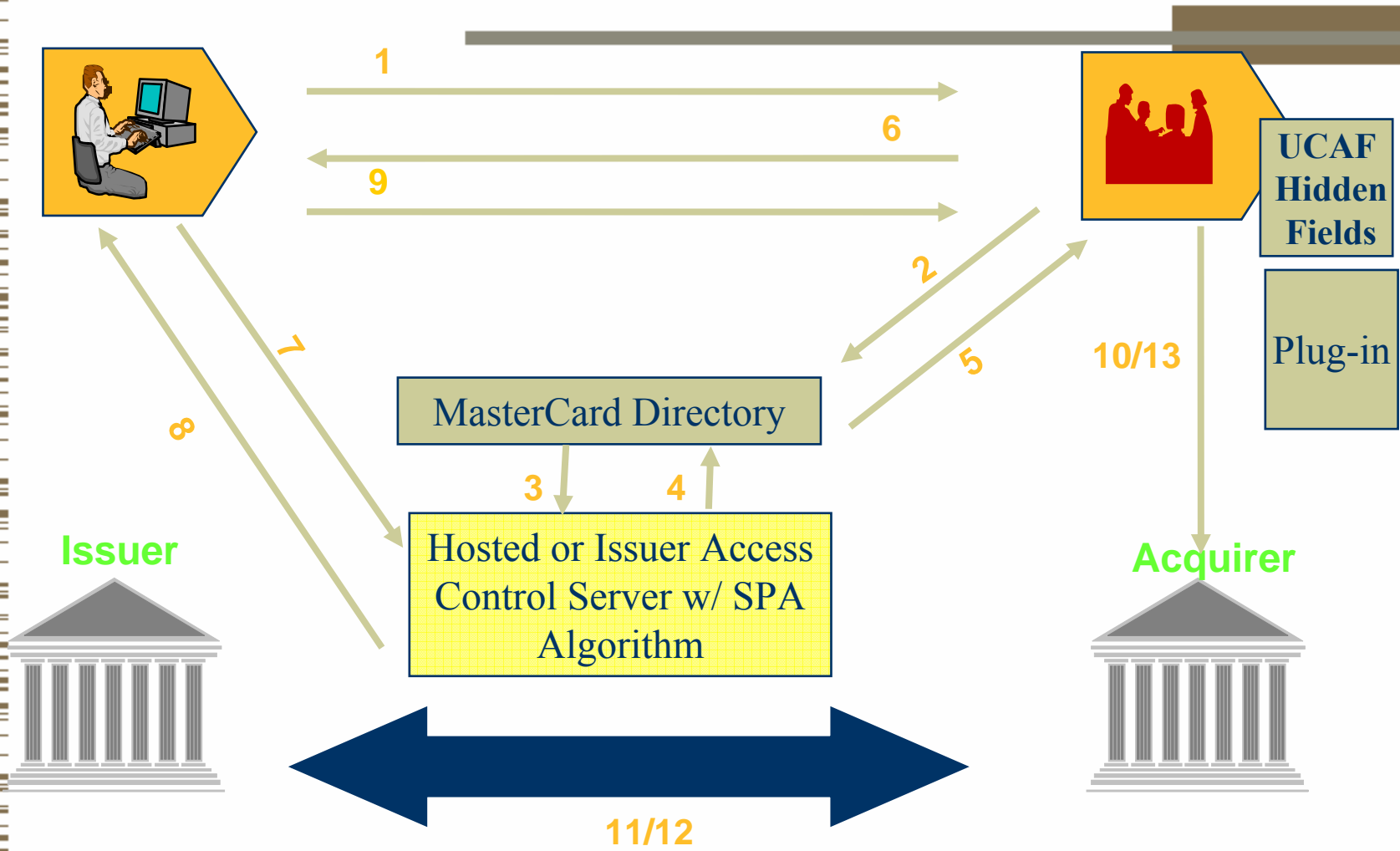
B

K

BANKALARARASI
KART MERKEZI

M

MC SecureCode Uygulaması



B

K

M

BANKALARARASI
KART MERKEZİ

MasterCard Kart Sahibi Doğrulama Ekranı

The screenshot shows a Microsoft Internet Explorer browser window displaying a checkout page for TestbookX.com. The page title is "Checkout - Microsoft Internet Explorer". The browser's address bar shows "TestbookX.com - Checkout". The page content includes a section titled "6. Enter payment information" with the following text:

- * - information required to complete your order
- * * You may use your SPA wallet to make an authenticated transaction at this site

The payment information section contains the following fields:

- * credit card type:
- * name on card:
- (Enter your name exactly as it appears on your card)
- * card number:

Below the payment information section, there is a light blue dialog box with the following text:

You may make a Secure Payment Application (SPA) transaction at this website. Please enter your username and password to proceed with an authenticated payment.

Merchant Name: TestbookX.com
Transaction Amount: USD 341.45

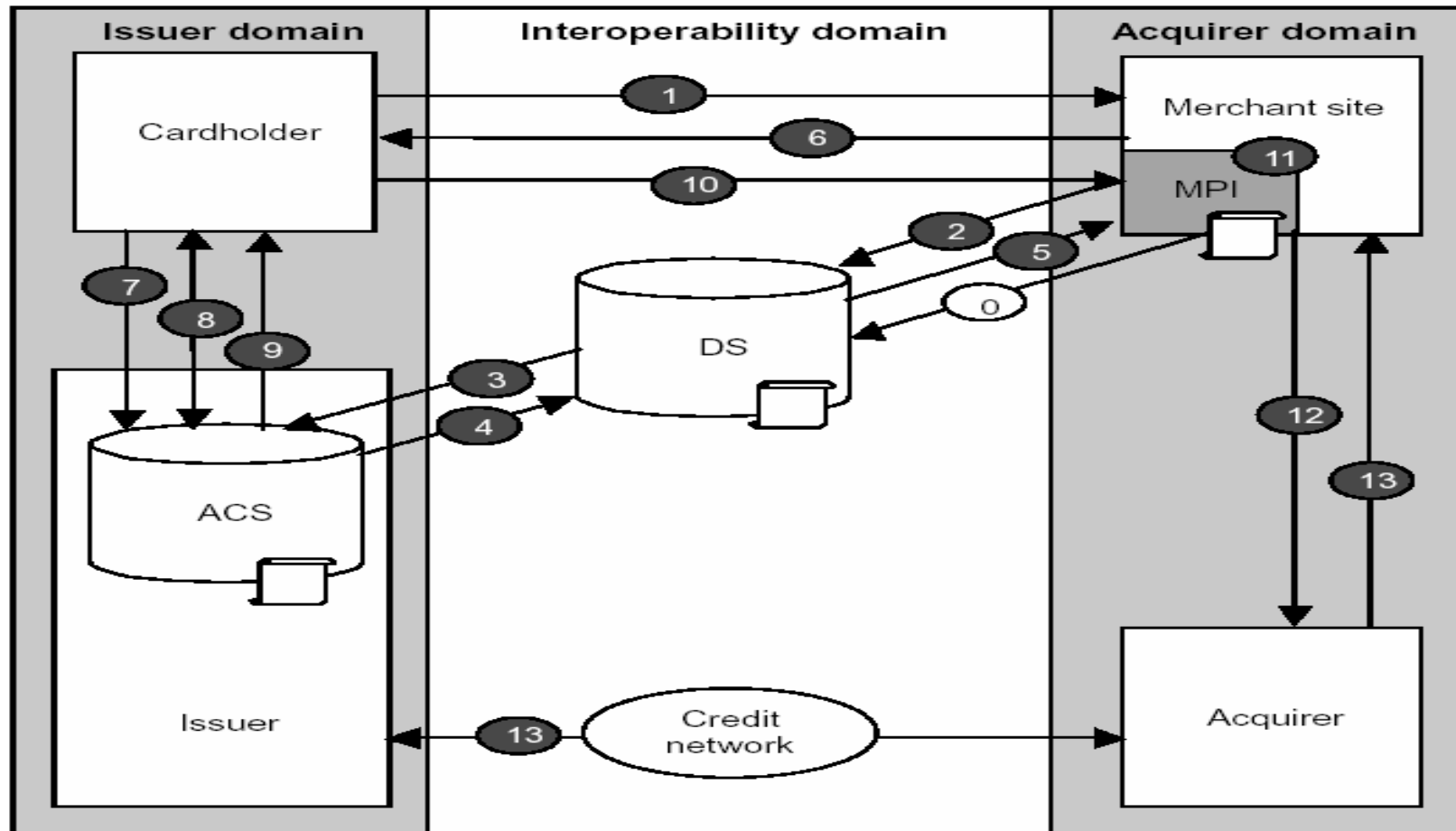
The dialog box contains the following fields:

- Username:
- Password:
- submit

At the bottom of the page, there is a "MasterCard ActiveCheckout" logo and a "BizRate.com" logo. The browser's status bar shows "Local intranet zone" and the time "11:53".

B**K**BANKALARARASI
KART MERKEZİ**M**

JCB J-Secure



Kıyaslamalar – İşlem Süreci

- ◆ 3-D Secure sistemi, kart sahibi doğrulama adımında başka bir URL'den pop-up kullanıcı adı, şifre girişi ekranı açmaktadır.
- ◆ Bu durum, sistemi “man in the middle” saldırısına açık hale getirmektedir.
- ◆ Bunu engellemek için “personal assurance message” konseptini geliştirilmiştir.

Teşekkür Ederim

Hazırlayan: M. Korhan Güçođlu
Yazılım Geliştirme Yöneticisi

