CLEARİNGHOUSE KAVRAMI VE TÜRKİYE'DE KART DOĞRULAMA SİSTEMİ OLUŞTURMA SÜRECİ

ÖZET

Bu çalışmanın amacı Türkiye'de bir kart doğrulama sistemi kurmak için gereken yasal ve bilişimsel altyapıyı açıklamaktır. Bu doğrultuda ilkin takas odaları (clearinghouse) ve bunların işleyişi üzerine literatür taraması yapılmış, ardından VISA ve MasterCard gibi uluslararası kart doğrulama sistemleri incelenmiş ve 3-D Secure doğrulama sisteminin işleyişine ve protokolüne değinilmiştir. Ardından Türkiye bağlamında Takasbank'ın merkezi takas hizmetlerindeki rolüne ve Bankalararası Kart Merkezi (BKM) tarafından geliştirilen Türkiye'nin Ödeme Yöntemi'ne (TROY) değinilmiştir. Son bölümde Türkiye'de bir doğrulama sistemi kurmak için gerekli olan yasal süreçler, sertifikasyonlar ve standartlar ele alınmıştır. 6493 sayılı Kanun ve ilgili yönetmeliklere göre TCMB'den faaliyet izni alınması gerektiğini, faaliyet izni alınması için sistem işleticisi olmak gerektiğini ve bunun için haiz olunması gereken şartların ne olduğu açıklanmıştır. Veri güvenliği için KVKK çerçevesinde sorumluluklar; kimlik doğrulama süreçlerinde ise 31676 sayılı Tebliğ'deki minimum gereklilikler ve ödeme geçidi gibi sistemlere değinilmiştir. Ayrıca PCI DSS ve EMVCo gibi uluslararası standartlara uymanın zorunlu olduğuna ve bu standartların neler olduğuna da değinilmiştir. Çalışma Türkiye'de oluşturulacak bir doğrulama sistemi için atılması gereken adımlara yönelik yol haritası sunmaktadır.

Anahtar Kelimeler: Takas Odası, Merkezi Karşı Taraf, Ödeme Sistemi, TROY, PCI DSS, Kimlik Doğrulama Sistemi, 3-D Secure, 6493 Sayılı Kanun.

GİRİŞ

Takas odası anlamına gelen clearinghouse, finansal piyasalarda işlem gören varlıkların alıcıdan satıcıya güvenli ve etkin bir şekilde aktarılmasını sağlayan kuruluş veya mekanizmadır. Takas odaları, küresel finansal altyapının çok önemli bir unsurunu temsil eder (Baker, 2016: 4); borsalar, hisse senetleri ve emtia (ticareti yapılabilir mallar) türevleri gibi çeşitli menkul kıymetlerin alımları ve satımları için bir pazar yeri sağlarlar (Yadav, 2012: 408).

Finansal anlamda türev, değeri bir dayanak varlığın değerine göre belirlenen bir araçtır (Russo vd., 2002: 59). Bir benzer tanımlamada ise türevler, değerlerini bir finansal varlık, bir varlık demeti, bir emtia, bir faiz oranı veya pratik olarak ölçülebilen ve nesnel olarak doğrulanabilen temel bir referans varlıktan türeten finansal sözleşmelerdir (Baker, 2016: 5).

Türev işlemler, yapılandırılmış borç yükümlülükleri ve mevduatlar, takas sözleşmeleri, vadeli işlem sözleşmeleri, alım/satım seçenekleri, faiz tavanı, faiz tabanı, faiz oranı aralığı kontrolü, vadeli işlemler ve bunların çeşitli kombinasyonları gibi bir dizi finansal sözleşmeyi içerirler (OCC, 2024) ve hem düzenlenmiş borsalarda hem de tezgâh üstü piyasalarda işlem görürler (Baker, 2016: 6). "Türev işlemler geleceğe dair beklentiler doğrultusunda oluşan risklerin yönetildiği piyasalardır. Risklerden korunmak isteyen yatırımcılar, risk alarak kazanç sağlamak isteyen spekülatörlere risk transferi yapmaktadırlar. Burada her iki taraf da beklentilerine göre pozisyon alır." (Gündoğdu, 2023: 30-31). Spekülatörler, gelecekteki döviz kuru fiyat hareketlerini tahmin etmeye çalışarak böylesine büyük bir riskin hakkını verecek kadar kazançlar elde etmeyi umarlar (Rusk, 2024: 101).

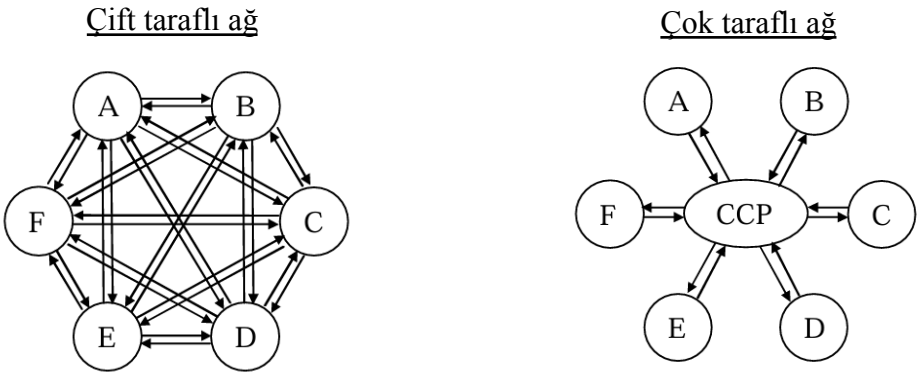
Takas Odaları, Tezgâh Üstü Piyasalar ve Merkezi Karşı Taraf

Takas odalarının sağladığı türev işlemler ve çeşitli pazar yerleri alıcı ve satıcıları bir araya getirerek onlara şeffaf fiyatlandırma yapıları sağlar ve borsada kullanılan sözleşmelerin tamamen standartlaştırılmasını zorunlu hâle getirir. Takas odalarının böyle bir işlev amacıyla kurulmalarının sebebi, finansal piyasa ticaretinde güvenliği ve kesinliği sağlayarak olası risk faktörlerini en az seviyeye indirmek içindir (Chang, 2014: 751; Yadav, 2012: 408). Risk faktörlerini en az seviyeye indirmek çift taraflı (tezgâh üstü piyasa) gerçekleşebileceği gibi merkezi karşı taraflar vasıtasıyla da gerçekleşebilir (Friesz ve Váradi, 2021: 398).

Tezgâh üstü piyasalar (OTC), merkezi takas noktası olmaksızın, iki ticaret ortağının doğrudan birbirleriyle pazarlık yaptığı ve alım satım işlemlerini telefon ya da bilgisayar vasıtasıyla gerçekleştirdikleri piyasalardır (Gündoğdu, 2023: 125). OTC piyasalarında ticaret genellikle bayiler aracılığıyla yapılır. Bayiler sıklıkla alım satım görüşmeleri yapıp bilgi alırken müşteriler genellikle daha sınırlı alım satım fırsatlarına sahip olduğu için son işlemler hakkında bayilere nispeten daha az bilgiye sahiptir. Bu durum sonucunda piyasaya erişim ve hakimiyet dereceleri farklı olduğundan bayiler pazarlık avantajını kendi ellerinde bulundururlar (Duffie, 2012: 2). OTC piyasalarında fiyatlar ve tahsisler kurumlardan ve bayilerden etkilendiği için şeffaflıktan oldukça uzakta konumlanırlar (Duffie, 2012: 1). Bu risk faktörlerinden ötürü, karşı tarafların tüm işlemlerini kapsayan bir teminat anlaşması yapmaları gerekmektedir. Bu anlaşmayı yapabilmek için Credit Support Annex (CSA) adı verilen, taraflarca teminat sağlanmasına ilişkin şartları tanımlayan kredi destek eki belgesini imzalamak gerekmektedir (Alavian vd., 2008: 3). Ancak bu her kurumun karşılayabileceği bir

teminat değildir. Kredi destek eki çoğu zaman nakit teminatı eksikliği, karşı taraf kredi riskinin bir türü olan (Risk, 2024.) yanlış yol riski gibi nicel sorunları da beraberinde getirebilmektedir (Kamtchueng, 2011: 6).
Ayriyeten OTC piyasaları, karşı tarafın iflası, temerrüde düşmesi, yani ödeme yükümlülüklerini yerine getirememesi (Gündoğdu, 2023: 125) gibi faktörler sebebiyle, sözleşmede belirtilen şekilde ifa edememe gibi risk faktörlerini de ortaya çıkarır ve bu yüzden Credit Valuation Adjustment (CVA) adı verilen, karşı tarafın temerrüt riski dikkate alınarak yapılan fiyat ayarlamasına dayanan kredi değeri ayarlaması sözleşmesi imzalamak gerekir (Duffie, 2012: 8). OTC türevleri yaygın olarak sistemik risk yaratma konusunda doğal bir yeteneğe sahiptir. OTC türevlerinde karşı taraf riskine artan odaklanma sebebiyle merkezi takasa önemli bir ilgi oluşmuştur (Gregory, 2010: 1).

Merkezi karşı taraf (MKT), karşı taraf kredi riskini üstlenip yönetir (Yadav, 2012: 409), takas yaptığı üyelerinin türev risklerinden kaynaklanan olası temerrüt kayıplarını sigortalamalarına yardımcı olur, temerrüde düşmesi anında ifasını garanti eder (Gregory, 2010: 3) ve karşı taraf kredi riskini (KKR) karşılıklı hâle getirir (Fiedor, 2018: 1). KKR, sözleşme taraflarından birinin yükümlülüklerini yerine getirememesi ve sözleşme şartlarını karşılayamaması olasılığına dayanan bir risktir (Rehlon ve Nixon, 2013: 148). Böylelikle MKT, çift taraflı takasın olası risk faktörlerini kendi üzerine alır (Yadav, 2012: 410); alıcı için satıcı, satıcı için alıcı olur ve risk ağının merkezine kendisini yerleştirir (Berndsen, 2021: 2012; Chang, 2014: 751). Bilgi toplama, izleme ve risk yönetiminin merkezine yerleşmesi sonucunda takas üyeleri için işlem maliyetlerini azaltır (Baker, 2016: 25).

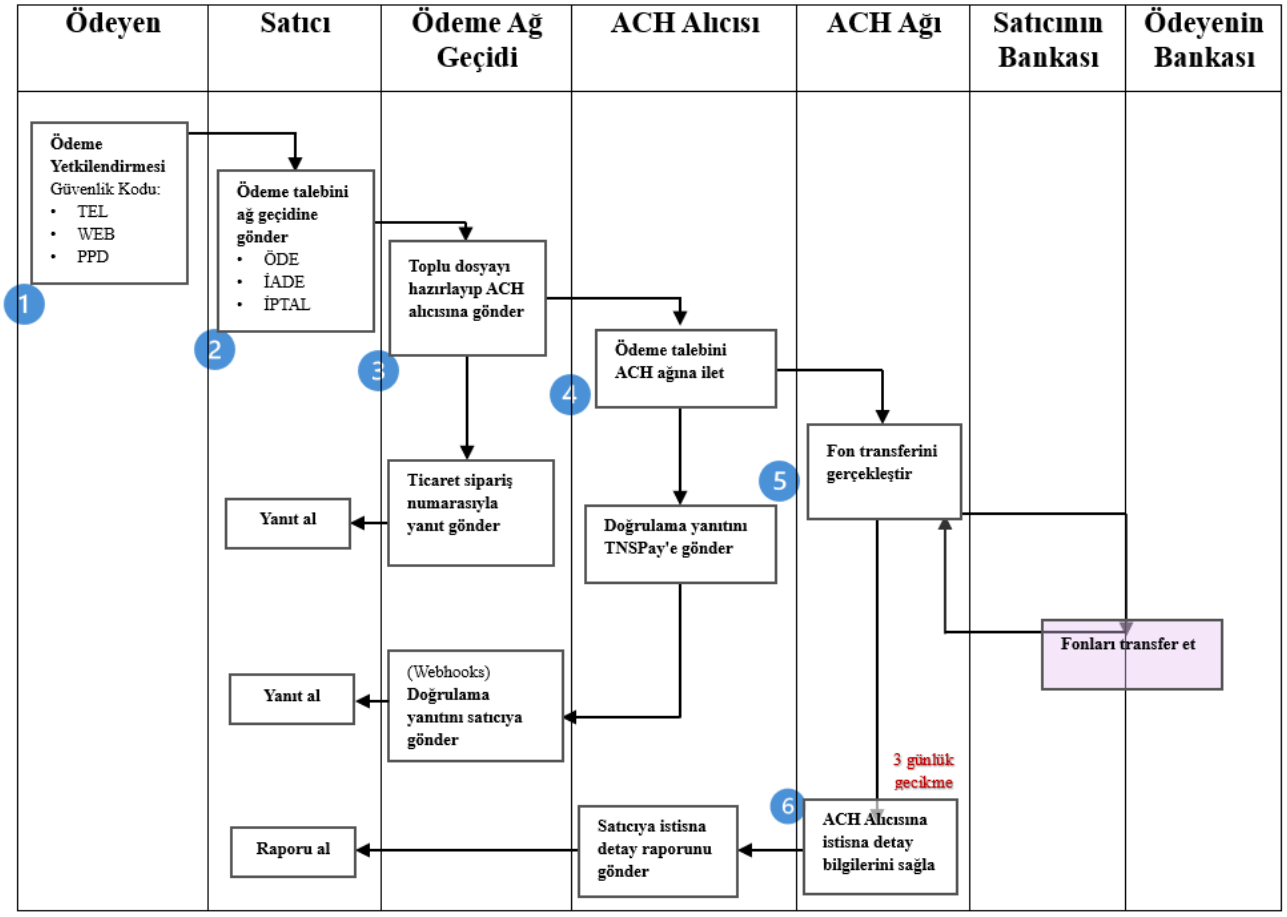


Şekil 1: Çift taraflı ve çok taraflı takas ağının karşılaştırılması (Gregory, 2010: 3).

Şekil 1'e bakarsak açıkça görülüyor ki, merkezi karşı taraf (çok taraflı ağ) ağın ortasına kendisini yerleştiriyor ve tüm olası riskleri kendi üzerine alıyor. Buna mukabil çift taraflı ağa (tezgâh üstü ağ) baktığımızda ise bütün riskler karşı taraflar arasında konumlanmaktadır. Tezgâh üstü piyasa ile mukayese ettiğimizde şeffaflık ve güvenlik bakımından merkezi karşı tarafın çok daha ön planda olduğu göze çarpmaktadır.

Otomatik Takas Odası

Otomatik takas odası (ACH) fikri, ilk defa 1968 yılında San Francisco ve Los Angeles takas odası birliklerinin elektronik bir takas odasının nasıl oluşturulacağını incelemek üzere bir komite kurmasıyla ortaya çıkmış, 1972 yılında ise ABD'de Federal Rezerv Sistemi (FED) tarafından işletilen ilk ACH Kaliforniya'da kurulmuştur (McAndrews, 1994: 17; Bradford, 2007: 1). ACH, yinelenen ödemeler yapmak için kullanılan yaygın bir elektronik ödeme mekanizmasıdır (Committee on Payment and Settlement Systems [CPSS], 2012: 485). ACH işleminin gerçekleşmesi için işlemin her iki tarafındaki bankaların bu mekanizmayı benimsemesi gerekmektedir (Ackerberg ve Gowrisankaran, 2003: 2); çünkü ACH, bankaları birbirine bağlayan elektronik bir sistemdir. Bankalar, işlem merkezindeki bir bilgisayara bağlı başka bir bilgisayar kullanırlar ve ödeme bilgilerini telefon hatları üzerinden iletirler (McAndrews, 1994: 16). FED, FedACH sistemi aracılığıyla Merkez Bankaları Sistemine gönderilen ACH ödemelerini işlemek için kullanılan yazılımı yönetir ve bakımını yapar. FedACH sistemi, işlemlerin güvenli ve verimli bir şekilde sonuçlandırılmasını sağlar (CPSS, 2012: 493).



Şekil 2: Otomatik Takas Odası Veri Akışı (Mastercard, 2024).

https://eu-gateway.mastercard.com/api/documentation/integrationGuidelines/supportedFeatures/pickPaymentMethod/achPayments.html?locale=en_US#h2_Automated_Clearing_House_Data_Flow

Kısa süre sonra ülke çapında başka ACH birlikleri de kurulmuştur ve bölgesel ACH ağlarını işletmek için tesisler, ekipmanlar ve personeller gibi gereklilikleri sağlamak için anlaşmalar yapılmıştır. 1978 yılında gelindiğinde FED ile birlikte yerel ACH birlikleri ülke çapında birbirlerine bağlanmıştır (Bradford, 2007: 1).

Elektronik Ödeme Sistemleri: VISA ve MasterCard

Elektronik ödemeler, nakit içermeyen elektronik ortam kullanan ödeme mekanizmalarıdır. Elektronik ödeme sistemleri, işlem sistemleriyle ilgili çeşitli kuruluşları birbirine bağlayan ve bireysel müşterilerle bağlantı kuran bir tür kuruluşlar arası bilgi olarak da tanımlanabilir (Fatonah vd., 2018: 2).

VISA Nedir?

VISA, dünya çapında 20.000'den fazla finansal kuruluşun ortaklığıyla oluşturulan bir kooperatif üyelik birliğidir. Bu kuruluşlar, çoğunlukla bankalardan oluşur ve aynı anda hem VISA'nın sahipleri hem de müşterileridir. Üye bankalar, kart çıkarma ve üye işyeri kazanma konularında birbirleriyle rekabet halindedir. Ancak VISA, bu rekabetin işbirliği içinde sürdürülebileceği bir yapı sunar. VISA, doğrudan bir banka işlevi görmez; bu nedenle kart çıkarma, üye işyeri kazanma, kredi verme, hesap yönetimi veya ödenmemiş bakiyelere faiz uygulama gibi işlemleri gerçekleştirmez (Stearns, 2007: 3).

"VISA, üç temel işleve hizmet etmektedir. İlki, işlemlerin kabul edildiği ve anlaşmazlıkların çözüldüğü kuralların sürdürülmesi, yorumlanması ve uygulanmasıdır. İkincisi, bu işlemleri elektronik ortamda yetkilendiren, takas eden ve sonuçlandıran dünya çapındaki bilgisayar sistemlerini ve telekomünikasyon ağlarını sağlaması ve işletmesidir. Üçüncüsü ise, VISA adını ve hizmet markalarını genel reklam ve ticari sponsorluklar yoluyla tanıtmalarıdır" (Stearns, 2007: 3).

VISA'nın Elektronik Yetkilendirme Sistemi: BASE I ve BASE II

BASE I, kredi kartı ödemelerinde güvenli ve kesintisiz bir hizmet sunmak amacıyla geliştirilmiş (Stearns, 2007: 94) ilk elektronik yetkilendirme sistemidir (Investopedia, 2022). Merkezî bilgisayar prensibiyle çalışan BASE I; kart sahipleri, satıcılar ve üye bankalar için birincil iletişim noktası olarak hizmet ederek işlemlerin gerçek zamanlı olarak onaylanmasını veya reddedilmesini sağlamaktadır (Stearns, 2007: 93, 132).

BASE I, kendisinden önceki yavaş ve hantal olan manuel yetkilendirme süreci gibi organizasyonel sorunlara bir çözüm sağlamıştır (Stearns, 2017: 101). Ancak takas işlemlerinin takası ve mutabakatı, yetkilendirme, dolandırıcılık gibi operasyonel sorunlar hâlen çözümlenmiş değildi (Stearns, 2007: 81, 101) ve bu yüzden BASE II'nin çıkması gerekiyordu (Stearns, 2007: 107).

BASE II, ACH fikrinin ilk uygulaması olmamakla birlikte en büyük, en iddialı; ulusal kapsamda ve banka kartları arasındaki ilk uygulama olmuştur. Merkezi takas odası olarak

hareket eden BASE II ile birlikte kağıt alışverişinin yerini elektronik kayıtlar almıştır. Elektronik işlemler telekomünikasyon hatları üzerinden iletildiğinden saate bakılmaksızın BASE II aracılığıyla takas ve mutabakat yapılabiliyordu ve üyeler takas işlemlerini birbirleriyle değil, takas merkezi aracılığıyla gerçekleştiriyorlardı (Stearns, 2007: 106).

MasterCard Nedir?

MasterCard, tıpkı VISA gibi, binlerce üye bankadan oluşan kooperatifler olarak örgütlenmiştir. Bu nedenle her ikisi de bazen "dört taraflı sistemler" olarak adlandırılmaktadır. Dört taraflı sistemler; satıcı, ödeyen, satıcının bankası ve ödeyenin bankasından oluşur (Chang, 2004: 37). MasterCard, merkezi operasyonları yürütürken işin büyük kısmını (kâr elde etme çabaları dâhil) bireysel üyelerin eline bırakır. "MasterCard, MasterCard olmaktan para kazanan bir işletme değildir; MasterCard'ın reklamları üyelerin kart satmasına yardımcı olur ancak MasterCard'ın kasalarını doldurmaz" (Chang, 2004: 31). Yine tıpkı VISA'da olduğu gibi, MasterCard'da bir banka değildir ve herhangi bir kart çıkarmaz, kredi vermez ve bireysel kart hesaplarına hizmette bulunmaz. MasterCard, MasterCard'ı kabul eden satıcılarla doğrudan sözleşme yapmak yerine üye işyeri başarısızlığı ile ilişkili riskleri önlemek amacıyla işletmelerin düzenlemelere tabi bir finansal kuruluşla kurduğu anlaşma aracılığıyla ağa katılmalarını tercih etmektedir. Yani MasterCard doğrudan işletmelerle değil, bankalar gibi düzenlemelere tabi finansal kuruluşlar aracılığıyla çalışmayı tercih eder. Böylece ödeme sistemine katılımında doğabilecek riskleri bu güvenilir aracılar üzerinden yaptığı sözleşmelerle yönetir. Sözleşme yapılan banka, kendisi de dâhil olmak üzere aracıların mali yükümlülüklerinden; dolandırıcılıktan korunma ve bilgi güvenliği standartları da dâhil olmak üzere ağ kurallarına uyulmasını sağlamaktan sorumludur (Herbst-Murphy, 2013: 4). Aynı zamanda VISA ve MasterCard, işbirliği yaptıkları faiz oranları, ücretler, yenilikçi teklifler ve hizmetler gibi alanlarda "eş-rekabet" olarak adlandırılan işbirlikçi rekabet modelini benimserler (Evans, 2004: 3).

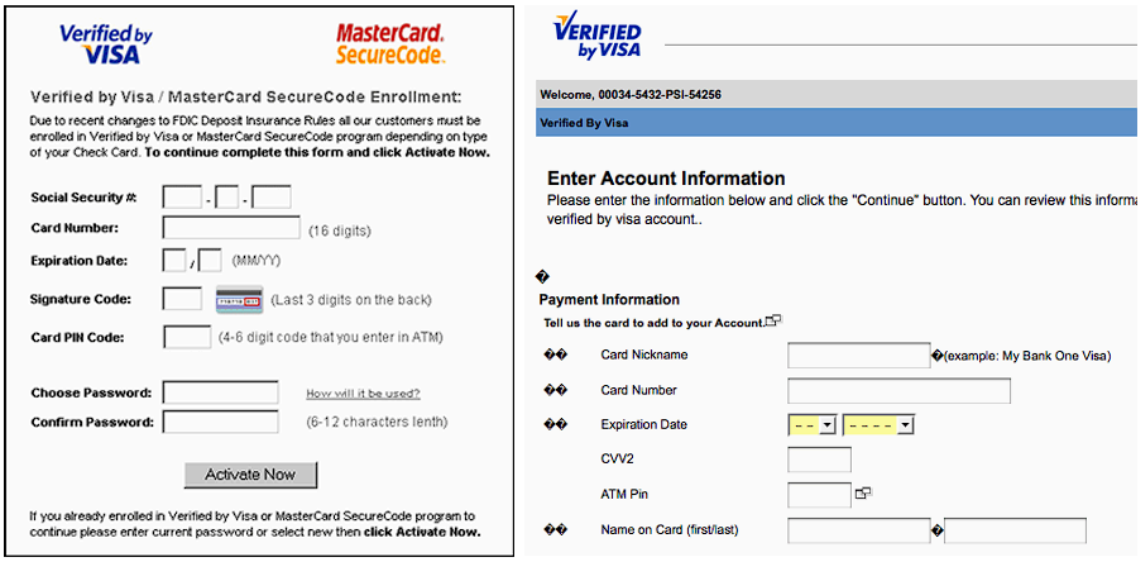
3-D Secure Doğrulama Sistemi

Başta VISA ve MasterCard olmak üzere Netscape ve Microsoft gibi büyük yazılım satıcıları tarafından desteklenen Secure Electronic Transaction (SET), e-ticaret işlemlerini güvence altına almak için tasarlanılan bir protokoldü (Shoniregun ve Zhao, 2007: 313). Ancak SET'in 1000 sayfayı aşan dökümantasyonları, dijital imza ve şifreleme katmanı içeren karmaşık protokolleri (Bella vd., 2005: 18), bu protokoller sebebiyle işlemlerin oldukça yavaş işlemesi, uygulayıcılarla doğrulayıcılar açısından çıkardığı zorluklar ve uygulanmasının hem zaman alması hem de pahalı olması gibi çeşitli sorunları mevcuttu (Merkow, 2004: 247; Shoniregun ve Zhao, 2007: 315). Nihayetinde SET'in ABD'de başarılı olamayacağını anlayan kart birlikleri yeni proje geliştirme aşamasına geçtiler (Merkow, 2004: 255).

"Verified by Visa" ve "MasterCard SecureCode" olarak da bilinen 3-D Secure (3DS) doğrulama sistemi (Murdoch ve Anderson, 2010: 337), internet üzerinden dijital istemciler tarafından yapılan otomatik işlemlerin zarar görmemesini sağlamak için kullanılan XML tabanlı bir sistemdir (Alt ve Huch, 2022: 213). 3DS'nin ortaya çıkışı 2001 tarihine dayanır. 3DS'den önce var olan CardNotPresent (CNP) ödemelerinde müşterinin kart bilgilerini satıcının internet sitesi üzerinden sağlanan ödeme sayfasına girmesi gerekiyordu. Ardından

satıcı kart bilgilerini işlem bilgileriyle birleştirerek yetkilendirme için bankaya iletirdi ve banka bu işlem sırasında onaylamaya ya da reddetmeye karar verirdi. Bilgilerin satıcıyla paylaşıldığı göz önüne alındığında, bu bilgilerin sızması ve istenmeyen işlemlerde kullanılması gibi önemli bir risk faktörü söz konusu olmaktaydı. CNP ödeme sistemini dolandırıcılıktan korumak için 2001 yılında 3-D Secure 1.0 (3DS 1.0) tanıtıldı. Böylelikle CNP ödemeleri için "kimlik doğrulaması" kavramı ortaya çıkmış ve işlemler doğrudan kartı veren kuruluşa yönlendirilip işlemi başlatan kişinin meşru kart sahibi olarak doğrulanabilmesi sağlanmıştır (Ali vd., 2020: 2). Kart sahiplerine tam kimlik doğrulaması sağlayan ve çevrim içi işlemlerin performansını artıran 3DS, kredi veya banka kartı bilgilerini satıcıya değil, doğrudan bankaya sağlayarak güvenli bir işlem gerçekleştirmekteydi. Şifrelenen bilgiler HTTPS protokolü aracılığıyla aktarıldığından bu bilgileri yalnızca banka okuyabiliyordu (Amrita ve Shukla, 2022: 392). 3DS, ilk başlarda teknik eksiklikleri olmasına rağmen bankacıların ve satıcıların ekonomik çıkarlarıyla uyumlu olduğu için yaygın olarak benimsenmiştir (Murdoch ve Anderson, 2010: 341).

Ancak 3DS 1.0 adres çubuğu olmayan bir iframe veya pop-up (açılır pencere) görevi gördüğünden, benzer görünüşteki formlarla oltalama saldırılarına ve diğer kimlik avı saldırı girişimlerine oldukça açık bir yerde konumlanmıştır (Murdoch ve Anderson, 2010: 338).



Şekil 3: Oltalama saldırısı örnekleri (Murdoch ve Anderson, 2010: 339).

2016 yılına gelindiğinde daha güçlü bir kimlik doğrulaması ihtiyacını karşılamak için 3-D Secure 2.0 (3DS 2.0) geliştirilmiştir. 3DS 2.0, zorlu veya sürtünmesiz kimlik doğrulamalarından birini kullanarak ödemeyi başlatan kişinin kimliğini doğrulamaktadır. Zorlu kimlik doğrulama, yüksek riskli işlemler için tasarlanmıştır. Başarılı bir şekilde doğrulamayı tamamlayabilmek için kartı veren kuruluş tarafından kayıtlı cihaza gönderilen tek seferlik şifreyi girmek gerekmektedir. Buna mukabil sürtünmesiz kimlik doğrulaması ise düşük riskli alım satımlar için tasarlanmıştır. Bu doğrulamayı tamamlayabilmekse ödeme esnasında ödeme yapılacak olan cihazdan alınan tarayıcı yapılandırma bilgilerine dayanmaktadır (Ali vd., 2020: 2). Bu bilgiler tarayıcı adı, desteklenen diller ve yüklü diller, işletim sistemi adı ve sürümü, işletim sistemi platformu, tarayıcı ekranı genişliği ve yüksekliği

gibi bilgiler de dâhil olmak üzere çeşitli bilgileri kapsamaktadır (Ali vd., 2020: 3). Bu bilgiler arka kanal kullanılarak üye işyerinin sitesinden 3DS sunucusuna, oradan dizin sunucusuna ve son olarak kartı çıkaran kuruluşun ACS'sine iletilir. Arka kanal doğrudan bir bağlantı olmayıp aşamalı iletişim ağı üzerinden bilgileri iletir. Kartı çıkaran kuruluş, bu bilgiler doğrultusunda kimlik doğrulamanın gerekli olup olmadığına karar verir. Kimlik doğrulama gerekli değilse üye işyeri hemen yetkilendirme işlemini başlatır; gerekliyse, kartı çıkaran kuruluşun ACS'sine bir yönlendirme ile işlem devam eder ve bu aşamada zorlu kimlik doğrulama işlemi başlar (Corella ve Lewison, 2019: 5)

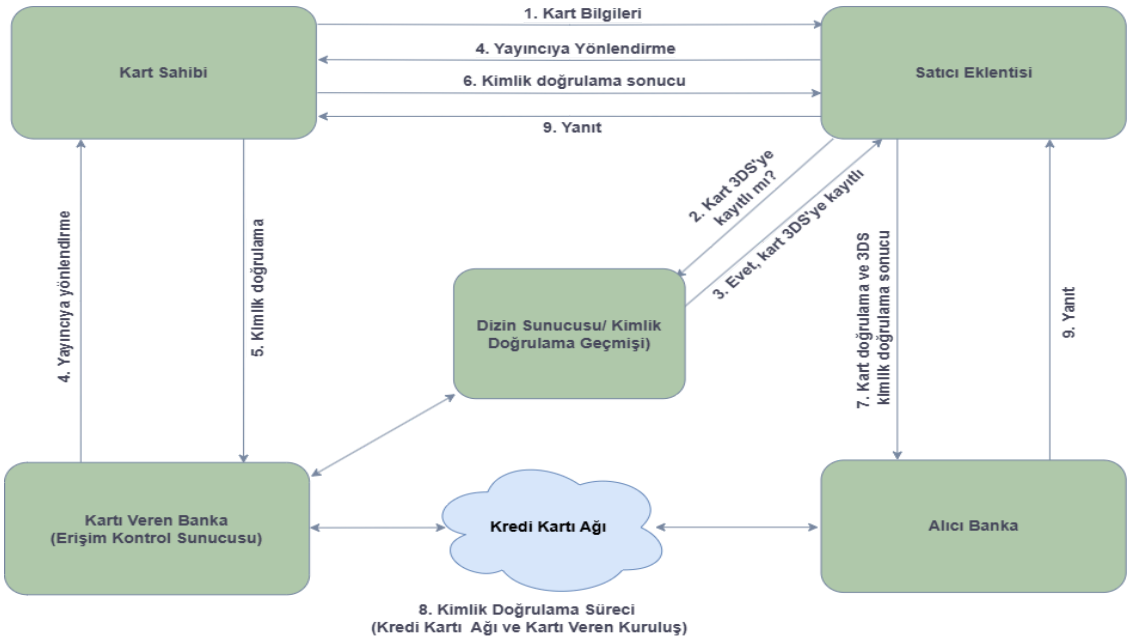
3-D Secure Protokolü

"Üç alan" anlamına gelen 3D; kartı veren kuruluş, ödemeyi alan satıcı ve alıcıyla satıcı arasında güvenli bir geçiş görevi gören 3DS altyapı platformunu temsil etmektedir (Amrita ve Shukla, 2022: 394).

Kartı veren kuruluş, kullanılan kartı sağlayan bankayı ve kart sahibini kapsar. Kartı çıkaran finansal kuruluşların ve müşterilerinin sistemleri ile işlevlerini içerir; örneğin, kart sahibi tarayıcısı, ilgili yazılımlar, kayıt sunucusu, erişim kontrol sunucusu ve kart sahibinin kimlik doğrulama süreçleri bu kapsamda yer alır. Kartı çıkaran kuruluş, kart sahiplerinin kayıt süreçlerini yönetmek ve çevrim içi alışverişlerde kimlik doğrulamalarını gerçekleştirmekle sorumludur (Chowdhary, 2018: 836).

Alıcı alanı, ödemenin gerçekleştirildiği bankayı ve satıcıyı kapsar. Alıcı, hem satıcının hem de müşterilerinin sistemlerini ve işlevlerini içerir; satıcı eklentisi ve imza doğrulama sunucusu bu kapsamda yer alır. Alıcı, internet üzerinden yapılan işlemlerde satıcıları belirli bir satıcı anlaşması çerçevesinde faaliyet göstermesi için gerekli prosedürleri oluşturmak ve kimliği doğrulanmış işlemler için işlem işleme hizmeti sunmakla sorumludur (Chowdhary, 2018: 836).

3DS altyapı platformu ise kartı veren kuruluş ve alıcı alanlarının uyum içinde çalışmasını sağlayan sistemleri, işlevleri ve mesajları kapsar. VISA ve MasterCard gibi uluslararası finansal kuruluşlar tarafından yönetilen bu bileşenler, dizin sunucusu, sertifika yetkilisi, kimlik doğrulama geçmişi sunucusu gibi unsurları içerir (Chowdhary, 2018: 836).



Şekil 4: 3-D Secure Protokolünün İşleyişi (Chowdhary, 2018: 836).

Bankalararası Kart Merkezi

Bankalararası Kart Merkezi (BKM), Türkiye'deki bankalar arası kart işlemlerini yöneten bir kuruluştur. BKM, bankalar arasında yetkilendirme işlemlerini yürütmek, kredi/banka kartı sektöründe bankalara uygulanacak prosedürleri geliştirmek, yurt içi şema kurallarını ve düzenlemelerini oluşturmak, standartlaştırılmasının sağlanmasıyla ilgili çalışmalar yapmak/kararlar almak, uluslararası kuruluşlar ve komisyonlarla ilişkiler kurup gerektiğinde bu kuruluşlardaki üyeleri temsil etmek ve devam eden banka operasyonlarını tek bir merkezi operasyon sitesinden daha güvenli, hızlı ve uygun maliyetli bir biçimde yürütmek gibi görevleri üstlenmektedir (Canko ve Bruggink, 2016: 232).

Takasbank ve Sermaye Piyasası Kanunu

Türk hukukunda ilk kez 6362 sayılı Sermaye Piyasası Kanunu (SerPK) ile hukukî bir düzenlemeye tabi tutulan merkezi karşı taraflar, sermaye piyasası araçlarının teslimi, bedellerinin ödenmesi ve teminat yükümlülüklerinin ifası gibi işlemleri yürütmekle görevlendirilmişlerdir (Köroğlu 2013: 2). Merkezi takas kuruluşlarının kurulmasına Sermaye Piyasası Kurulunun (SPK) teklifi üzerine ilgili Bakan tarafından izin verilmektedir. Bu kuruluşların faaliyete geçmesi SPK'nin iznine tabidir (SerPK, md. 77/1). "Merkezi takas kuruluşları, bu işlemler sırasında aracılık faaliyetlerinin karşı tarafı hâline geldiklerinde, merkezi karşı taraf (MKT) olarak adlandırılmaktadır" (Köroğlu, 2013: 2).

1992 yılında Takas ve Saklama A.Ş. olarak kurulan Takasbank, 1996 yılında bankacılık lisansını alarak İstanbul Menkul Kıymetler Borsası (İMKB) Takas ve Saklama Bankası A.Ş. adını aldı. Bu tarihten itibaren Takasbank, Borsa İstanbul bünyesindeki piyasalarda gerçekleştirilen pay, borçlanma araçları, türev araçlar ve kıymetli madenler gibi çeşitli

finansal enstrümanların takasını gerçekleştirmek üzere yetkilendirilmiş merkezi takas kuruluşu olarak faaliyet göstermektedir. Kuruluşundan bu yana güvenli, hızlı ve düşük maliyetli hizmet anlayışını benimseyen Takasbank, para ve sermaye piyasaları arasında etkin bir köprü vazifesi görmektedir. Sermaye piyasası ve bankacılık mevzuatı çerçevesinde, Borsa İstanbul bünyesindeki piyasalar için tam ve tek yetkili takas kurumu olarak hizmet sunan Takasbank, 1996 yılında aldığı bankacılık lisansıyla birlikte ürün yelpazesini genişletmiş ve hem Borsa İstanbul bünyesinde hem de bankacılık sektöründe önemli bir rol üstlenmiştir (Selcen, 2019: 3; Peker ve Karaağaçlı, 2015: 352).

Takasbank'a merkezi takas kurumu ve merkezi karşı taraf yetkilerinin verilmesi 6362 sayılı SerPK ile gerçekleşmiştir. Takasbank, MKT olarak finansal piyasalarda satıcıya karşı alıcı, alıcıya karşıysa satıcı olmakta ve üyelerinin piyasalarda yaptığı işlemlerden kaynaklanan risklere karşılık topladığı teminatların yanı sıra MKT olarak kendisinin de potansiyel üye iflaslarına karşı özgülediği kaynaklarla risk yönetimini gerçekleştirmektedir (Yay ve Kara, 2018: 44). MKT hizmeti bağlamında Takasbank, hem risklerin hem de maliyetlerin düşürülmesini sağlamaya çalışmaktadır (Eren, 2019: 172).

Türkiye'nin Ödeme Yöntemi: TROY

Adını "Türkiye'nin Ödeme Yöntemi" kelimelerinin baş harflerinden alan TROY (Gökmen, 2021: 75), 2014 yılında yerli bir ödeme yöntemi şeması yapılmasına karar verildikten sonra 2015 yılının Ekim ayında ortaya çıkmış (Salğit, 2020: 36) ve Türkiye'nin ilk ve yerel ödeme yöntemi olarak adlandırılmıştır (Gökmen, 2021: 77). Sağ alt köşesinde kendine özgü logosu olan TROY logolu kartlarda VISA ve MasterCard logolu kartlarla yapılan işlemlerin tamamı yapılabilmektedir (Akçakaya, 2019, akt. Gökmen, 2021: 76). TROY'un sunduğu hizmetler arasında banka kartı (Gökmen, 2021: 79), kredi kartı, ön ödemeli kartlar (Gökmen, 2021: 80), temassız ödeme, güvenli ödeme (Gökmen, 2021: 81) ve karekod ile ödeme (Gökmen, 2021: 82) vardır.

Karekod ile ödeme işlemi, öncelikle karekodun sisteme okutulmasıyla başlar ve ardından ödenecek tutar sisteme girilir ve doğruluğu onaylandıktan sonra ekrana gelen şifre alanına şifre yazılarak işlem tamamlanır. Bu işlemlerin güvenli bir şekilde gerçekleştirilmesi büyük önem taşıdığından gerekli altyapının oluşturulması ve çeşitli güvenlik katmanlarının sağlanması gerekmektedir (Salğit, 2020: 37).

Temassız ödeme işlemleri ise kartın üzerindeki çipe bağlı POS (Point of Sale) cihazı, anten ya da ödeme kayıt cihazında bulunan okuyucunun radyo frekansı dalgaları aracılığıyla haberleşmesi sayesinde gerçekleştirilir (Salğit, 2020: 38).

POS cihazı, işletmelerin satış işlemlerini kolaylaştırmak ve stok yönetimini optimize etmek amacıyla tasarlanmış hem donanım hem de yazılım bileşenlerini içeren kapsamlı bir sistemdir. Genellikle bir bilgisayar veya terminal ile barkod tarayıcıları, kasa kaydedicileri ve kart okuyucular gibi çeşitli çevre birimlerini içeren POS sistemleri, satış kaydı tutma, stok takibi

yapma, müşteri alışverişlerini izleme ve nakit, kredi/banka kartları ve mobil ödemeler gibi çeşitli ödeme yöntemlerini işleme gibi çeşitli iş operasyonlarında önemli bir rol üstlenmenin yanı sıra makbuz veya fatura oluşturmak, işletmelerin operasyonel yönetimi için verimlilik, doğruluk, satış ve stok verileri sağlamak gibi görevleri de üstlenmektedir (Asrani vd., 2024: 358).

TROY'un Doğrulama Sistemi: GO - Güvenli Öde

TROY logolu kartlarla e-ortam üzerinden yapılan alışverişlerde doğrulama sağlamak ve yurt içi e-ticaret işlemlerinde güvenliği artırmak amacıyla BKM tarafından geliştirilen bir kart hamili doğrulama sistemi olan Güvenli Öde (GO), 3DS'nin çalışma prensibine benzerlik göstermekle beraber (BKM, 2024a; Gökmen, 2021: 81) kart şemalarına ait kartlarla yapılan çevrim içi alışverişlerde de ek bir güvenlik katmanı sağlamaktadır. Kart kullanıcıları için e-ticaret sitelerinde ödeme esnasında "satın al" butonuna basıldıktan sonra GO tarafından cep telefonlarına gelen SMS kodunu girerek işlemler güvence altına alınmaktadır. İş yerleri ise GO altyapısı sayesinde e-ticaret sitelerindeki ödemeleri "güvenli işlem" olarak kabul ederek dolandırıcılık riskini minimize etmektedir (BKM, 2024b). Aynı zamanda GO, "3DS sistemini destekleyen tüm üye işyerlerinde de kullanılabilmektedir" (Gökmen, 2021: 81).

TROY ve Güvenlik

TROY kartları, çok katmanlı yazılım korumaları ve gelişmiş çip teknolojisiyle donatılmıştır. Her işlem sırasında özel olarak üretilen dinamik güvenlik kodları sayesinde kart güvenliği üst düzeyde tutulmaktadır. Dünya çapında kabul gören EMVCo (Europay, MasterCard, VISA) standartlarına uygun olarak üretilen bu kartlar, hem küresel ölçekte tüm uyumlu terminallerde kullanılabilmekte hem de bu standartların sağladığı güvenlik önlemleri sayesinde kopyalanma ve sahtecilik girişimlerine karşı tam koruma sağlamaktadır. Uygulanan bu çok yönlü güvenlik teknolojileri sayesinde TROY kartların kopyalanması imkânsız hâle getirilmiştir (Gökmen, 2021: 83).

Türkiye'de Doğrulama Sistemi Kurmak: Yasal Süreç

28 Haziran 2014 tarihli ve 29044 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemlerinin Faaliyetleri Hakkında Yönetmeliğin 5'inci maddesinin birinci fıkrası uyarınca bir yapının sistem olarak değerlendirilebilmesi için en az üç katılımcısının bulunması ve katılımcılar arasında gerçekleşen işlemlerin takas ve mutabakat süreçlerinden en az birini gerçekleştirmesi gerekmektedir (Resmî Gazete, 2024: 3). Aynı yönetmeliğin 9'uncu maddesinin birinci fıkrası uyarınca sistem işleticisi olarak faaliyette bulunmak isteyen kuruluşun sistem kurup işletebilmesi için Türkiye Cumhuriyet Merkez Bankası'ndan (TCMB) faaliyet izni alması gerekmekte (Resmî Gazete, 2024: 5) ve faaliyet izni almak için 27 Haziran 2013 tarihli ve 6493 kanun nolu Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunun 5'inci maddesinin ikinci fıkrasının sırasıyla (a), (b), (c), (ç) ve (d) bentleri uyarınca; anonim şirket şirket hâlinde kurulması, asgari beş milyon Türk lirası sermaye şartını sağlaması, sistemi işletebilmek için yeterli sayıda nitelikli personele ve teknik donanıma sahip olması, yeterli risk yönetimine ve bilgilerin güvenliğine

yönelik tedbirler alması, sistemin kaplamının bu Kanuna ve Kanun uyarınca çıkarılacak düzenlemeleri uyması gibi niteliklere haiz olması gerekmektedir (Resmî Gazete, 2013: 3). 29044 sayılı Yönetmeliğin 9'uncu maddesinin üçüncü fıkrasının (a), (b), (n) ve (ö) bentleri uyarınca başvuru içeriğinde fizibilite raporu ve üç yıllık bütçe planı, iç kontrol ve risk yönetimi çerçevesi, organizasyon yapısı ve görev dağılımı, sistem kuralları ve katılım koşulları ile teknik altyapı ve bilgi güvenliği dokümanları gibi birçok döküman yer almalıdır (Resmî Gazete, 2024: 5).

1 Aralık 2021 tarihli ve 31676 sayılı Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmeliğin 11'inci maddesinin birinci fıkrası uyarınca faaliyet izni başvurusu yapacak olan şirketin unvanında "ödeme kuruluşu" veya "elektronik para kuruluşu" ibaresi yer alması zorunludur (Resmî Gazete, 2021a: 13).

29044 sayılı Yönetmeliğin 29'uncu maddesinin ikinci fıkrası uyarınca TCMB, gerekli gördüğü diğer incelemeleri yaptıktan sonra faaliyet izni verip vermeme hususunda karar verir ve faaliyet izni vermesi durumunda bu kararı Resmî Gazete'de yayımlar (Resmî Gazete, 2024: 19).

29044 sayılı Yönetmeliğin 10'uncu maddesinin ikinci fıkrası uyarınca faaliyet izni alındıktan sonra sistem işleticisinin yönetiminden sorumlu olan kişilerin atanması ve aynı fıkranın (a) ve (b) bentleri uyarınca bu kişilerin 19 Ekim 2005 tarihli ve 25983 sayılı Bankacılık Kanununun 8'inci maddesinin (a), (b), (c) ve (d) bentlerinde yer alan niteliklere haiz olması; 29044 sayılı Yönetmeliğin aynı madde ve aynı fıkrasının (c) bendi uyarınca yüksek öğrenim görmesi; maliye, iktisat, bankacılılık, bilişim veya ödeme ve menkul kıymet mutabakat sistemleri alanlarında bilgi ve tecrübeye sahip olması gerekmektedir (Resmî Gazete, 2024: 9).

Kişisel Verilerin Korunumu Kanunu (KVKK)

Kişisel verilen işlenebilmesi için hukuka ve dürüstlük kurallarına uygun olma; doğru ve gerektiğinde güncel olma; belirli, açık ve meşru amaçlar için işlenme; işlendiklere amaçla bağlantılı ve sınırlı olma; ilgili mevzuatta öngörülen veya işlemdikleri amaç için gerekli olan süre kadar muhafaza edilme şartları vardır (Kişisel Verilerin Korunumu Kanunu [KVKK], md. 4/2). Kişisel veriler açık rıza olmadan ancak alınmasının ve paylaşılmasının koşulları kanunlarda açıkça öngörülmesi; hayat veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifası için gerekli olması, veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için zorunlu olması gibi sebeplerle işlenebilir (KVKK, md. 5/2) ve aktarılabilir (KVKK, md.8/2-a). Bunların dışındaki kişisel veriler açık rıza olmadan işlenemez (KVKK, md.5/1).

Kişiler; verilerin hangi amaçla, nasıl ve ne kadar süreyle işleneceği, veri sorumlusunun kim olduğu ve kişisel verileri toplamanın hukukî sebebi hususunda bilgilendirilmelidir (KVKK, md.10/1). Veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesiyle erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamakla ve bu amaç bağlamında uygun güvenlik düzeyini temin etmeye yönelik her türlü teknik ve idari tedbirleri almak zorundadır (KVKK, md.12/1). Veri sorumlusu, kişisel verilerin üçüncü kişiler tarafından işlenmesi durumunda

gerekli güvenlik tedbirlerinin alınmasından bu kişilerle birlikte ortak sorumluluk taşır (KVKK, md.12/2) ve kendi kurumunda kanun hükümlerine uygunluğun sağlanması için gerekli denetimleri yapmak veya yaptırmak zorundadır (KVKK, md.12/3). Veri sorumluları ve veri işleyen kişiler, öğrendikleri kişisel verileri kanuna aykırı şekilde başkalarına açıklayamaz veya işleme amacı dışında kullanamaz ve bu yükümlülük görevden ayrıldıktan sonra da devam eder (KVKK, md.12/4). Kişisel veriler yasa dışı yollardan elde edilirse veri sorumlusu bunu en kısa sürede ilgili kişilere ve Kurula bildirir; Kurul gerekirse bu durumu kamuya duyurabilir (KVKK, md.12/5).

Bu maddelerde ön görülen yükümlülüklerin yerine getirilmemesi durumunda on beş bin Türk lirasından bir milyon Türk lirasına kadar idari para cezası verilir (KVKK, md.18/1-b) ve bu ceza veri sorumlusuna uygulanır (KVKK, md.18/2).

Türkiye'de Doğrulama Sistemi Kurmak: Bilişimsel Gereklilikler

29044 sayılı Yönetmeliğin 4'üncü maddesinin (m) ve (n) fıkralarında geçen tanıma göre sistem işleticisi, ödeme ve menkul kıymet mutabakat sistemlerinin günlük işleyişinden sorumlu olan (Resmî Gazete, 2024: 2) ve aynı yönetmeliğin 11'inci maddesinin birinci fıkrası gereğince bu sistemlerin kesintisiz, güvenli, etkin ve verimli bir biçimde çalışmasını sağlamakla yükümlü olan tüzel kişidir. Aynı fıkranın (a), (b), (ç) ve (ğ) bentleri gereğince sistem işleticisi, gerekli bilgi sistemlerini ve teknolojik altyapıyı sağlayıp kurmak ve bu bağlamda önlemler almak; gerekli bilgi, belge ve muhasebe kayıt sistemleri ile düzenli iş akıcı ve haberleşmeyi sağlayacak altyapıya sahip olmak; yeterli ve nitelikli personel ve öz kaynağa sahip olmak, sistem katılımcılarının şikâyet ve önerilerini dile getirebilecekleri uygun platformlar oluşturmaktan gibi süreçlerden sorumludur (Resmî Gazete, 2024: 10).

Kimlik Doğrulama Sistemi

1 Aralık 2021 tarihli ve 31676 sayılı Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğin 10'uncu maddesinin birinci fıkrası uyarınca, elektronik para işlemlerini gerçekleştirecek olan kuruluşun işlemlerde gerçekleştirilmek üzere etkin ve yeterli bir kimlik doğrulama sistemi kurması gerekmektedir (Resmî Gazete, 2021b: 12). İlgili maddenin dördüncü, beşinci ve altıncı fıkrası uyarınca günün teknolojisine uymak koşuluyla uygun ve güvenli bir parola politikası belirlenmeli ve belirlenen tek kullanımlık parolaların ihtiyaç duyulan güvenlik seviyesini sağlayacak koşullarda olması (parolanın uzun olması, tespit, tahmin ve taklit edilebilmesine ilişkin risklerin minimize edilmesi vb.) ve bunlar için gerekli altyapının sağlanması gerekmektedir (Resmî Gazete, 2021b: 13).

Aynı maddenin yedinci fıkrasının (a), (b), (c), (ç) ve (d) bentleri uyarınca kimlik doğrulama sürecinde kullanıcı başarıyla sisteme giriş yaptığında önceki başarısız giriş denemeleri hakkında bilgi verilmeli; başarısız denemelerde ise kullanıcı adı veya parola hatasının detayı açıklanmamalı ve belirli sayıda başarısız deneme sonrasında ilgili kullanıcının erişimi bloke edilmelidir. Uzun süre işlem yapılmayan veya düzgün çıkış yapılmadan arka planda kalan oturumlar otomatik olarak sonlandırılmalı; özel yetkilendirme durumları haricinde, aynı

müşteri için eş zamanlı birden fazla oturum açılmasına izin verilmemeli ve bu durumda müşteri uyarılmalıdır (Resmî Gazete, 2021b: 13).

Ödeme Geçidi (Payment Gateway)

Ödeme geçidi; müşteri, satıcı ve bankalar arasında World Wide Web (WWW) üzerinden ödeme işlemlerini gerçekleştirmek için araçlar sağlayan bir e-ticaret uygulama hizmeti sağlayıcısıdır. Ödeme geçidi, bir web sitesinin güvenliğini sağlamaya, işlemlerini yetkilendirmeye ve finansal sahtekârlıklara karşı korumaya yardımcı olur; kredi/banka kartı gibi hassas bilgileri şifreleyerek ödeme bilgilerini korur ve bilginin müşteri ile ödeme işlemcisi arasında güvenli bir şekilde iletilmesini sağlar (Oo, 2019: 1330).

Ödeme geçidinin tasarlanması:

RSA (Rivest-Shamir-Adleman), ödeme ağ geçitlerinde yaygın olarak kullanılan bir açık anahtarlı şifreleme tekniğidir (Diko ve Ibraimi, 2023: 152). RSA, büyük tam sayıları çarpanlara ayırmanın zorluğuna dayanır ve bu da RSA şifrelemesini kırmayı son derece zorlaştırır (Diko ve Ibraimi, 2023: 153).

Ödeme geçidinin tasarlanmasında öncelikle şifreleme ve şifre çözme işlemleri gerçekleştirilir, ardından ödeme geçidinde RSA algoritması devreye girer. Her çevrim içi satıcı ve banka için ödeme geçidi, özel ve açık anahtar çiftleri oluşturur. Bu anahtarlar dağıtım amacıyla ödeme geçidinin anahtar veritabanına kaydedilir. Ödeme geçidi, müşteri kartı bilgilerini şifreli bir şekilde aldıktan sonra, satıcının özel anahtarıyla bu bilgileri çözer ve kart bilgisini doğrulamak için kart veritabanıyla karşılaştırma yapar. Eğer kart geçerliyse kart bilgileri bankanın açık anahtarı ile yeniden şifrelenir ve bu şifreli bilgiler kartı veren bankaya iletilir. Banka, müşterinin hesabını kontrol edip onayladıktan sonra ödeme geçidi müşteriye işlem sonucunun onaylandığını ya da reddedildiğini bildirir (Oo, 2019: 1331). Sanal POS üzerinden gerçekleşen bu aşamalarda devreye 3-D Secure sistemi de girebilir. 3-D Secure, işlemin gerçek kart sahibi tarafından yapılıp yapılmadığını onaylayabilir (Ödero, 2024a). Bu onay esnasında zorlu veya sürtünmesiz kimlik doğrulaması devreye girerek işlem tamamlanır (Ali vd., 2020: 2).

Şifreleme mekanizmalarında EMVCo gibi onaylı ve doğruluğu kanıtlanmış algoritmalar kullanılmalıdır (Gelir İdaresi Başkanlığı -GİB-) (GİB, 2019: 23). Ayrıca ödeme işlemlerini güvenli bir şekilde gerçekleştirmek için tasarlanan sertifikalı fiziksel donanımlar kullanıldığında regülasyon otoriteleri tarafından PCI ve EMV sertifikalarının alınması zorunlu kılınmıştır (GİB, 2019: 12). İlgili fiziksel donanımlar üzerinden işlem yapacak olan kuruluşların da PCI VE EMV sertifikalarını alması şart koşulmuştur (GİB, 2019: 13).

EMVCo: Europay, Mastercard ve VISA

EMVCo; Europay, MasterCard ve VISA tarafından çip teknolojisini kullanan ödeme kartları için küresel birlikte çalışabilirliği sağlamak amacıyla 1990'larda ortaklaşa geliştirilen bir standarttır. EMV ile birlikte analogdan dijitale geçiş söz konusudur. Bu geçiş beraberinde her işlem benzersiz, daha güvenli ve dijital olarak imzalanmış hâle gelmektedir (Manahan, 2013: 181). EMV, işlemlerini kartların fiziksel olarak POS terminaline veya ATM'ye takılmasıyla

kablolu bir bağlantı üzerinden gerçekleştir. Temassız ödeme versiyonuysa işlemleri daha pratik hâle getirmiş (Freitas vd., 2018: 1); kartın yalnızca okuyucuya yaklaştırılmasıyla ödeme hızlı bir şekilde tamamlanabilir hâle gelmiştir. Ayrıca EMV teknolojisi mobil ödemelerde de kullanılabilmektedir. "Mobil EMV" olarak bilinen bu yöntemle kullanıcılar EMV'yi akıllı telefonlarına yüklediklerinde telefonlarını ödeme noktalarına dokundurarak kolayca ödeme yapabilmektedir. EMV; temaslı, temassız ve mobil ödeme olarak üç farklı biçimde kullanılabilmektedir (Ahmad vd., 2016: 240).

Kart Yönetimi: PCI DSS Uyumluluğu

10 Mart 2007 Tarihli ve 26458 sayılı Banka Kartları ve Kredi Kartları Hakkında Yönetmeliğin 27/A maddesinin yedinci fıkrası uyarınca kart hamili tarafından başlatılan ve internet kullanılarak gerçekleştirilen işlemlerde veri işleme, kaydetme veya iletişiminde asgari seviyede Ödeme Kartı Endüstrisi Veri Güvenliği Standardının (Payment Card Industry –PCI-Data Security Standard –DSS-) hükümlerinin dikkate alınması gerekmektedir (Resmî Gazete, 2007: 9).

PCI DSS, kredi kartı bilgilerini işleyen, saklayan veya ileten tüm kuruluşlar için zorunlu bir dizi güvenlik standardıdır. PCI DSS, 7 Eylül 2006 tarihinde Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyi (Payment Card Industry Security Standarts Council) tarafından kurulmuştur. VISA, MasterCard, American Express, JCB ve Discover gibi büyük ödeme kartı markaları tarafından kurulmuş olan bu konsey günümüzde de hâlen devam etmektedir (Wilson vd., 2018: 74).

PCI DSS'nin kredi kartı verilerinin güvenliğini sağlamak için altı temel hedef altında toplanan 12 ana gereksinimi vardır. Bu gereksinimler ilkin güvenli bir ağ altyapısı oluşturmayı ve sürdürmeyi hedefler ve bunun için güvenlik duvarı yapılandırması ve güvenli sistem şifreleri kullanılması gerekir. Kart sahibi verilerinin korunması için verilerin hem depolanması hem de iletimi sırasında şifreleme yapılmalıdır. Güvenlik açıklarına karşı koruma sağlamak için güncel anti-virüs yazılımları kullanılmalı ve sistemler düzenli olarak güncellenmelidir. Erişim kontrolü için verilere sadece yetkili kişilerin erişebilmesi sağlanmalı ve her kullanıcıya benzersiz kimlikler atanmalıdır. Sistemin güvenliği sürekli izlenmeli, düzenli testler yapılmalı ve tüm erişimler kayıt altına alınmalıdır. Son olarak, tüm bu gereksinimleri kapsayan ve tüm personeller için geçerli olan kapsamlı bir bilgi güvenliği politikası oluşturulmalı ve sürdürülmelidir. Bu 12 ana gereksinim altında toplam 200'den fazla alt madde bulunmaktadır (Wilson vd., 2018: 75). İlgili bilişimsel gereksinimler sağlandıktan sonra bu ana gereksinimler ve alt maddeleri detaylı bir şekilde Konsey tarafından incelenir ve sonuca göre PCI DSS sertifikası verilir (Ödero, 2024b).

Sonuç

Sonuç olarak, Türkiye'de bir doğrulama sistemi kurmak hem yasal hem de bilişimsel açıdan oldukça katmanlı bir süreçtir. Bu çalışma Türkiye'deki ödeme sistemlerinin yasal altyapısını, teknik gerekliliklerini ve uluslararası standartlarla uyum sağlanmasının kritik noktalarını ele almıştır. Özellikle 6493 sayılı Kanun, ilgili yönetmelikler ve tebliğin doğrulama sistemi kurulumundaki rolü incelenmiş ve bu yasal çerçevelerin PCI DSS ve EMVCo gibi

uluslararası güvenlik standartlarıyla uyumlu hâle getirilmesinin önemine dikkat çekilmiştir. Çalışma, Türkiye'de bir doğrulama sistemi kurmanın yalnızca yasal gereklilikleri yerine getirmekle kalmayıp aynı zamanda küresel standartlara uygun bir altyapı geliştirilmesinin de gerektiğini ortaya koymuştur. Kimlik ve kart doğrulama süreçleri, ödeme sistemlerinin güvenliği ve kullanıcı güveni açısından kritik öneme sahiptir. Bu bağlamda Türkiye'deki kişisel verilerin korunmasına yönelik KVKK düzenlemeleri ile uyumlu bir doğrulama altyapısının oluşturulması gerektiği vurgulanmış; veri güvenliği, ödeme sistemlerinin önemli bileşenlerinden biri olarak ele alınmış ve kullanıcı verilerinin korunmasına yönelik alınması gereken asgari tedbirler anlatılmıştır. Ayrıca teknolojik gelişmelere uygun güvenlik mekanizmalarının uygulanması ve kimlik doğrulama süreçlerinde kullanıcı adı, parola ve oturum yönetimi gibi unsurların güncel güvenlik standartlarıyla uyumlu olması gerektiği belirtilmiştir.

Bilişimsel altyapı gereklilikleri bağlamında şifreleme ve veri iletimi sırasında PCI DSS ve EMVCo gibi uluslararası standartların uygulanması gerektiği; doğrulama bağlamında 3-D Secure veya asgari düzeyde onunla aynı işlevi gören Güvenli Öde (GO) gibi sistemlerin kullanılması gerektiği ortaya konmuştur. Bu standartlar ödeme işlemleri ve kullanıcı verilerinin korunması için gereken güvenliği sağlamaktadır. Çalışma Türkiye'de bir kart doğrulama sistemi kurulurken hem yasal hem de bilişimsel açıdan atılması gereken adımlara yönelik bir yol haritası sunmaktadır.

Kaynakça

Ackerberg, D. A. ve Gowrisankaran, G. (2003). Quantifying equilibrium network externalities in the ACH banking industry. *NET Institute Working Paper*, 3(6), 1-39.

Ahmad, Z., Zeki, A.M. ve Olowolayemo, A. (2016). Security failures in EMV smart card payment systems. *6th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, 240-243.

Alavian, S., Ding, J., Whitehead, P. ve Laudicina, L. (2010). Credit Valuation Adjustment (CVA*). SSRN Electronic Journal,* 1-22.

Ali, M. A., Groß, T. Ve Moorsel, A. v. (2020). Investigation of 3-D Secure's model for fraud detection. *Proceedings of the 8th Workshop on Socio-Technical Aspects in Security and Trust.* 1-17.

Alt, R. ve Huch, S. (2022). *Fintech Dictionary: Terminology for the Digitalized Financial World.* Springer Gabler.

Amrita, A. S. ve Shukla, A. (2022). 3D-security in digital India. *EPRA International Journal of Research and Development (IJRD),* 7(6), 392-394.

Asrani, H., Vishwakarma, S., Asrani, D. ve Asrani, K. (2024). Point of sale systems. *International Journal of Innovative Research in Computer Science and Technology (IJIRCST),* 12(1), 358-363.

Baker, C. M. (2016). Clearinghouses for over-the-counter derivatives. *SSRN Electronic Journal,* 3-75.

Bella, G., Massacci, F. ve Paulson, L. C. (2005). An overview of the verification of SET. *International Journal of Information Security*, *4*(1/2), 17–28.

Berndsen, R. (2021). Fundamental questions on central counterparties: A review of the literature. *Journal of Futures Markets*, 41(12), 2009-2022.

BKM (Bankalararası Kart Merkezi). (2024a). https://bkm.com.tr/faydali-bilgiler/guvenli-internet-alisverisi (Erişim Tarihi: 22 Kasım 2024)

BKM (Bankalararası Kart Merkezi). (2024b). https://bkm.com.tr/urunler-ve-hizmetler/odeme-cozumleri (Erişim Tarihi: 22 Kasım 2024)

Bradford, T. (2007). The evolution of the ACH. *Payments System Research Briefing.* Federal Reserve Bank of Kansas City, 1-4.

Canko, S. ve Bruggink, D. (2016). The Turkish payment market and its specifics: An interview with Soner Canko. *Journal of Payments Strategy & Systems*, 10(3), 230-238.

Chang, F. B. (2014). The Systemic Risk Paradox: Banks and Clearinghouses Under Regulation. *Columbia Business Law Review*, *2014*(3), 747–816.

Chang, H. H. (2004). Payment card industry primer. *Payment Card Economics Review, 2*(1), 29–46.

Chowdhary, A. (2018). Online Business Security: SSL, TLS, SET and 3D-Secure. *Journal of emerging technologies and innovative research*, 5(4), 833-837.

Committee on Payment and Settlement Systems (CPSS). (2012). Payment, clearing and settlement systems in the CPSS countries: Volume 2. *Bank for International Settlements (BIS),* 1-544.

Corella, F. ve Lewison, K. P. (2019). Frictionless Web Payments with Cryptographic Cardholder Authentication. *HCI International 2019 – Late Breaking Papers*, 468-483.

Diko, E. ve Ibraimi, M. (2023). RSA & extended euclidean algorithm with examples of exponential RSA ciphers, RSA example solution with extended euclidean algorithm. *Vision International Refereed Scientific Journal*, 8(1), 161-175.

Duffie, D. (2012). *Dark markets: Asset pricing and information transmission in over-the-counter markets (Vol. 6).* Princeton University Press.

Eren, E. (2019). Merkezi karşı taraf uygulaması ve merkezi karşı taraf üyelik sözleşmesinin hukuki niteliği. *Ticaret Ve Fikri Mülkiyet Hukuku Dergisi*, 5(2), 170-191.

Evans, D. S. (2004). More than money: The development of a competitive electronic payments industry in the United States. *Payment Card Economics Review, 2*(1), 1–27.

Fatonah, S., Yulandari, A. ve Wibowo, F. W. (2018). A review of e-payment system in e-commerce. *Journal of Physics: Conference Series, 1140*(1), 1-7.

Fiedor, P. (2018). Clearinghouse-five: Determinants of voluntary clearing in European derivatives markets. *ESRB Working Paper Series*, 72(1), 1-107. European Systemic Risk Board.

Freitas, L., Modesti, P., ve Emms, M. (2018). A methodology for protocol verification applied to EMV® 1. *Formal Methods: Foundations and Applications*, 180–197.

Friesz, M. ve Váradi, K. (2021). How is it done? Comparison between the margin calculation methodology of central counterparties and clearinghouses. *Public Finance Quarterly*, 66(3), 397-412. Corvinus University of Budapest.

Gelir İdaresi Başkanlığı (GİB). (2019*). Güvenli mobil ödeme ve elektronik belge yönetim sistemi* : *Başvuru, izin, onay ve denetim süreçleri kılavuzu. 2-34.*

Gökmen, M. (2021). *Türkiye'de dijital ödeme yöntemlerinin gelişimi: Milli örneğimiz Troy* (Tez No. 678261) [Yüksek lisans tezi, İstanbul Arel Üniversitesi, Lisansüstü Eğitim Enstitüsü). YÖK Tez Merkezi.

Gregory, J. (2010). Are we building the foundations for the next crisis already? The case of central clearing. 1-12.

Gündoğdu, A. (2023). *Herkese Göre Finans.* İstanbul: Remzi Kitabevi.

Herbst-Murphy, S. (2013). Clearing and settlement of interbank card transactions: A MasterCard tutorial for Federal Reserve payments analysts. *Consumer Finance Institute Discussion Papers*, 13(1), 1-19. Federal Reserve Bank of Philadelphia.

Investopedia. (2022). https://www.investopedia.com/terms/b/base-i.asp#:~:text=Base%20I%20was%20first%20developed,part%20of%20the%20VisaNet%20system (Erişim Tarihi: 23 Ekim, 2024).

Kamtchueng, C. (2011). CVA, DVA, LVA, FVA, CSA and What Else? *SSRN Electronic Journal. 1-23.*

Kişisel Verilerin Korunumu Kanunu (KVKK). (2016). *Resmî Gazete* (Kanun No: 6698) (Sayı: 29677). 1-21.

Köroğlu, B. (2013). *Türev araçların alım satımına aracılık sözleşmeleri* (Tez No. 348038) [Yüksek lisans tezi, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü). YÖK Tez Merkezi.

Manahan, O. (2013). EMV: Building the foundation for the future of payments. *Journal of Payments Strategy & Systems*, 7(2), 180–185.

Mastercard. (2024). https://eu-gateway.mastercard.com/api/documentation/integrationGuidelines/supportedFeatures/pickPaymentMethod/achPayments.html?locale=en_US (Erişim Tarihi: 30 Ekim 2024).

McAndrews, J. J. (1994). The automated clearinghouse system: Moving toward electronic payment. *Business Review*, *Federal Reserve Bank of Philadelphia*, 15-23.

Merkow, M. S. (2004). Secure electronic transactions (SET). H. Bidgoli (Ed.), *The Internet encyclopedia* (Vol. 3, pp. 247-260). John Wiley & Sons, Inc.

Murdoch, S. J. ve Anderson, R. (2010). Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication. In R. Sion (Ed.), *Financial cryptography and data security.* FC 2010. Lecture notes in computer science, 6052(1), 336-342.

OCC (Office of the Comptroller of the Currency). (2024). https://occ.gov/topics/supervision-and-examination/capital-markets/financial-markets/derivatives/index-derivatives.html (Erişim Tarihi: 11 Ekim 2024).

Oo, K. Z. (2019). Design and Implementation of Electronic Payment Gateway for Secure Online Payment System. *International Journal of Trend in Scientific Research and Development (IJTSR)*, 3(5), 1220-1225.

Ödero. (2024a). Ödeme Ağ Geçidi Nedir, Nasıl Çalışır? https://oderopay.com.tr/blog/finans-rehberi/odeme-ag-gecidi-nedir-nasil-calisir (Erişim Tarihi: 30 Kasım 2024).

Ödero. (2024b). PCI DSS Nedir, Neden Önemlidir? https://oderopay.com.tr/blog/finans-rehberi/pci-dss-nedir-neden-onemlidir (Erişim Tarihi: 29 Kasım 2024).

Peker, İ. ve Karaağaçlı, B. (2015). Dünyada ve Türkiye'de sermaye piyasası altyapı kurumları. *Finansal Araştırmalar ve Çalışmalar Dergisi*, 7(13), 341-375.

Rehlon, A. ve Nixon, D. (2013). Central counterparties: What are they, why do they matter and how does the Bank supervise them*? Bank of England Quarterly Bulletin*, 53(2), 147-156.

Resmî Gazete. (2007). Banka Kartları ve Kredi Kartları Hakkında Yönetmelik. Sayı: 26458, 1-17.

Resmî Gazete. (2013). Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun. Kanun No. 6493, Sayı: 28690, 1-19.

Resmî Gazete. (2021a). Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik. Sayı: 31676, 1-73.

Resmî Gazete. (2021b). Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ. Sayı: 31676, 1-43.

Resmî Gazete. (2024). Ödeme ve Menkul Kıymet Mutabakat Sistemlerinin Faaliyetleri Hakkında Yönetmelik. Sayı: 29044, 1-31.

Risk. (2024). https://www.risk.net/definition/wrong-way-risk-wwr (Erişim Tarihi: 14 Ekim 2024).

Rusk, S. (2024). *Bir Solukta Ekonomi* (Çeviri: Samet Öksüz). İstanbul: Say Yayınları.

Russo, D., Hart, T. L. ve Schönenberger, A. (2002). The evolution of clearing and central counterparty services for exchange-traded derivatives in the United States and Europe: A comparison. *ECB Occasional Paper*, 5(1), 3-62.

Sermaye Piyasası Kanunu (SerPK). (2012). *Resmî Gazete* (Kanun No: 6362) (Sayı: 28513).

Selcen, Ö. (2019). *Finans sistemindeki likidite riski yönetiminde Merkezi Takas Kurumu'nun işlevi ve önemi: Takasbank örneği* (Tez No. 572463) [Yüksek lisans tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü). YÖK Tez Merkezi.

Shoniregun, C. A. ve Zhao, S. (2007). SET: A questionable security protocol. In *International Conference on Web Information Systems and Technologies*, 2(1), 313-319.

Stearns, D. L. (2007). *"Think of it as Money": A History of the VISA Payment System, 1970–1984* (Doktora tezi, University of Edinburgh), 1-223.

Yadav, Y. (2012). The problematic case of clearinghouses in complex markets. *Georgetown Law Journal,* 101(1), 387-444.

Yay, G.G. ve Kara, B. (2018). Takasbank'ın risk yönetimindeki rolü: Karşılaştırmalı bir analiz. *Ekonomik Yaklaşım Dergisi,* 29(108), 43-68.

Wilson, D., Roman, E. ve Beierly, I. (2018). PCI DSS and card brands: Standards, compliance and enforcement. *Cyber Security: A Peer-Reviewed Journal*, 2(1), 73-82.