E-Ticarette Güvenlik

Elektronik Ticaret`de Güvenlik...

Elektronik ticarette alıcı ve satıcı birbirlerini görmeksizin iş yaptıklarından karşılıklı olarak güvenin sağlanması için ek bir takım önlemler almaya ihtiyaç duyarlar. Öncelikle alıcı ve satıcı taraflar birbirlerinin kimliklerinden emin olmak isterler. İşte bu ihtiyaçtan dolayı daha sonra bahsedeceğimiz "dijital imza" ve "dijital sertifika" kavramları geliştirilmiştir.

Bunlar aracılığıyla iki taraf birbirlerinin kimliğinden emin olabilmektedir. Türkiye'de şu anda dijital sertifikalar ile ilgili yasal altyapı henüz oluşturulmadığı için alıcı tarafında bulunan bireysel kullanıcılar henüz dijital sertifika kullanmaya başlamamışlar, satış yapan siteler de müşterilerine bunu şart koşmamışlardır. Bu nedenle satıcılar alıcıların kimliklerini kontrol edememektedirler. Bazı özel kuruluşlar, özel sistemler geliştirerek bu kuşkuyu ortadan kaldırmaya çalışmaktadır.

Elektronik ticarette güvenlik konusunda değerlendirilmesi gereken diğer bir konu da alıcıların elektronik ticaret sitelerinden alışveriş yapmak için vermek durumunda kaldıkları kredi kartı vb. bilgilerin Internet üzerinden iletilirken üçüncü şahısların eline geçmesi riskidir. Bilindiği gibi özellikle telefonla yapılan satışlarda (gazeteye ilan vermek, katalog satışları vb) kredi kartı numarası ve son kullanma tarihi alışveriş için yeterli olmaktadır. Bu yüzden bu bilgilerin korunması e-ticaretin gelişimi için büyük önem taşımaktadır.

Ancak e-ticarette kredi kartı bilgilerinin başkalarının eline geçme riski günlük hayattakine göre çok daha azdır. Günlük hayatta ödeme yaparken kredi kartı bir başkasına verilmekte, bu yüzden kredi kartının üzerindeki bilgilerin gizliliği büyük oranda ortadan kalkmaktadır. Sanal alışveriş hizmeti veren firmalar, kredi kartı bilgilerinin güvenliği ve gizliliğini sağlamak için yaygın olarak SSL ve SET gibi güvenlik standartlarını kullanmaktadırlar. Kullanıcı, işyeri ve banka arasındaki veri akışı sırasında bilgilerin şifrelenerek aktarılması esasına dayanan güvenlik sistemleri sayesinde bilgilerin başka bir kişinin eline geçmesi durumunda çözülebilmesi (yani kullanılabilmesi) önlenir. Böylece kart bilgilerinin gizliliği ve alışverişin güvenliği sağlanmış olur. Burada önemli bir noktada, gizlilik sağlansa da müşteriye itiraz hakkının verilip verilmeyeceğidir.(Kuruluşlar genelde itiraz hakkı verirler.)

Nasıl ki kredi kartınızı çaldırmanız, kaybetmeniz, kasa başında unutmanız v.b. gibi normal kullanım riskleri varsa, internet üzerinden alışverişte de, söz gelimi, kredi kartı bir başkasına vermişseniz ve kişisel bilgilerinizi (isim, adres, telefon vb) başkaları biliyorsa, benzer riskler vardır. Ancak bu risk, genellikle teknolojinin yetersizliğinden değil tam tersine, yanlış ve bilinçsiz kullanımından doğmaktadır.

Güvenlik İçin Kullanılan Yaygın Protokoller:

İnternet üzerinde dolaşan bilgi paketleri, bir takım güvenlik protokolleri yardımıyla "şifrelenerek" gönderilir. Bunlardan en popülerleri SSL (güvenlikli web oturumu ve karşılıklı bilgi değiş-tokuşu) ve SET (kredi kartı uygulamaları) dir. SSL (Secure Sockets layer) ve SET (Secure Electronic Transaction) sayesinde, bilgi güvenli bir şekilde "sadece" doğru kişiye iletilir ve bilgiyi gönderen bilgisayar ile alan bilgisayar arasında güvenli bir veri iletişimi kurulur.

Kredi kartı numarası, isim, adres vb gibi bilgiler güvenli olarak iletilir. İnternet üzerinde alışveriş yapılan tüm merkezlerde alışveriş yapılırken bu tip güvenlik sistemleri kullanılır. 128 bir şifreleme algoritmaları kullanan bu sistemler, e-ticaret için gerekli "güvenli iletişim" ortamını sağlarlar. Anahtarlar üretilirken kullanılan bazı popüler algoritmalar olarak, DES (Data Encryption Standard), RSA, IDEA verilebilir. Bunlardan RSA'nın RC4 algoritması (128 bit şifreleme olarak) Netscape ve Internet Explorer'da da kullanılan bir algoritmadır.

Sanal Mağazaya müşterilerin güvenli erişimi için, SLL standartı kullanılmaktadır. Satıcı firma, bir onay kurumundan aldığı elektronik web sitesi kimliği ile mağazasının sanal dünyadaki kaydını gerçekleştirmektedir. Müşteri ile Satıcı Firma arasındaki iletişimde güvenliği sağlayan SLL; internette ulaşılan adresin gerçekten aranan mağaza olup olmadığını kontrol etmekte ve bilgilerin şifrelenerek gönderilmesini sağlamaktadır.

Satıcı firma ile banka arasındaki iletişimin güvenliği ise SET protokolü ile gerçekleştirilmektedir. Müşteriden SLL ile alınan ödeme bilgileri (kredi kartı), satıcı firma tarafından bankaya SET protokolü ile şifrelenerek gönderilmektedir. Banka, müşterinin hesabının uygun olması durumunda, alışverişini onaylamakta ve provizyon bilgisini satıcı firmaya göndermektedir. Satıcı firma, müşterisine siparişin tamamlandığını bildirdikten sonra bankaya bağlanarak alışveriş tutarını hesabına aktarmaktadır. Ülkemizde kitap, kaset, CD, çiçek, elektronik, giyim, bilgisayar, gıda, vb. ürünlerin İnternette doğrudan müşteriye satışını yapan sanal mağaza sayısı 250'yi aşmıştır (*).

Geniş Anlamıyla SSL

SSL (Secure Sockets Layer), ağ üzerindeki web uygulamalarında güvenli bilgi aktarımının temini için (bilginin doğru kişiye güvenli olarak iletimi), "Netscape" firması tarafından geliştirilmiş bir program katmanıdır . Burada, bilgi iletiminin güvenliği, uygulama programı (web browser, HTTP) ile TCP/IP katmanları arasındaki bir program katmanında sağlanmaktadır. SSL, web sunucularına (Apache vb), bir modül olarak yüklenir ve böylece web sunucuları güvenli erişime uygun hale gelir. SSL, hem istemci (bilgi alan) hem de sunucu (bilgi gönderen) bilgisayarda bir doğrulama (authentication: iki bilgisayarın karşılıklı olarak birbirini tanıması) mekanizması kullanır. Böylece, bilginin doğru bilgisayardan geldiği ve doğru bilgisayara gittiği teyit edilir.

Bilgisayarların birbirlerini "tanıma" işlemi, açık-kapalı anahtar tekniğine (public-private key encryption) dayanan bir kripto sistemi ile sağlanır. Bu sistemde, iki anahtardan oluşan bir anahtar çifti vardır. Bunlardan açık anahtar (public key) herkes tarafından bilinebilen ve gönderilen mesajı "şifrelemede" kullanılan bir dijital anahtardır. (Burada anahtar' dan kasıt, aslında bir şifreleme -kriptolama- algoritmasıdır. Bu algoritma (yani, anahtar) kullanılarak gönderilecek bilgi şifrelenir). Ancak, açık anahtar ile şifrelenen mesaj sadece bu anahtarın diğer çifti olan "kapalı anahtar" (private key) ile açılabilir (deşifre edilebilir). Kapalı anahtar da, sadece sizin bildiğiniz bir anahtar olduğundan, mesaj güvenliği sağlanmış olur. Örnek olarak, size mesaj göndermek isteyen birine kendi açık anahtarınızı gönderirsiniz. Karşı taraf bu anahtarı kullanarak mesajını şifreler ve size gönderir. Şifrelenen mesajı, sadece sizde olan ikinci bir anahtar (kapalı anahtar, private key) çözebilir ve bu anahtarı sadece siz bilirsiniz.

SSL, web sunucusunu tanımak için, dijital olarak imzalanan sertifikalar kullanır. Sertifika, aslında, o organizasyon hakkında bazı bilgiler içeren bir veri dosyasıdır. Aynı

zamanda da, kuruluşun açık-kapalı anahtar çiftinin "açık" anahtarı da sertifika içinde yer alır. Sunucu sertifikası da, o sunucuyu işleten kuruma ait bilgiler içeren bir sertifikadır. Sertifikalar, "güvenilir" sertifika kuruluşları tarafından dağıtılır (Örneğin VeriSign vb.).

İstemci(bilgi alan) bilgisayar, SSL destekleyen bir sunucuya bağlandığı anda, (bu, https:// ile başlayan URL satırları ile gerçekleşir) doğrulama işlemi başlar. İstemci, kendi açık anahtarını sunucuya gönderir. Sunucu ise, bu anahtarı kullanarak şifrelediği bir mesajı istemciye geri gönderir. Bir sonraki adımda istemci sadece kendinde olan kapalı (private) anahtarı kullanarak gelen şifreli mesajı çözer ve sunucuya geri gönderir. Mesajı alan sunucu ise, bunu kendisinin gönderdiği orijinal mesaj ile karşılaştırır ve eğer iki mesaj "aynı" ise "doğrulama" işlemi başarıyla tamamlanmıştır ve sunucu bu noktadan itibaren "doğru bilgisayarla/kişiyle" iletişimde olduğunu anlar. Daha sonra sunucu istemciye o an gerçekleşen web oturumunda kullanılacak tüm önemli anahtarları gönderir ve güvenli iletişim başlar.

SSL, bugün için yaygınlıkla kullanılan ve birçok yazılımın desteklediği bir stantard haline gelmiştir. Özellikle internet üzerinden bankacılık, elektronik kimlik belgesi çıkartma gibi hizmetler veren siteler SSL kullanmaktadırlar.

SET nasıl işliyor ?

SET (Secure Electronic Transaction), elektronik ticarette, internet üzerinde güvenli bilgi aktarımını sağlamak amacıyla aralarında VISA, MasterCard ve IBM'in de olduğu kuruluşlar tarafından geliştirilen bir protokoldür. SET uyumlu ilk alışveriş, 18 Temmuz 1997'de San Francisco'da yapılan tanıtımla İspanya ve Singapur'da bulunan sanal mağazalardan gerçekleştirilmiştir. Garanti Bankası Şubat 1998'de gerçekleştirdiği SET uyumlu alışverişle, bu protokolü kullanmaya başlayan Dünya'da yedinci, Avrupa'da dördüncü ve Türkiye'de ilk kuruluş olmuştur.

Amaç, internet üzerinden kredi kartıyla güvenli ödeme yapabilmektir. Diğer bir deyişle, kullanıcının kredi kartı ikinci taraflarca okunmamalı ve ödeme emrindeki mal miktarı, ödeme miktarı zaman bilgisi vb. diğer bilgiler, hem alıcı, hem satıcı hem de aracı kurum olaarkbanka tarafından inkar edilemez nitelikte olmalıdır. Uygulanma aşamasında, bir takım yazılımların birleştirilmesi ile yapılır. Bunlardan ilki, internet tarayıcı cüzdanı yada elektronik cüzdan(browser wallet)'dır. Tarayıcı czdanı, bir internet tarayıcısı ile birlikte çalışan ve kredi kartı sahibinin alış-veriş yaparken kredi kartlarını ve elektronik kimlik belgelerini taşımasını sağlayan yazılımdır. Satıcıdan gelen SET mesajlarına cevap olarak, alıcıya hangi kredi kartıyla alışveriş yapmak istediğini sorar ve tanımlı olan bütün SET protokolü işlemlerini yerine getirir. Diğer yanda, satıcılar ve satıcı sunucusu yazılımı(merchant server) kullanırlar. Bu yazılım, alıcı ödemelerini karşılar, satıcının iş yaptığı veya anlaşmalı bankası ile iletişime geçer, ödeme ve sipariş ile ilgili benzeri işlemler yapar. Bankalar ise, satıcının yaptığı kredi kartı işlemlerinin doğrulanması ve ödemelerin bankalar arası takasını sağlamak üzere bir yazılım kullanırlar.

SET, özellikle on-line (gerçek zamanda) kredi kartı bilgileri iletimi için geliştirilmiş bir standarttır. SET, kredi kartı ile yapılan online ödemelerde, bilgilerin internet üzerinden aktarımında gizlilik ve güvenlik entegrasyonunu sağlar. SET protokolü sadece müşteri (ürün siparişi veren kredi kartı sahibi) ile sanal dükkan (e-dükkan) ve kredi kartı şirketi arasındaki ödeme fazını şifreler.

SET ile, ödeme işlemine taraf olan herkes (müşteri, dükkan sahibi, kredi kartı şirketi), birbirlerini tanırlar (teşhis ederler, authentication) ve bu ispatlanabilir. "Tanıma" işlemi, SSL'dekine benzer bir dijital sertifikasyon sistemi ile yapılır. Yani, ödeme fazına dahil bütün taraflar kendi kimliklerini belirten dijital bir sertifika kullanır.

Mevcut güvenlik sistemlerinden SET'i farklı kılan sebep; alıcı ile satıcıyı bir finansal kurum ile ilişkilendiren sertifikaların varlığıdır.

SET güvenli bir iletişim altyapısı sağlamasına karşın, beklendiği hızda yaygınlaşamamıştır. Bunun nedenleri uzmanlar tarafından , kullanıcı kolaylığında yaşanan sıkıntılar ve bahsedilen yazılımların dağıtımı ile ilgili zorluklar olarak tespit edilmiştir.

Dijital imza nedir ?

İlk kez ABD eski başkanı Billy Clinton' ın tanıtımıyla kullanılmaya başlanan dijital imza , günlük hayatta kullanılan imzalarda olduğu gibi, dijital imzalar da elektronik ortamda gönderilen bilginin veya e-mail'in kime ait olduğunu göstermek için kullanılır. Dijital imzaların oluşturulmasında ve doğrulanmasında dijital sertifikalar kullanılır. Gönderdiğiniz veriyi imzalamak için kendinize ait bir dijital sertifikanız bulunmalıdır.

Dijital imzanın başlıca özellikleri uzmanlar tarafından şöyle sıralanıyor:

1. Dijital imza bir kullanıcı, sunucu ya da host'tan gönderilen bilgilerin kesinlikle o kuruma veya kişiye ait olduğunu doğrulayarak, verinin başkası tarafından yollanmadığını garanti eder.

2. Dijital imza, veri akışı sırasında bilgilerin içeriğini korur, bir başka kişinin eline geçmesini ya da değiştirilmesini engeller, bilginin sadece alıcıya gittiğini ve sadece alıcı tarafından okunacağını garanti eder.

3. Dijital imza, veriyi gönderenin ve alanın kim olduğunun kanıtlanmasına imkan tanır. Yani imzalanmış bir dokümanı yollayan kişi onu yolladığını inkar edemez ve alıcı da aldığını inkar edemez.

Alternatif Güvenlik Olabilecek Bir Uygulama: E-para

e-para, tam olarak, kullandığınız bilgisayarın sabit diskinde sizin adınıza bulunan, ve internet üzerinde yaptığınız alışverişlerde harcayabileceğiniz paradır. Siz harcama yaptıkça, harcadığınız miktar toplamdan düşülür. e-para kullanımı pek yaygın değildir. Ancak, gelecekte sık kullanacağımız bir araç olabilir. Aşağıdaki satırlar bazılarımıza şu an bir fantazi gibi gelebilir.

Temel olarak, gidip, e-para servisi veren bir bankadan, kredi kartımızla ya da peşin ödemeyle, bir miktar e-para alıyoruz. Daha sonra, banka bu miktarı bizim bilgisayarımıza transfer ediyor.Internet üzerinde bir alışveriş yaptığımızda da, eğer burada e-para geçiyorsa, sipariş formunda e-para ile ödeme yapılacağını belirtiyoruz. Miktar otomatik olarak bilgisayarımızdaki miktardan düşülüyor. Bütün bu işlemler, e-para servisi veren bankamızdan da kontrol ediliyor. Bazı uygulamalarda, e-para ödemesi doğrudan bankadan yapılıyor. Bu durumda, size bir e-posta mesajı ile, ilgili siparişi alıp almayacağınız soruluyor. Böylece, alışverişlerde, fiziksel olarak alışageldiğimiz "para dolaşımı" ortadan kalkıyor.

En popüler 3 dijital para sistemi şunlardır : Digital Cash (http://www.digicash.com), Cyber Cash (http:www.Cybercash.com) ve First Virtual (http://www.fv.com). Ilgili yerlere web listeleyicinizle bağlanıp daha ayrıntılı bilgiler alabilirsiniz. Tüm dünyada, e-para kabul eden banka sayısı ise hızla artmaktadır.

Kredi Kartı Sahiplerine Uzmanlardan Öneriler

• Alışveriş yaptığınız sayfanın güvenilir olduğunu anlamanın en kesin yolu, kredi kartınızla ilgili bilgileri gireceğiniz sayfanın Internet adresindeki "http" nin "https" ye dönüşmesidir. Bu dönüşüm firmanın sanal mağazasının bulunduğu sitenin SSL güvenlik protokolünü kullandığını gösterir.

• Internet üzerinde sanal alışveriş hizmeti veren firmalar, sanal alışverişin güvenliğini sağlayan standartlar ve teknolojiler kullanmaktadır. Internet tarayıcınızın Explorer veya Netscape olmasına bağlı olarak kilit ikonu kilitlenmiş ve anahtar ikonunun kırık olmadığı sayfalar güvenli sayfalardır. Fakat bu durum tarayıcı versiyonlarına göre ve sertifikanın alındığı sertifikasyon kurumuna göre değişiklik gösterebilir.

• Güvenilir ve isim sahibi sitelerden yaptığınız alışverişlerinizde güvenlik açısından bir problem çıkması ihtimali çok düşüktür. Tanımadığınız veya güvenliğinden emin olmadığınız bir siteden alışveriş yapmanız gerekiyorsa limiti düşük bir kredi kartı kullanınız.

• Satın aldığınız ürün ile ilgili teslim tarihi, ilave ücretler, garanti koşulları gibi detaylara çok dikkat ediniz.

• Satın alma işleminizin bittiğini belirten mesajı yazıcıdan çıkartarak saklayınız.

• Kredi kartı ekstrelerinizi dikkatle inceleyiniz, şüphe duyduğunuz bir harcamayı bankanıza bildiriniz ve takip ediniz.

Türkiye İçin Neler Yapılabilir ?

Elektronik ticaret konusunda yasal düzenlemelerini tamamlamış örnek bir ülke(şu an için) olmadığı gibi, uluslararası platformlarda, bu konuda tartışmalar da devam etmektedir. Türkiye gibi gelişmekte olan ülkelerin, gelişmiş ülkelere göre geride kaldığı söylenemez. Ancak, elektronik ticarette yaşanan hızlı gelişme, ülkemizde, fiziki alt yapı eksikliklerinin hızla tamamlanmasını ve gerekli yasal düzenlemelere ilişkin çalışmaların bir an önce başlatılmasını zorunlu kılmaktadır.

Ülkemizde elektronik ticaretin üç aşamada gerçekleştirilebileceğini söylemek mümkündür.

- Birinci aşama, bilgisayar ağları üzerinden bilgi ve belgelerin değişimidir. Bu konuda ülkemizde de kapalı sistemlerde başarılı uygulamalar vardır. Ancak, açık sistemler üzerinde ulusal ve uluslararası veri değişimi için, örneğin BM/EDIFACT gibi bir standardın uluslararası düzeyde kabul edilmesi gerekmektedir.

- İkinci aşama, sipariş verme, faturalama, sözleşme yapma, sigortalama, nakliye ve ödeme gibi işlemlerin elektronik ortama aktarılmasıdır.

- Üçüncü aşama ise, sayısal imzaya yazılı imza statüsü kazandırılması, elektronik kayıtların belge olarak kabul edilmesi, iç ve dış ticaret mevzuatı, gümrük mevzuatı ve elektronik ortamda vergilendirme gibi devletin yetkili olduğu konularda, uluslararası uygulamalar da dikkate alınarak yasal düzenlemelerin yapılmasıdır.

-Dördüncü aşama, internet üzerinden güvenli bir şekilde bilgi ve belge değişiminin sağlanmasıdır. Böylece iç ve dış ticaret mümkün olduğu kadar çok kesime yayılmış olacaktır.

Gönderilecek mesaj özgün bir biçimde kısaltılarak mesajın yeni bir versiyonu elde edilir, buna "hash" adı verilir. Sonra saklı anahtar kullanılarak bu "hash" kodlanır. Bu kodlanmış "hash" dijital imza olarak kullanılır. Mesaj iletilirken bir şekilde değişirse bunun "hash"i ilk mesajdan farklı olur. Yani dijital imza mesaj ve saklı anahtara özgüdür. Dijital imza mesaja eklenir ve mesajla birlikte alıcıya gider. Alıcı mesajı, şifrelenmiş "hash"i yollayan kişinin açık anahtarını kullanarak çözer. Bu iki "hash" aynı ise saklı anahtarı sadece gönderen bildiği için bu mesajın gönderen kişiye ait olduğu ve mesajın değişmeden geldiği onaylanmış olur.

Kaynaklar :

The Emerging Digital Economy, U.S. Department of Commerce, 1997,http://www.ecommerce.gov/
The Emerging Digital Economy II, U.S. Department of Commerce, 1999, http://www.ecommerce.gov/
Small and Medium Sized Enterprises and Electronic Commerce, 1998, http://www.oecd.org/

SET Secure Electronic Transfer

SET banka kartları ve ödemeler ile ilgili bilgilerin güvenliğini sağlamak amacıyla Visa, Mastercard, Microsoft, Netscape, GTE, IBM, SAIC, Terisa Systems ve Verisign'ın katılımıyla oluşan bir konsorsiyum tarafından geliştirilmiştir. SET uyumlu ilk alışveriş, 18 Temmuz 1997'de San Francisco'da yapılan tanıtımla İspanya ve Singapur'da bulunan sanal mağazalardan gerçekleştirilmiştir. Garanti Bankası Şubat 1998'de gerçekleştirdiği SET uyumlu alışverişle, bu protokolü kullanmaya başlayan Dünya'da yedinci, Avrupa'da dördüncü ve Türkiye'de ilk kuruluş olmuştur.

SET protokolünde alışveriş, sanal cüzdan ve sertifika aracılığı ile daha güvenli bir ortamda gerçekleştirilir. SET, alışveriş işlemi sırasında ödeme bilgisi gizliliğini, kart kullanıcısının gerçek kart sahibi olduğunu ve işyerinin banka ile anlaşmalı bir işyeri olduğunu garantiler.

SET sisteminde provizyon işlemi müşteri alışveriş seçimini yaptıktan sonra müşterinin sanal cüzdanı ile mağazanın Sanal POS'unun (V-POS) birbirlerinin gerçekliklerini dijital sertifikalar aracılığıyla kontrol etmeleri ile başlar. Mağazanın Sanal POS yazılımı sipariş tutarını ve sanal cüzdanda bulunan ve alışveriş için seçilen kredi kartının sertifika bilgilerini bankaya iletmesi ile devam eder. Banka yapılan alışverişin içeriğini (malın ne olduğu, kaç tane alındığı vb.) görmeksizin provizyon verir. Müşterinin kredi kartı bilgilerini görmeyen sanal mağaza ise bankadan gelecek onayı bekler. Onayı aldıktan sonra da ürünü alıcısına gönderir.

SET sistemi (SSL'de olduğu gibi) işyeri ve banka arasındaki veri akışı sırasında bilgilerin şifrelenerek gönderilmesi esasına dayanır. Bu sistemden faydalananabilmek için kullanılmak istenen kredi kartının SET uyumlu olması gerekir. SET protokolünü kullanmak isteyen kredi kartı sahipleri iki ön koşulu yerine getirmek zorundadırlar: Öncelikle kullanmak istedikleri her bir kredi kartı için sertifikasyon kurumu (Certificate Authority) ayrı birer SET sertifikası almalıdırlar. Ardından kart sahipleri yine kredi kartı veren bir bankadan sanal cüzdan adı verilen bir programı alıp bilgisayarlarına yüklemeli ve bu yükleme sırasında SET sertifikalı kredi kartlarını programa tanıtmalıdırlar. SET uyumlu alışverişler sanal cüzdanın yüklü olduğu bilgisayar kullanılarak SET uyumlu mağazalardan yapılabilecektir. Sanal cüzdan programı en fazla üç kez yüklenmek üzere yazıldığından en fazla üç bilgisayarda kullanılabilecektir. SET protokolünün SSL'e göre çok daha yüksek denebilecek güvenliğine rağmen yeterince yaygınlaşamaması sanal cüzdanın mobilitesinin olmamasına bağlanabilir. Bu yüzden Garanti Bankası sistemi SET uyumlu olmasına karşın SET protokolünü tam olarak uygulamamaktadır. Sanal mağazalar ise Sanal POS (Point of Sale) olarak adlandırılan V-POS yazılımını yükledikten sonra bir sertifikasyon kurumundan (www.verisign.com, www.gte.com) dijital bir sertifika alarak alışverişlerin güvenliğini sağlarlar.

SET ile gerçekleşen alışveriş sırasında gerçekleşen işlemler sırasıyla aşağıdaki gibidir:

SET protokolü, kart sahibi Internet üzerinde araştırmasını tamamlayıp seçimini yaptıktan ve siparişini verdikten sonra devreye girmektedir. SET işleminin başlamasından önce kart sahibi sipariş formunu doldurmuş ve onaylamış olmalıdır. Kart sahibi ayrıca kart türünü de seçmiş olmalıdır.

1. Kart sahibinin yazılımı satıcı firmaya kullanılacak kredi kartını belirten ve ödeme altyapısını sağlayan kuruluşun sertifikalı açık anahtarının kopyasını isteyen bir mesaj gönderir.

2. Satıcı firmanın yazılımı mesajı aldığında, sadece o mesaja özel bir işlem tanımlama numarası belirler. Daha sonra bu özel tanımlama numarasıyla beraber kart sahibine satıcı firmanın açık anahtarını ve ödeme altyapısını sağlayan kuruluşun (genelde bankalar) onaylı açık anahtarını gönderir.

3. Kart sahibinin yazılımı satıcı firmanın ve ödeme altyapısını sağlayan kuruluşun sertifikalarını kontrol eder ve sipariş sürecinde kullanmak üzere bunları kaydeder. Kart sahibinin yazılımı sipariş bilgisini ve ödeme talimatlarını oluşturur. Yazılım satıcı firma tarafından belirlenen özel tanımlama numarası ile sipariş bilgisini ve ödeme talimatlarını ilişkilendirir. Bu tanımlama daha sonra satıcı firma tarafından ödeme talebi yapıldığında, ödeme altyapısını sağlayan kuruluş tarafından sipariş bilgisini ve ödeme talimatlarını ilişkilendirmede kullanılacaktır.

4. Kart sahibinin yazılımı sipariş bilgisi ve ödeme talimatları için bir dijital imza oluşturur. Yazılım daha sonra ödeme altyapısını sağlayan kuruluşun açık anahtarını kullanarak dijital olarak imzalanan ödeme talimatlarını şifreler. Son olarak yazılım imzalanmış ve şifrelenmiş sipariş bilgisini ve ödeme talimatlarını bir mesajla satıcı firmaya gönderir.

5. Satıcı firmanın yazılımı siparişi alır ve kart sahibinin açık anahtarı üzerindeki dijital sertifikayı kontrol eder. Bundan sonra gene bu açık anaharı kullanarak siparişin gerçekten kart sahibinden geldiğinden ve mesajın gönderim esnasında değiştirilmediğini teyit eder (Satıcı firma ödeme talimatları ödeme altyapısını sağlayan firmanın açık anahtarı ile şifrelendiği için deşifre edemez).

6. Bu işlemlerin ardından satıcı firmanın yazılımı ödeme onayı istenmesi de dahil olmak üzere siparişle ilgili işlemlere başlar (lütfen 9. Maddeye bakınız)

7. Sipariş bilgisi işleme alındıktan sonra, satıcı firmanın yazılımı bir cevap mesajı hazırlar ve dijital olarak imzalar (satıcı firmanın onaylı açık anahtarı ile). Kart sahibinin siparişinin alındığının ve işleme konulduğunun bildirilmesi amacıyla hazırlanan cevap mesajı kart sahibine gönderilir.

8. Kart sahibinin yazılımı satıcı firmadan cevap mesajını aldığı zaman dijital sertifikasını kontrol eder. Bunun ardından bu mesajı kullanarak kart sahibine bir teyit mesajı gösterir veya siparişin durumunu günceller.

9. Kart sahibinden gelen siparişlerin işleme konulması esnasında (lütfen 6. maddeye bakınız) satıcı firmanın yazılımı ödenmesi talep edilen tutarı, sipariş bilgisindeki işlemi belirleyen özel tanımlama numarasını ve işlemle ilgili diğer bilgileri içeren bir ödeme onay talebini hazırlar ve bu mesajı dijital olarak imzalar. Ardından bu talep ödeme altyapısını sağlayan kuruluşun açık anahtarı kullanılarak şifrelenir. Satıcı firmanın ödeme onay talebi ve kart sahibinin şifrelenmiş ödeme talimatları ödeme altyapısını sağlayan kuruluşa gönderilir.

10. Ödeme altyapısını sağlayan kuruluş onay talebini aldığı zaman satıcı firmadan gelen onay talebini kendi gizli anahtarını kullanarak deşifre eder. Ardından satıcı firmanın açık anahtarı üzerindeki dijital sertifikayı kontrol eder ve sertifikanın geçerlilik sürerisinin dolup dolmadığını belirler.

11. Ödeme altyapısını sağlayan kuruluş kart sahibinin satıcı firmadan gelen onay talebiyle

birlikte gönderilen ödeme talimatlarını kart sahibinin açık anahtarını kullanarak deşifre eder. Ardından bu açık anahtarı kullanarak kart sahibinin ödeme talimatları üzerindeki dijital imzasını kontrol eder ve böylece ödeme talimatlarının kart sahibi tarafından imzalandığından ve iletim esnasında değişikliğe uğramadığından emin olur.

12. Ödeme altyapısını sağlayan kuruluş satıcı firma tarafından gönderilen işlem tanımlayıcısı ile ile kart sahibinden gelen ödeme talimatlarındaki tanımları karşılaştırarak her ikisininde aynı olup olmadığını kontrol eder. Kontrolün ardından ödeme altyapısının sağlayan kuruluş, kredi kartını veren bankaya Internet üzerinden çalışmayan bir ödeme sistemiyle bir onay talebi gönderir.

13. Kartı veren banka onay talebini işleme alır ve ödeme altyapısını sağlayan kuruluşa güvenli ödeme sistemi aracılığıyla bir cevap gönderir.

14. Onay cevabını aldıktan sonra ödeme altyapısını sağlayan kuruluş kartı veren bankanın cevabını ve onaylı açık anahtarını içeren bir onay cevap mesajı yaratır ve dijital olarak imzalar. Cevap satıcı firmanın açık anahtarını kullanarak şifrelenir ve satıcı firmaya gönderilir.

15. Satıcı firmanın yazılımı ödeme altyapısını sağlayan kuruluştan onay cevabını aldığı zaman kendi gizli anahtarıyla deşifre eder. Ardından ödeme altyapısını sağlayan kuruluşun açık anahtarı üzerindeki dijital sertifikayı kontrol eder ve bu açık anahtarı kullanarak ödeme alyapısını sağlayan kuruluşun onay cevap mesajındaki dijital imzayı kontrol eder. Satıcı firmanın yazılımı, sipariş tamamen yerine getirildikten sonra ödeme talebinde bulunulabilmesi için (gün sonu işlemi ile) bu onay cevap mesajını kaydeder.

16. Satıcı firma onay cevabını aldıktan sonra kart sahibinin siparişi tamamlar ve ilgili ürünü sevkeder veya sözkonusu hizmeti verir.

17. Siparişi yerine getirdikten sonra satıcı firma ödeme talebinde bulunur (Siparişin tamamlanması esnasındaki gecikmeler onay talebi ile ödeme talebi mesajları arasında önemli zaman aralıkları oluşmasına yol açabilir).

18. Ödeme talebinde bulunmak için satıcı firmanın yazılımı işlemin nihai tutarını, sipariş bilgisindeki işlem tanım numarasını ve işlem hakkındaki diğer bilgileri içeren bir gün sonu işlemi oluşturur ve dijital olarak imzalar. Bu talep ödeme altyapısı sağlayan kuruluşun açık anahtarı ile şifrelenir ve ödeme sağlayan kuruluş gönderilir.

19. Ödeme altyapısını sağlayan kuruluş gün sonu işlemi talebini aldığı zaman, kendi açık anahtarını kullanarak talebi deşifre eder. Daha sonra satıcı firmanın açık anahtarını kullanarak gün sonu işlemindeki dijital imzayı kontrol eder. Satıcı firmadan gelen gün sonu işlemiyle, daha önce işleme alınan onay talebini karşılaştırır ve bir tahsilat talebi oluşturarak bunu kredi kartını veren bankaya güvenli ödeme sistemiyle gönderir.

20. Ödeme altyapısını sağlayan kuruluş kendi onaylı açık anahtarını içeren bir gün sonu cevap mesajı oluşturur ve bunu dijital olarak imzalar. Bu cevap satıcı firmanın açık anahtarı ile şifrelenerek satıcı firmaya gönderilir. Bu mesaj sayesinde gün sonu işleminin ödeme altyapısını sağlayan kuruluş tarafından alındığını ve işleme konulduğunu satıcı firmaya bildirir.

21. Satıcı firmanın yazılımı ödeme altyapısını sağlayan kuruluştan gün sonu işleminin cevabını alınca, mesajı kendi gizli anahtarını kullanarak deşifre eder. Ardından ödeme altyapısını sağlayan kuruluşun açık anahtarı üzerindeki dijital sertifikayı kontrol eder ve yine bu açık anahtarı kullanarak ödeme altyapısını sağlayan kuruluşun dijital imzasını kontrol eder. Son olarak satıcı firmanın yazılımı günsonu işlemi cevabını yapılan ödemeler için gönderilen günsonu talep mesajları ile mutabakat için kaydeder.