

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

ÖDEME SİSTEMLERİNDE BİLGİ TEKNOLOJİLERİ RİSKLERİ

Yüksek Lisans Tezi

Özlem Menekşe Rumelili

Ankara-2006

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

ÖDEME SİSTEMLERİNDE BİLGİ TEKNOLOJİLERİ RİSKLERİ

Yüksek Lisans Tezi

Özlem Menekşe Rumelili

Tez Danışmanı
Doç.Dr. Yalçın Karatepe

Ankara-2006

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

ÖDEME SİSTEMLERİNDE BİLGİ TEKNOLOJİLERİ RİSKLERİ

Yüksek Lisans Tezi

Tez Danışmanı :

Tez Jürisi Üyeleri

Adı ve Soyadı

İmzası

.....
.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
.....

Tez Sınavı Tarihi

İÇİNDEKİLER

1	ÖDEME SİSTEMLERİ KAVRAMLARI.....	4
1.1	Ödeme Sistemi Nedir?.....	4
1.2	Ödeme Sistemlerinin Önemi.....	6
1.3	Ödeme Sistemlerinin Amaçları.....	7
1.4	Rakamlarla Ödeme Sistemleri.....	8
1.5	Ödeme Sistemlerinin Sınıflandırılması	11
1.5.1	Tutara Göre.....	11
1.5.2	Mutabakat Türüne Göre	12
1.5.3	Sınırlarına göre	16
1.6	Ödeme sistemleri yapıları	16
2	ETKİN BİR ÖDEME SİSTEMİNİN ÖNEMİ.....	19
2.1	Etkinlik Nedir?	19
2.2	Etkin Ödeme Sistemi Nedir?.....	19
2.3	Paranın Dolaşım Hızı Ödeme Sistemleri İlişkisi :	21
2.4	Merkez Bankalarının Ödeme Sistemlerindeki Rolü :.....	25
2.4.1	Merkez Bankası Parası.....	26
2.4.2	Gözetim Fonksiyonu.....	27
2.4.2.1	Ödeme Sistemleri Gözetiminde Kilometre Taşları.....	27
2.5	Ödeme sistemleri ve finansal istikrar	29
2.6	Ödeme sistemleri ve para politikası	29
3	EFT ve EMKT SİSTEMLERİ.....	34
4	BAZI ÖDEME SİSTEMLERİNE GENEL BİR BAKIŞ :	44
4.1	RTGSplus – Almanya.....	44
4.2	Fedwire and CHIPS- Amerika	45
4.3	BOJ-Net - Japonya	46
4.4	SIC – İsviçre :	47
4.5	PNS - Fransa	48
4.6	SPI /SBLE – İspanya	49
4.7	POPS/Bof-RTGS – Finlandiya	50
4.8	CHAPS – İngiltere.....	52
4.9	SWIFT - Society for Worldwide Interbank Financial Telecommunication.....	55
4.10	TARGET.....	56
4.11	CLS Continuous Linked Settlement.....	61
5	ÖDEME SİSTEMLERİNDE RİSK.....	66
5.1	Risk grupları.....	66
5.1.1	Kredi Riski	66
5.1.2	Likidite Riski.....	67
5.1.3	Yasal Risk	67
5.1.4	Operasyonel Risk.....	68
5.1.5	Sistematik Risk.....	69
5.2	Risk Açısından RTGS ve DNS sistemler:	70
5.3	Temel İlkeler	71
5.3.1	Temel ilkelerin ana başlıkları:	72
5.3.2	Temel ilkeleri uygulamada merkez bankalarının görevi nedir?.....	76

6	Bilgi Teknolojileri Riskleri.....	78
6.1	Bilgi Teknolojileri Riskleri Nelerdir	81
6.1.1	Bilgi Güvenliđi	83
6.1.2	İnternet Bankacılıđı.....	85
6.1.3	Yeni Teknolojiler.....	88
6.1.4	Ađ Yapıları.....	90
6.1.5	Yazılım ve Donanım.....	93
6.1.6	Olađandışı Durumlar.....	99
6.1.7	Standartlar	100
6.1.8	Bilgi Teknolojileri Risklerini Dođarabilecek Diđer Durumlar	103
6.2	Temel İlke VII: İleri düzeyde güvenlik ve işlemler açısından güvenilirlik sağlamanması	105
6.3	Bilgi Teknolojileri Riskleri ve Seçilmiş Örnekler.....	111
6.3.1	RTGSPlus – Almanya.....	114
6.3.2	Fedwire – Amerika	114
6.3.3	SIC – İsviçre	118
6.3.4	PNS- Fransa.....	118
6.3.5	SBLE – İspanya	119
6.3.6	CHAPS-İngiltere	119
6.3.7	POS-Finlandiya / BOJ-Net Japonya	120
6.3.8	TARGET	120
7	ÖDEME SİSTEMLERİNİN GELECEĞİ	123
7.1	Ulusal Sistemlerden Uluslararası Sistemlere Geçiş	125
7.2	E-Mutabakat.....	127
7.2.1	E-Mutabakatın Kazandırdıkları	133
7.2.1.1	Genel Kazanımlar	133
7.2.1.2	Mevcut RTGS sistemlere göre kazanımları	134
8	SONUÇ VE ÖNERİLER	136
9	KAYNAKÇA.....	141

ŞEKİLLER

Şekil 1 - EFT sisteminde Milyon YTL bazında Toplam Ödeme Tutarı.....	10
Şekil 2 - V tipi ödeme sistemi	17
Şekil 3 - Y tipi ödeme sistemi	17
Şekil 4 - L tipi ödeme sistemi.....	18
Şekil 5 - T tipi ödeme sistemi.....	18
Şekil 6 - EFT – EMKT şeması	366
Şekil 7 – AB Ülkelerinde Tutar Bazında Ulusal ve Uluslararası Ödeme değerleri	122
Şekil 8 - Merkezileşmiş RTGS sistemi	132
Şekil 9 - E-mutabakat Sistemi	133

TABLolar

Tablo 1- AB Ülkelerinde Ödeme ve Gayrı safi milli hasıla oranları ,2003	9
Tablo 2 – AB Ülkeleri Ödeme Sistemlerinin ve Türkiye Ödeme Sistemi EFT Sisteminin Karşılaştırılması.....	54
Tablo 3 - TARGET üyesi ülkelerde ulusal ve uluslararası ödemeler (Tutar Bazında)	60
Tablo 4 – TARGET Üyesi Sistemlerin CPSIPS İlkeleri ile Uyumu	113
Tablo 5 – Fedwire Sistemi Yıllar Bazında Çalışırlık Oranları.....	116
Tablo 6 – Fedwire Sisteminde Kesintilerin Detayları	117

KISALTMALAR

Kısaltma	Açılım
AB	Avrupa Birliği
BIC	Bank Identifier Code
BIS	Bank for International Settlements
BoE	Bank of England
BT	Bilgi Teknolojileri
CNS	Continuos Net Settlement
CLS	Continuous Linked Settlement
CPSIPS	Core Principles for Systemically Important Payment Systems
DNS	Deferred Settlement ya da Netting
ECB	European Central Bank
EFT	Elektronik Fon Transferi
EMKT	Elektronik Menkul Kıymet Transferi
EMU	European Monetary Union
EVDS	Elektronik Veri Dağıtım Sistemi
FIFO	First In First Out
FX	Foreign eXchange
G-10	Belçika, Kanada, Fransa, Almanya, İtalya, Japonya, Hollanda, İsviçre, İsveç, İngiltere, Amerika Birleşik Devletleri
NewCHIPS	New Clearing House InterBank Payment System
OTA	Office of Technology Assessment
PKI	Public Key Infrastructure
PNS	Paris Net Mutabakat
RTGS	Real Time Gross Settlement
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SIC	Swiss Interbank Clearing System
TARGET	Trans_european Automated Real-time Gross settlement Express Transfer
TARGET 2	Trans_european Automated Real-time Gross settlement Express Transfer 2. Nesil
TCMB	Türkiye Cumhuriyet Merkez Bankası
TCP/IP	Transmission Control Protocols/Internet Protocols
TBB	Türkiye Bankalar Birliği
XML	Extensible Markup Language
XML	Extensible Markup Language

ÖZET

Ekonomik birimler arasında mal ve hizmetlerin deęişimini kolaylařtıran araçları, kurumsal ve örgütsel çatıyı, iřletim süreçlerini ve haberleřme aęını kapsayan ödeme sistemleri, finansal sistemin ve ekonominin etkin iřleyiři için önem arz etmektedirler. Küreselleřen dünyamızda finansal iřlemlerin sayısı ve hacmi hızla artmakta, yapılan iřlemler de küreselleřmektedir. Bu durum ödeme sistemlerinin daha yoğun ilgi görmesine ve merkez bankalarının önemli gündem maddelerinden biri haline gelmesine neden olmaktadır.

Ödeme sistemleri ekonominin can damarlarından biri haline gelirken, oluřabilecek risklerin yaratabileceęi etkilerin boyutları da büyümektedir. Kredi riski, likidite riski, operasyonel risk, yasal risk, sistemik risk bařlıkları altında incelenen risk gruplarının oluřmasını engellemek için merkez bankalarının bankası olarak bilinen Bank for International Settlement (BIS) bünyesinde çalışmalar yürütölmektedir. Bu kapsamda sistemik açıdan önemli ödeme sistemleri için temel ilkeler (Core Principles of Systemically Important Payment Systems:CPSIPS) Ocak 2001’de yayınlanmıřtır. Ülkeler sistemik açıdan önemli ödeme sistemlerinin bu raporda belirtilen prensiplere uygunluęunu inceleyip, aksayan yönlerini gidererek risk oluřumlarını en aza indirmeye çalışmaktadırlar.

Geliřen bilgi teknolojileri ödeme sistemlerinin gelişmesinde önemli altyapıyı hazırlarken ödeme sistemleri için riskler de oluřturmaktadır. Operasyonel risk bařlığı

altında, CPSIPS raporunda VII. ilkede irdelenen bilişim risklerinin, en aza indirilmesi yönünde ilgili otoritelerce çalışmalar sürdürülmektedir.

Çalışma ödeme sistemlerinin önemini vurgulamak, ödeme sistemlerinin barındırdığı bilgi teknolojileri risklerini belirlemek ve bu risklerin ortadan kaldırılmasına yönelik öneriler sunmak amacı ile hazırlanmıştır. Bu kapsamda çalışmada ödeme sistemlerinin tanımı yapılmış, etkinliği değerlendirilmiş, çeşitli ödeme sistemlerinin yapıları irdelenmiş, ödeme sistemlerinin barındırdıkları bilgi teknolojileri riskleri genel olarak ve tanıtılan ödeme sistemleri bünyesinde incelenmiş, risklerin ortadan kaldırılması için önerilerde bulunulmuştur.

Anahtar Kelimeler: Ödeme sistemleri, CPSIPS, Bilgi teknolojileri Riskleri, EFT, E-mutabakat

ABSTRACT

Payment systems containing tools that facilitates exchange of goods and services, institutional and organizational framework, telecommunication and communication network are important for efficient functioning of financial system and economy.

In our globalizing world, number and volume of financial transactions are enhancing and transactions are becoming global. As a result of this change, payment systems take more interest and place in central banks' agendas.

While payment systems are becoming vital points of the economy, the effects of possible risks are growing as well. For preventing risks studies are made in the Bank for International Settlement known as the bank of the central banks. Within this context, Core Principles of Systemically Important Payment Systems: CPSIPS is published at 2001.

After the CPSIPS report and the increased importance of the payment systems, central banks take an active role on the oversight. Payment systems are the main actors for the financial stability and monetary policies.

Developing information techonologies prepares an important infrastructure for development of the payment systems, at the same time they make the payment systems more vulnerable.

The aim of this stduy is to stress the importance of the payment systems, to determine the information technology risks arising from these systems and to propose solutions for to alleviating these risks. In this context payment systems are

described, efficiency of payment systems are evaluated, same payment system examples are given, information technology risks exposed in payment systems are analyzed within introduced payment system in general, recommendations have been made to alleviate the risks.

Key Words : Payment systems, CPSIPS, IT Risks, EFT, E-settlement.

Giriş

Ödeme sistemlerinin önemi, özellikle mali sektörde üstlendikleri rollerden kaynaklanmaktadır. Mali sistem içinde finansal risklere, güvenilirliğe ve hızlılığa yönelik reformlar sonrasında ödeme sistemlerinde de büyük değişimler görülmüş; bu ise para otoritelerini para politikasına yönelik karar verme süreçlerinde güçlü ve etkin ödeme sistemlerine sahip olma ve ödeme sistemi bağlantılı gelişebilecek sistemik risklerden kaçınılmasına katkıda bulunacak yönde çalışmalara yöneltmiştir. Mali sektörde ortaya çıkan, paranın daha çabuk, daha güvenli ve daha risksiz hareket edebilmesi düşüncesi çağımızın en etkili ve en hızlı gelişen teknolojisi durumunda bulunan elektronik ve bilgisayar teknolojisi ile birlikte gelişerek “elektronik ödeme” fikrini doğurmuş ve bununla birlikte elektronik ödeme sistemlerine hızlı bir geçiş süreci başlamıştır (Türkiye Cumhuriyet Merkez Bankası, 2006). Bu çalışmada ödeme sistemleri ifadesi ile elektronik ödeme sistemleri kastedilmiştir.

Bu çalışmanın amacı;

- Ödeme sistemlerinin gelişen finans dünyasında gün geçtikçe önem kazandığını, geliştiğini belirtmek,
- Paranın dolaşım hızı, para politikaları ve finansal istikrar ilişkilerini değerlendirmek,
- Merkez bankalarının gündeminde önemli yer tuttuğunu belirtmek,
- Ödeme sistemlerindeki gelişim ve finansal konulara etkileri nedeniyle oluşacak risklerin etkilerinin de büyüdüğünün altını çizmek,

- Bilhassa ödeme sistemleri ve bilgi teknolojileri risklerini irdelemek ve çözüm önerileri sunmak,
- Çeşitli ödeme sistemlerini irdelemek, bilgi teknolojileri kapsamında değerlendirmelerini yapmak
- Ödeme sistemlerinin geleceğinin bilgi teknolojileri riskleri açısından tartışmak olarak

özetlenebilir.

Çalışmanın birinci bölümünde ödeme sistemleri tanımı yapıp, amaçları, önemi ve nasıl sınıflandırıldığı açıklanmıştır. Ödeme sistemlerinin öneminin ve yaygın kullanımının gözler önüne serilmesi amacıyla çeşitli ödeme sistemlerinden rakamsal değerler derlenmiştir.

Çalışmanın ikinci bölümünde etkinlik ve etkin ödeme sistemi kavramları açıklanmış, etkin ödeme sistemlerinin önemi ve bu önem çerçevesinde merkez bankalarının ödeme sistemlerindeki rolü, ödeme sistemleri merkez bankaları ilişkileri irdelenmiştir.

Çalışmanın üçüncü bölümünde Türkiye ödeme sistemi Elektronik Fon Transferi (EFT) ve Elektronik Menkul Kıymet Transferi (EMKT) sistemleri incelenmiştir.

Çalışmanın dördüncü bölümü ise önemli ödeme sistemlerinin tanıtımını yapmaktadır.

Çalışmanın beşinci bölümünde ödeme sistemleri açısından risk kavramları irdelenmiştir.

Çalışmanın altıncı bölümünde bilgi teknolojileri risklerinin ne durumlarda oluşabileceği, neler yapılarak bu risklerin en aza indirgenebileceği tartışılmıştır.

Çalışmanın yedinci bölümünde ödeme sistemlerinin geleceği, bilgi teknolojileri riskleri barındırabilecek yönleri ile irdelenmiştir.

Çalışmanın sekizinci ve son bölümünde sonuç ve öneriler oluşturulmuştur.

BİRİNCİ BÖLÜM

1 ÖDEME SİSTEMLERİ KAVRAMLARI

1.1 Ödeme Sistemi Nedir?

Ödeme sistemleri kavramına ödeme, ödeme aracı ve ödeme sistemi arasındaki ayrımı yaparak bir giriş yapmak yararlı olacaktır :

Ödeme basitçe paranın transferi;

Ödeme aracı kullanıcılarına para transferi sağlayan banknot, çek ve benzeri herhangi bir araç;

Ödeme sistemi ise, pek çok şekilde tanımlanabilecek araç, enstrüman, kullanılan teknik altyapı üzerinde anlaşmayı içeren, sistem katılımcılarının aralarında fon transferini sağlayacak kurallar bütünüdür. Ödeme sistemleri teknik altyapı üzerindeki anlaşmayı içerir ve bu altyapıyı tanımlayan bir terim olarak da kullanılmaktadır (Pringle & Robinson, 2002: 4).

Türkiye Cumhuriyet Merkez Bankası internet sitesinde ödeme sistemlerinin tanımını şu şekilde yapmaktadır:

“Ödeme sistemleri, ekonomik birimler arasında mal ve hizmetlerin değişimini kolaylaştıran araçları, kurumsal ve örgütsel çatıyı, işletim süreçlerini ve haberleşme ağını kapsamaktadır. “

Bir başka tanıma göre ise ödeme sistemleri insanlar ya da örgütler arası değerler transferidir. Bir ödeme sistemi değerlerin katılımcılar arasında aktarımını sağlayacak organize edilmiş anlaşmalar bütünü olarak tanımlanabilir.

Bank of England (BoE), ödeme sistemleri bütün ekonomilerin işleyişi için temel niteliktedir, eğer işlemler piyasa ekonomilerinin can damarlarıysa, ödeme sistemleri bu işlemler için dolaşım sistemidir, ifadesini ödeme sistemleri için kullanmaktadır.

Gregor Henrich'in 2000 yılında ödeme sistemleri üzerine bir çalıştayda belirttiği üzere finansal sistemi üç bileşenden oluşan bir yapı olarak düşünebiliriz :

- Ticaret yapan kurumlar
- Ticaret yaptıkları piyasa
- Bu piyasaları destekleyen ödeme ve mutabakat mekanizmaları

Ödeme sistemleri ekonominin finansal altyapısının önemli bir parçasıdır. Piyasa ekonomilerinde hemen her işlem bir ödeme içermektedir. Küçük ödemeler nakit olarak yapılmaktayken büyük ödemeler için kredi transferi ya da çek tercih edilmektedir. Bu durum nakit olmayan yöntemlerde bankalararası fon transferini dolayısı ile bankalararası ödeme sistemlerini gündeme getirmektedir (Lindley , 2002:77).

Tanımlar çeşitli olmasına rağmen ifadeler ödeme sistemlerinin organize yapıları, finansal ve ekonomik sistem açısından önemli oldukları hususunda bütünleşmektedir.

1.2 Ödeme Sistemlerinin Önemi

Piyasa ekonomilerinde hemen her işlem bir ödeme gerçekleştirmektedir ve yeni işlemlerin gerçekleşebilmesi için daha önceki işlemlerin ödemelerinin zamanında alıcılarına ulaşması gerekmektedir. Güvenilir ve etkin ödeme sistemleri finansal piyasaların ve ekonominin düzenli çalışması ile ilişkilidir. Ödeme sistemleri işlemlerin zamanında ve güvenli tamamlanmasına ortam hazırlar. Firmalar mal ve hizmet alıp sattıklarında, kişiler maaşlarını alırken ya da perakende alımlarda, hükümetler vergi alırken ya da ödemelerinde ödeme sistemlerini kullanmaktadırlar.

Ödeme sistemleri bir bankanın müşterilerinin başka bankaların müşterilerine ödeme yapmalarına imkan sağlar. Kişiler kullanacakları bankayı seçerken çalıştıkları kişi ve kuruluşların ilgili bankanın müşterisi olup olmamasına bakmaksızın bankanın sunduğu kredi imkanları, hizmet kalitesi gibi özelliklere odaklanabilirler.

Etkin ödeme sistemleri finansal piyasaların işleyişi açısından önem taşımaktadır. Tahvil, bono, türev araçları, döviz işlemlerinin parasal tarafının mutabakatında ödeme sistemleri rol oynamaktadır. Katılımcılar fonlarının bankaları tarafından zamanında verileceğine güvenerek izleyen ve ilişkili işlemlerini gerçekleştirirler (Bank of England, 2000:6).

Para politikalarının başarı ile yürütülmesi ve finansal istikrarın sağlanması çalışmalarında da ödeme sistemleri önem taşımaktadır.¹

¹ 2.5 başlığı altında ödeme sistemleri ve finansal istikrar, 2.6 başlığı altında ödeme sistemleri ve para politikası ilişkisi detaylıca irdelenmiştir.

1.3 Ödeme Sistemlerinin Amaçları

Ödeme sistemlerinin amaçları

- Bankalar arası fon aktarımlarında etkinlik sağlanması
- Ödeme riskinin en aza indirgenmesi
- Fon yönetiminde kolaylık sağlanması
- Bankacılık sistemine yeni hizmetler sunma fırsatı verilmesi²
- Para politikalarının yürütülmesine ve finansal istikrara katkı sağlanması

şeklinde sıralanabilir.

Amaçlar net olmasına rağmen ödeme sistemleri pek çok yıllardan beri gelişimini sürdürmektedir. Her ülkedeki değişik koşullar (hukuki yapı, iletişim, altyapı, araç ve kurumların gelişme evreleri) her bir ödeme sistemini tekil kılmaktadır (Listfield & Negret, 1994:1). Bir ülkenin ödeme sisteminin alınıp başka bir ülkeye kopyalanması söz konusu olmamaktadır.

Ödeme sistemleri ile gerçekleştirilen işlemler şu şekilde listelenebilir :

- ❖ finansal kuruluşlar arasındaki ödemeler,
- ❖ döviz, karpayı, bono, para piyasası araçlarının mutbakatı gibi büyük hacimli işlemler
- ❖ ücret, maaş, vergi, çek, borç, alacak kartlarının ödemeleri gibi sayıca çok küçük hacimli işlemler (BoE ,2005 :7).

² İlk dört madde Türkiye Cumhuriyet Merkez Bankası internet sayfasından alınmıştır.

1.4 Rakamlarla Ödeme Sistemleri

Ödeme sistemlerinde gayri safi milli hasılları aşan, çok büyük meblağlar dönmektedir. Ödeme sistemlerinin önemi kavrandıkça, sistemler teknolojik olarak geliştikçe ve finansal işlemler globalleştikçe ödeme sistemlerinde gerçekleşen işlem hacmi de büyümektedir.

Bank of England'ın yayınladığı 2005 yılı gözetim raporuna göre Birleşik Krallık'ın ödeme sistemlerinden yıl bazında 130 trilyon sterlin civarında akış olmuştur ki bu rakam yurt içi gayrisafi milli hasılanın 120 katına karşılık gelmektedir. Ödeme akışlarının boyutunun büyüklüğü sistemde gerçekleşen işlem çeşitliliğini de yansıtmaktadır (BoE, 2005 :7).

2002 yılında yayınlanan bir çalışmadan alınan veriler G-10 ülkelerinin ödeme sistemlerinden günde 6 trilyon doların üzerinde bir tutarda işlem gerçekleştirdiğini belirtmektedir (Lindley, 2002: 77).³

Tablo- 1 ile Avrupa Birliği (AB) ülkelerindeki Real Time Gross Settlement (RTGS) sistemlerde işleme konu olan tutar ve gayri safi milli hasılaya oranları listelenmiştir.⁴ Rakamlar ödeme sistemlerinde dönen paranın büyüklüğünü gözler önüne sermektedir.

³ Belçika, Kanada, Fransa, Almanya, İtalya, Hollanda, İsviçre, İsveç, İngiltere, Amerika G-10 ülkelerini oluşturmaktadır.

⁴ RTGS : Real Time Gross Settlement bir ödeme sistemi türüdür ve 1.5.2 bölümünde detaylıca açıklanmıştır.

Tablo 1- AB Ülkelerinde Ödeme ve Gayri safi milli hasıla oranları ,2003

Ülke adı	Sistemin Adı	RTGS tutar toplam tutar / Gayri Safi Milli Hasıla	Yıllık RTGS tutar toplam Milyon AVRO
Lüksemburg	LIPS-Gross	206	4,755
İspanya	SLBE	95	70,208
Fransa	TBF	62	96,327
Almanya	RTGSplus	60	128,544
Belçika	ELLIPS	51	13,558
Hollanda	TOP	47	21,365
İrlanda	IRIS	41	5,502
Finlandiya	BoF-RTGS	25	3,645
Portekiz	SPGT	25	3,255
Avusturya	ARTIS	23	5,177
Yunanistan	HERMES	22	3,343
İngiltere	CHAPS	20	31,180
İtalya	BI-REL	19	24,761
Danimarka	KRONOS	17	3,208
İsviçre	ERIX	7	1,897

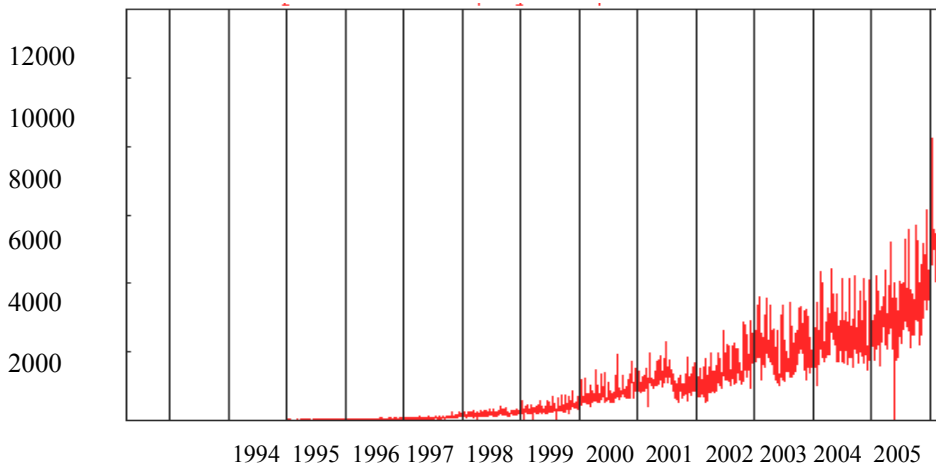
Kaynak : (Iivarinen, 2004: 22)

Türkiye ödeme sistemi EFT (Elektronik Fon Transferi), TCMB internet sayfasından edinilen bilgiler doğrultusunda, işleme geçtiği 1992 yılı boyunca sistemde toplam 534.853 işlem gerçekleşmiştir. Yıllar geçtikçe EFT sisteminin tüm bankalar arası ödemeleri kapsamına alması ve müşteri bankacılığı alanında yaygın bir kullanıma ulaşması sonucunda, yıllık işlem adedi önemli oranda artmış ve bu rakam 2004 yılı için 59.565.514 işleme ulaşmıştır. Parasal değerler yönünden bakıldığında ise 1992 yılında 1,8 Katrilyon TL (1992 yılı ABD Doları karşılığı 267 Milyar) olan bu değer; 2004 yılı sonunda 5.697 Katrilyon TL (2004 yılı ABD Doları karşılığı 3.985 Milyar) değerine ulaşmış bulunmaktadır

EFT sisteminde işlem gören paranın grafiği ise Şekil-1 ile gösterilmektedir. 2001 yılı krizinin etkileri grafikte de açık bir biçimde görülmektedir. Ödeme

sistemimizden geçen toplam meblağın giderek arttığı grafikten çıkarılacak sonuçlardan biridir. Türkiye Cumhuriyet Merkez Bankası elektronik veri dağıtım sisteminden (EVDS) elde edilen bilgiler doğrultusunda 22 Şubat 2006 tarihinde sistem bir rekor kırarak 103,368.744 milyon YTL para döndürmüş bulunmaktadır.

Şekil 1 - EFT sisteminde Milyon YTL bazında Toplam Ödeme Tutarı



Kaynak:: TCMB / EVDS

Para miktarının 2006 yılında bu şekilde artmış olmasının muhtemel nedenlerinden birisi olarak, kısa dönemde reel para arzı veri iken, artan para talebinin karşılanmasına yönelik olarak paranın dolaşım hızının söz konusu dönem için artmış olması ifade edilebilir. 2005 yılının son çeyreğinde yaşanan büyüme rakamları, söz konusu dönemde mal piyasasında ciddi bir canlılığa işaret etmektedir. Reel sektörde bu döneme ilişkin ödemelerin vadeli yapılmış olması da olasılıklardan bir diğeridir. Vadesi 2006 yılına sarkan bu ödemeler de, işlem hacmini artırmış olabilir.

1.5 Ödeme Sistemlerinin Sınıflandırılması

1.5.1 Tutarı Göre

Ödeme sistemleri işlemlerin tutar büyüklüğüne göre büyük tutarlı ve küçük tutarlı olarak ikiye ayrılmaktadır. Fakat büyük ve küçük tutarlı sistemler arasında kesin bir ayrım bulunmamaktadır. Genel olarak bankalararası işlemler, menkul kıymet ve ticari kurumlara ait işlemler işlem zamanlarının kısa olması gerekliliğinden dolayı büyük tutarlı ödemeler sınıfında yer almaktadır (Summers, 1994 :74). Başka bir deyişle, ödemenin tutarının rakamsal büyüklüğünden çok, ödemenin önceliği ve zaman kısıtları göz önüne alınmaktadır.

Büyük ölçekli ödeme sistemleri bölgesel ticaret ve finans merkezlerini birbirine bağlayarak fonların aynı gün içerisinde bölgeler arasında transferine olanak sağlamaktadırlar. Bu durum, takas ve mutabakat işlemlerinde meydana gelebilecek gecikme ve belirsizliklerin önüne geçmekte ve bölgeler arasındaki faiz farklılıklarını ortadan kaldırmaktadır.

Makroekonomik bir yaklaşımla; büyük ölçekli ödeme sistemleri kısa vadeli faiz oranlarının bölgeler arasında eşitlenmesini ve belli bir anda ülke genelindeki parasal göstergelerin ortaya çıkmasını sağlamaktadır.

Mikroekonomik bir yaklaşımla; söz konusu sistemler bankacılık kesiminin ve bankalar arası para piyasalarının likidite olanaklarını arttırarak bankaların merkez bankasına olan bağımlılıkları azaltıp piyasa koşullarına bağlı fon yönetimi imkanı

ortaya çıkarmaktadır. Aynı zamanda, likit bir bankalar arası para piyasasının varlığı parasal operasyonlarda merkez bankasına esneklik sağlamaktadır (Ergin, 2001: 16-17).

Çoğu ülkede büyük tutarlı ödeme sistemlerinin sahibi ve işletimcisi merkez bankaları iken, küçük meblağlı ödeme sistemlerinin sahibi ve işletimcisi genelde merkez bankaları olmamaktadır.

1.5.2 Mutabakat Türüne Göre

Ödeme sistemleri mutabakat türlerine göre ise Gerçek Zamanlı Birebir Mutabakat (RTGS :Real Time Gross Settlement) ve Gecikmeli Mutabakat (Deferred Settlement ya da Netting) sistemleri biçiminde ikiye ayrılmaktadırlar. Gecikmeli Mutabakat sistemlerinde bankaların gönderdikleri ve bankalara gelen ödemeler biriktirilmekte, gün içinde belli zamanlarda alacaklardan ve vereceklerden elde edilen net değer pozisyonlarına yansıtılarak mutabakat sağlanmaktadır (Johnson vd., 1998: 45). Bu sistemlerde mutabakat temsilcisi operasyonel ve finansal açıdan güvenilir olmalıdır, bu görevi de genelde merkez bankaları üstlenmektedir. Bu sistemler likidite kullanımını açısından ekonomiktir fakat katılımcıların gün içinde birbirlerine kredi vermesini gerektirmektedir (McAndrews & Trundle, 2001:127).

Gerçek zamanlı birebir mutabakat ve gecikmeli mutabakat sistemlerindeki farklılık mutabakata varma şekillerinden kaynaklanmaktadır. Her iki yaklaşımda da mesaj iletimi ve işleme aynı esaslarla yürütülmektedir.

1990 sonrası barındırdıkları kredi riskleri göz önünde bulundurularak DNS sistemleri, bilhassa büyük meblağlı ödeme sistemleri söz konusu olduğunda, yerini RTGS sistemlerine bırakmışlardır.

RTGS sistemlerinde her ödeme bağımsız olarak gönderilmekte ve fonlar uygunsa gönderilme zamanında mutabakatı yapılmaktadır. Netleştirme esasına dayanmayan sistemde gönderen banka borçlandırılmakta alıcı banka ise alacaklandırılmaktadır. Gönderen bankanın fonları işlem için yeterli değilse işlem gerçekleşmemektedir. Kimi sistemlerde ödeme mesajı gönderene iade edilmekte kimi sistemlere de ise mesaj kuyruklanarak fonların uygun olacağı zaman bekletilmektedir (Johnson vd, 1998:45). Bankaların gün içi likidite sıkışıklıklarını aşmak için pek çok ülkede merkez bankaları teminat karşılığı faizsiz gün içi ek likidite sağlamaktadır. Amerika Birleşik Devletleri'nde Federal Reserve Bankaları ise bu likiditeyi belirli bir faiz karşılığında sunmaktadır (McAndrews & Trundle, 2001:129). Modern RTGS sistemlerinde geri çevirme, kuyruklama, merkez bankası kredisi verme yöntemleri karma olarak kullanılmaktadır (BIS, 1997:10).

RTGS sistemlerinde mutabakatın kesin olması nedeniyle, bir ödeme sisteminin diğer ödeme sistemlerine bağlanması söz konusu olabilmektedir (BIS, 1997:11). Günümüz ödeme sistemlerinin diğer ödeme sistemleri ile bağlantıları düşünüldüğünde RTGS sistemlerin bu özellikleri bir kez daha önem kazanmaktadır. Gross ve Net sistemlerin seçimi görece maliyetler, mutabakat riskleri, operasyonel etkinlik, rezerv ihtiyaçlarına, sistemin merkez bankasının sahipliğinde ve yönetiminde olup olmasına göre şekillenmektedir (Johnson vd., 1998:45).

1990 sonrasında Kanada dışındaki tüm G-10 ülkeleri ve Avrupa Birliği ülkelerinin tümü RTGS sistemleri kullanmaya başlamıştır. Büyük tutarlı ödeme sistemlerinde reforma giden tüm ülkeler RTGS seçeneğini benimsemektedir. Dünya çapında işletime alınmış veya geliştirilmekte olan 70 RTGS sistem bulunmaktadır (McAndrews ve Trundle,2001:129).

İlerleyen bölümlerde detaylıca incelenecek olan ülkemiz ödeme sistemi EFT de RTGS esaslı bir sistemdir.

RTGS ve DNS sistemlerin olumlu yanlarının birleştirilmesi ile karma sistemler (Hybrid Systems) oluşmuştur. Kirdaban'ın 2005 yılında hazırladığı tezde 64 ve 65. sayfalarda Andrews ve Trundle'dan alıntılacağına göre bugüne kadar başlıca iki tür karma sistem ortaya çıkmıştır. İlk tür sürekli mutabakat (Continuous Net Settlement-CNS) olarak adlandırılmakta olup DNS'in gelişmiş bir şeklidir. Bu konudaki örnekler Fransız ve Amerikan sistemlerindeki Paris Net Mutabakat (PNS) ve NewCHIPS (New Clearing House InterBank Payment System)'dir. Bu sistemlerde katılımcılar hesaba bir miktar para yatırmakta ve tüm ödeme emirleri günün başlangıcında kuyruğa girmektedir. Bilgisayar algoritması büyük tutarlı netleştirmeleri aramaktadır. Bunlar mutabakat hesabının bakiyesinden daha fazla bir net borçlandırma yaratmamalıdır. Buna ve diğer belirli bazı kriterlere uyan bir grup ödeme bulunursa bunlar serbest bırakılır ve nihai olarak değerlendirilir. Algoritma gün boyunca sıklıkta çalışmakta ve (DNS'in tersine) bazı, belki de çoğu ödemelerin serbest bırakılmasına ve gerçek zamanlı olarak etkin bir şekilde mutabakatına izin vermektedir. Almanya'daki RTGSplus sistemi ile temsil edilen ikinci tür karma

sistem RTGS sisteminin içine kuyruklama imkanının dahil edilmesini savunmaktadır (artan kuyruklu RTGS sistemi). Bazı standart RTGS sistemlerinin ödemelerin serbestliğinin kontrolü için kuyruklama mekanizması olmasına rağmen, artan kuyruklu RTGS sisteminin ayırıcı özelliği, kuyruğa giren ödemelerle netleştirilen ödemelerin eş zamanlı olarak mutabakatlarının yapılmasıdır. Bu sıra basitçe, ödemelerin yalnızca ulaştıklarında önceliğin verildiği ilk giren ilk çıkar (FIFO) temelinde işleyebilir. İki taraflı netleşme süreci yalnızca bir çift katılımcı arasındaki karşılıklı ödemeye göre işlemektedir. Alternatif olarak, daha gelişmiş düzenlemeler, büyük tutarda netleştirilen daha geniş dizideki ödemeler için kuyruğu “çok taraflı” olarak tarayan algoritmayı da kapsayabilir. Böyle bir algoritma FIFO sisteminin zaman düzenini geçersiz kılmak için ya da aynı öncelik tanınan ödeme kategorileri içinde bunu yapmak için yazılabilir. Bu netleştirme süreci eş zamanlı toptan mutabakatı kapsamakta, yani bireysel ödemeler eş zamanlı olarak sık ve topluca yerine getirilmektedir. Yasal anlamda mutabakat toptandır (bireysel yükümlülükler net yükümlülüğün yerine konmamaktadır.) ancak, netleştirme ödemelerine ekonomik etkisi olmaktadır. Çünkü netleştirilen toptan ödemeler kendini teminat altına almaktadır.

Karma sistemlerin her iki türü de bir RTGS sistemine ihtiyaç duyarlar. Artan kuyruklu sistemde, sistemin kendisi örneğin yüksek öncelikli ödemelerde kullanılabilecek standart RTGS ödeme hizmetleri sunmaktadır. CNS sisteminde, gün boyunca ödemelerin yapılmasının mümkün kılınması ya da gün sonunda tamamlanmış ödemelerin yerine getirilmesi için bir RTGS sistemi yeterli olacaktır.

Bu alternatif tasarımlar arasındaki seçim bunları kurmanın ve işletmenin maliyetini içeren bir dizi unsura bağlı olacaktır. Merkez bankaları için kilit faktörler arasında mutabakat riskini ne ölçüde iyi içerdiği ve tasarımın katılımcılar için düzgün ödeme akışını sağlayıp sağlamadığı konularıyla ilgilidir (Kirdaban, 2005:65).

1.5.3 Sınırlarına göre

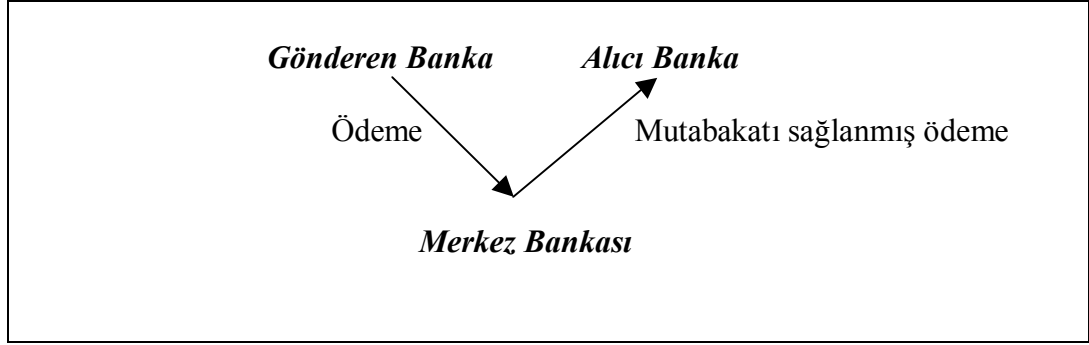
Ülke sınırları içinde gerçekleştirilip gerçekleştirilmemesine göre de ulusal ve uluslararası ödeme sistemleri olarak sınıflama yapmak mümkündür.

1.6 Ödeme sistemleri yapıları

Ödeme sistemleri gönderen banka, merkez bankası ve alan banka ilişkisi göz önüne alındığında merkez bankasının konumuna göre “V”, “Y”, “L” ve “T” olmak üzere 4 yapıda tanımlanır.

“V” yapılı sistemlerde tüm ödeme ayrıntıları merkez bankasına gönderilir ve merkez bankası tarafından alan bankaya ödeme iletilir. T.C. Merkez Bankası’nın EFT Sistemi “V” yapısındadır. Bu modele uygun olan diğer sistemler, Federal Reserve’ün Fedwire sistemi, Japon Merkez Bankası’nın BOJ-NET sistemi ve İsviçre Merkez Bankası SIC sistemidir. Şekil-2’de şematik olarak V yapısı gösterilmektedir.

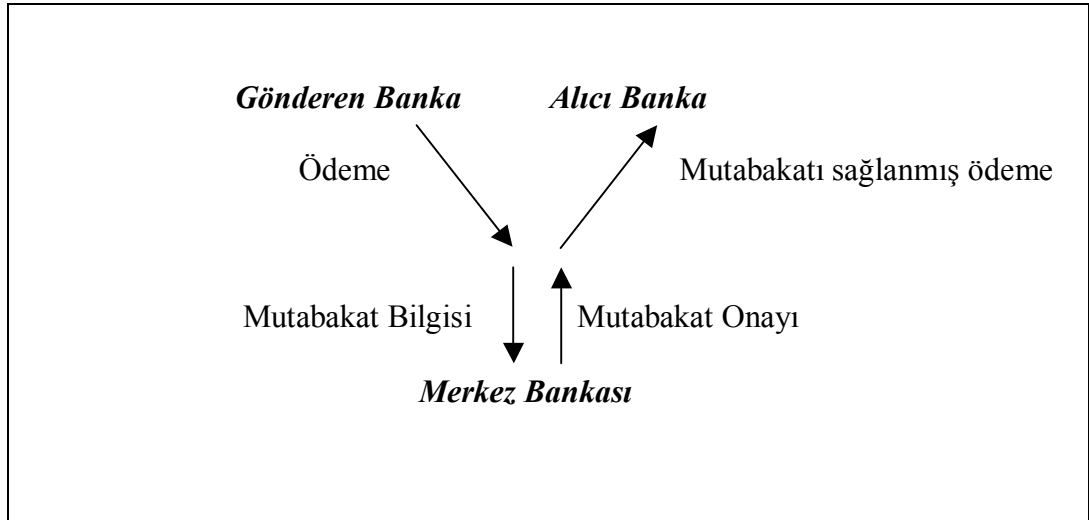
Şekil 2 - V tipi ödeme sistemi



Kaynak :Johnson vd. ,1998 :54.

“Y” yapılı ödeme sistemleri de oldukça yaygındır. “Y” yapısında, “V” yapısından farklı olarak ödeme ayrıntıları merkez bankasına gelmez yalnızca mutabakat ayrıntıları gelir. Bu modele de Fransa, İrlanda gibi ülkelerin ödeme sistemleri örnek verilebilir. Şekil-3’te şematik olarak Y yapısı gösterilmektedir.

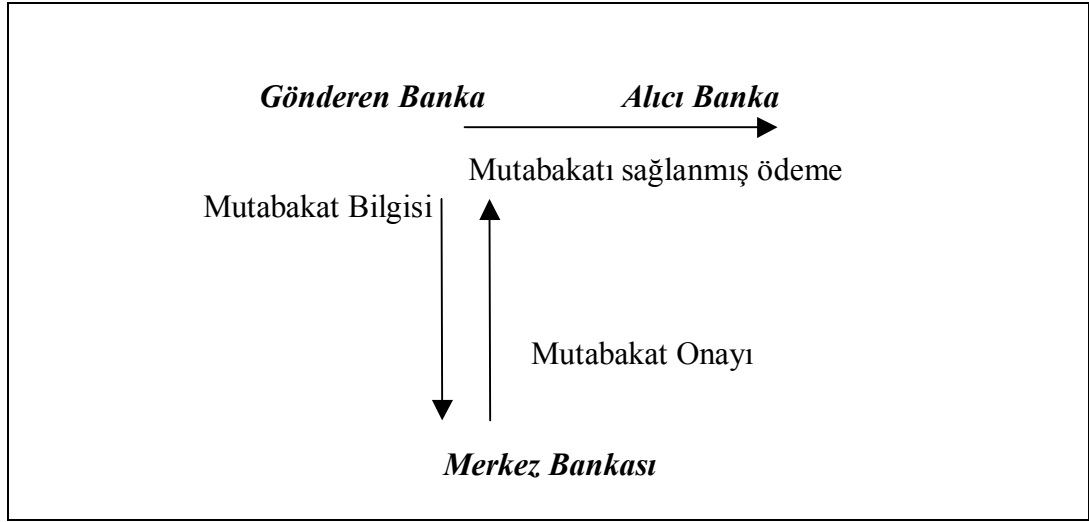
Şekil 3 - Y tipi ödeme sistemi



Kaynak :Johnson vd. ,1998 :54.

“L” yapısında gönderen banka merkez bankasına mutabakat bilgisini gönderir ve mutabakat yapıldıktan sonra yine gönderen banka tarafından mesajın kopyası alan bankaya iletilir. Şekil-4’da şematik olarak L yapısı gösterilmektedir.

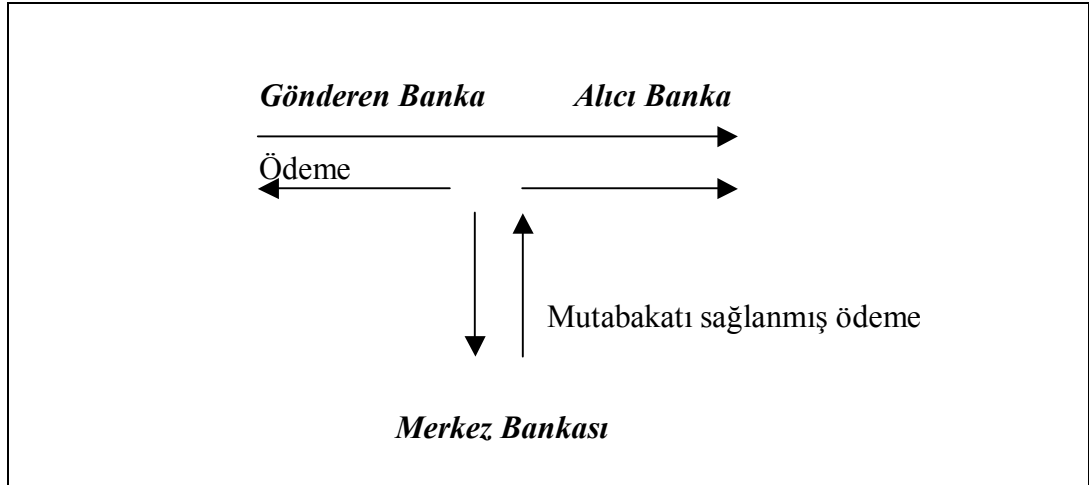
Şekil 4 - L tipi ödeme sistemi



Kaynak :Johnson vd. ,1998 :54.

“T” yapısında ise gönderen banka merkez bankası ve alan bankaya aynı zamanda mesajı gönderir ve merkez bankasından alan bankaya daha sonra teyit mesajı gönderilir (TCMB,2002:21). Şekil-5’de şematik olarak T yapısı gösterilmektedir.

Şekil5 – T tipi ödeme sistemi



Kaynak :Johnson vd. ,1998 :54.

İKİNCİ BÖLÜM

2 ETKİN BİR ÖDEME SİSTEMİNİN ÖNEMİ

2.1 Etkinlik Nedir?

Ödeme sistemlerinin etkinliğinden önce etkinlik kavramını netleştirmekte fayda bulunmaktadır. Etkinlik verimlilik kavramına göre daha geniş kapsama sahiptir. Verimliliği işleri doğru yapmak olarak tanımlarsak etkinlik kavramı doğru olan işi yapmak şeklinde ifade edilebilir. Etkinlik verimlilikten farklı olarak daha çok amaç ve hedeflerle ilgilidir ve şu şekilde formülize edilebilir:

$$\text{Etkinlik} = \text{Gerçekleşen Çıktı} / \text{Etkilerin amaç ve hedeflerle karşılaştırılması}$$

2.2 Etkin Ödeme Sistemi Nedir?

Ödeme sistemleri finansal marketlerin ve ekonominin düzgün çalışmasında can alıcı noktalardandır. Böyle önemli bir konuma sahip olan ödeme sistemleri için konulan hedefler stratejik önem taşımaktadır. Dolayısı ile bu hedeflere ulaşma derecesi yani etkinlik kavramı tüm otoritelerce kabul görmektedir. Amaç (finansal istikrar, para politikalarının uygulanması vb. kavramlar yardımıyla) finansal marketlerin ve ekonominin düzgün çalışması ise bir ödeme sistemi bu amaçları yerine getirebildiği ölçüde etkindir.

Ödeme sistemlerinin etkinliđi tüm merkez bankalarınca kabul gören ortak bir amaçtır. Öyle ki etkinlik kavramı sistemik açıdan önemli ödeme sistemleri için temel prensiplerden birini de oluşturmaktadır (Khiaonarong, 2003: 7).⁵

Ödeme sistemlerinin etkinliğine iki perspektiften bakılabilir: teknolojik ve ekonomik etkinlik. Teknolojik etkinlik gelişmiş bilgisayar ve iletişim teknolojilerinin ödeme ve mutabakat süreçlerine adaptasyonuna odaklanmaktadır. Ekonomik etkinlik ise, ödeme ve mutabakat süreçlerinde optimal maliyeti yaratacak operasyonel yönetim ve kaynak atamaları ile ilgilidir. Bu bağlamda teknolojik etkinlik ekonomik etkinliđin sağlanmasının bir yöntemidir. Ödeme sistemlerinin etkinliđi ise hem teknolojik hem de ekonomik etkinlikte artırımlarla sağlanabilir.

DNS sistemlerden RTGS sistemlere geçişle teknolojik etkinlik en iyi biçimde sağlanmıştır. Ekonomik etkinlik ölçek ekonomileri ile yakından ilişkilidir. Ölçek ekonomileri, birim ya da ortalama maliyette işlem hacimlerinin artması ile sağlanan düşüşle oluşur. Bir ödeme sistemi birden fazla çeşitte işlemi sabit maliyetlerle daha geniş bir çıktıyla oluşturduğunda da sağlanmaktadır. Ölçek ekonomilerinin kavranması, ödeme sistemlerinde servis sağlayıcıların optimal çıktıyı sağlayacak kaynak atamasını ve fiyatlandırma politikalarını sağlamalarında yardımcı olacaktır (Khiaonarong, 2003:10-11).

⁵Temel İlkeler başlıklı 3. bölümde Sistemik açıdan önemli ödeme sistemleri için temel ilkeler madde madde irdelenmiştir.

2.3 Paranın Dolaşım Hızı Ödeme Sistemleri İlişkisi :

Ödeme sistemleri, merkez bankaları ve ticari bankalarının özelleşmiş personeli için ana çalışma alanlarından birisi haline gelmiştir. Yüzyılın başında ekonomistler, “paranın dolaşım hızı”, “likit para stoğu (M1)” ve “ reel sektör (ekonomideki toplam işlem ölçüsü)” arasında ilişkiyi gözlemlemişler ve sonrasında bu ilişkiyi formüle etmişlerdir. Bu anlamda ekonomistlerin “ödeme sistemlerinin etkinliği” konusundaki ilişkilerinin de iki alanda yoğunlaştığı görülmektedir. Bunlardan ilki Ödeme sistemleri para arzı ilişkisi, ikincisi ve daha güncel olanı ise işlem (transaction) maliyetleri konularıdır (Listfiel ve Negret,1994).

Dolaşım Hızı:

Ödeme sistemleri ve paranın dolaşım hızı arasında yakın bir ilişki bulunduğu tezi oldukça eskidir. Wicksell (1898)’e göre “Paranın ödenebildiği ve transfer edilebildiği fiziksel koşullar dolaşımın hızının büyüklüğüne belirli sınırlar çizer.” Ödeme sistemlerinin etkinliği paranın dolaşım hızının büyüklüğü için bir üst sınır çizmektedir (Masha, 2002: 72) .

Miktar teorisinde ($MV = PT$) yer alan paranın dolaşım hızı V (M: Transfer edilebilir para (nakit (c) + vadesiz mevduat), P: Fiyatlar genel düzeyi, T: Ticaret Hacmi veya toplam işlem hacmi) ödemeler ile ödemenin yapıldığı para stoğunun arasındaki oranı ölçer. Kapsam olarak V, bütün ekonomideki işlem ve ödeme taleplerinin karşılanması için mevcut para stoğunun ne kadarlık miktarda tekrar kullanıldığını ifade eder.

Para stoğunu nakit ve vadesiz mevduat olarak ikiye ayırıp, farklı ödeme ve işlem taleplerini de işin içine katarsak;

$$(Mc.Vc + Md. Vd) = \text{Sum. } Pi*Ti$$

Md.Vd ekonomik aktivitenin göstergelerinden biri olarak kabul edilmektedir. Burada Md bankaların vadesiz mevduat hesapları, Vd ise bankanın bilançosunda borçların vadesiz mevduata oranı şeklinde ifade edilebilir. Bazı Merkez Bankaları, ki ABD Federal Reserve bunlardan biridir, bu oranları ilan etmektedir.

Ancak bu oranın yorumlanması ile ilgili çeşitli problemler vardır. Bunlardan ilki, birden fazla işlem tipinin, bankaların bu işlemlere dair ödemeleri ile ekonomideki üretim arasındaki bağlantıyı sınırlandırmamasıdır. Çünkü işlem ödemeleri arasında birbirinden ayırt edilmesi neredeyse imkansız olan, şirketlerin ve kişilerin kendi hesapları arasındaki para transferleri, menkul sermaye alım satımları, gelir transferleri ve çeşitli finansal piyasa hareketleri yer alır. Bu nedenle de çeşitli bankaların Vd oranları birbirinden aşırı derecede farklılık göstererek, bu oranın güvenilirliği konusunda kuşku uyandırabilir. Buna karşın, vadesiz mevduat hesaplarında gerçekleştirilen toplam işlem miktarındaki büyük artış kullanılabilir yeni finansal ürünler olduğunun, düzgün nakit yönetiminin işlem hızını arttırdığının ve bunların sonucunda da ödeme sisteminin güvenilirliğinin atıldığı göstergesidir.

Nakit ödemeler için kullanılan Vc için de kontrol edilmesi oldukça zor problemler söz konusudur. Ancak bu problemlere karşılık Vc ile kaba tahminler, bu oranın daha istikrarlı olduğunu ve gelişmiş ülkelerde 15 ile 20 arasında bulunduğunu ifade etmektedir. Eğer bu tahminler doğruysa, Vd'nin, Vc'den daha büyük olduğunu ve

nakit kullanımından vadesiz mevduat kullanımına doğru düzenli bir akışın gerçekleştiğini söylemek yanlış olmaz. Bu durum da toplamda para dolaşım hızının artışı anlamına gelir.

İşlem maliyetleri:

Ekonomistler tarafından işlem maliyetlerinin analizi de gün geçtikçe daha çok ilgi çekmektedir. İşlem maliyetleri aynen üretim maliyetleri gibi, firmaların işlem yapma, işlemlerin eşleşme, iletişim, bilgi değişimi, satın alınacak malın araştırılma, firmaların sözleşme yapma (ödeme şekli, zamanı ve ödeme yapılacak medyanın seçimi gibi parametreleri kapsayan) maliyetlerinin tamamını kapsar. Öte yandan işlem maliyetleri, mülkiyet transferi ve telif hakları ile ilişkili bütün maliyetleri de içerir.

İşlem teknolojisi (veya fonksiyonu) bir transferi gerçekleştirmek için gereken kaynakları belirler: Ticaret yapan firmaların değişik girdileri, araştırmanın ve işlem zamanının doğrudan ve fırsat maliyetleri, alış ve satış fiyatları (Ya da bunlarla ilgili alt ve üst sınırlar) arasındaki farklılık, diğer doğrudan (bir mal ya da fon elde etmenin ücreti) ve dolaylı işlem maliyetleri. Üretim fonksiyonuna benzer şekilde, işlem fonksiyonu, ödeme sisteminin tasarımı, mülkiyeti ve kontrolü için çeşitli anlamlar ifade edecek şekilde azalan, sabit veya artan ölçekte getiri sağlayabilir. Örneğin ölçek ekonomilerinde, rekabet kaynakların etkin bir şekilde tahsisine yol açmaz. İşlem maliyetleri, ulaştırma maliyetlerine benzese de, bunlar tek yönlü mal akımları ile değil, iki yönlü değişimle ilgilidir. Burada mal akımına karşılık bir ödeme akımı vardır.

İşlem maliyetlerini hesaba katmanın önemli sonuçlarından biri, bunun ekonominin brüt ticaret hacmine bir sınır getirmesidir. İşlem maliyetleri, işlem hacmini ve kazancı azaltıyorsa, bu durumda tüccarlar işlem maliyetlerini minimize etmeye çalışacaktır. Bu minimizasyon işleminin de daha etkin bir değişim medyasının ve ödeme sisteminin oluşmasına katkı sağlayacağı düşünülebilir. Bunlar da karmaşıklığı, maliyeti ve riskleri azaltıcı bir etki yaratacaktır. Daha etkin bir değişim medyasının ve ödeme sisteminin olmadığı, kısaca bunların regüle edilmediği çok firmalı bir dünyada ise karmaşıklığın, maliyetin ve risklerin arttığı ve işlemleri büyük ölçüde dengeleyici bir yapının oluştuğunu görmek kaçınılmaz olacaktır.

İşlem maliyetlerindeki azalma arttıkça, finansal servislerdeki işbölümü artacak, daha detaylı finansal sistem yapıları ortaya çıkacak, günlük işlem hacminin, işlem gören ticari varlık stoğuna oranı artacaktır. Bu da değişen işlem maliyetleri sonucunda finansal piyasalarda yaşanan hızlı değişimleri yorumlama ihtiyacını daha belirgin hale getirmektedir. Bir sonuç olarak, elektronik ödeme sistemleri ödeme gönderme alma işlemlerinde doğruluğu ve hızı arttırmaktadır.

Bir ödeme sistemini kurmak ve işletmek oldukça pahalı bir iştir. Bu sistemle sağlanan yeni kaydi paranın (kredi parasının) getirisinin, bu iş için ihtiyaç duyulan yatırımı dengelemesi gerekmektedir. Yararlar gün geçtikçe maliyetine daha ağır basarken, para da orijinal fiziksel ve metal birimlerinden ve kimliklerinden sıyrılmaktadır (Listfield ve Negret,1994:31).

2.4 Merkez Bankalarının Ödeme Sistemlerindeki Rolü :

Uzun yıllar ödeme sistemleri merkez bankalarının çok ilgisini çekmeyen arka planda kalan üzerinde politikalar üretilmeyen işlemler olarak devam etmiştir. Son 20 senede aşağıda sıralanan maddeler nedeni ile ödeme sistemleri merkez bankaları için önem kazanmıştır:

- a) Ödeme sistemlerinin ve yapılan transferlerin hem sayı hem de hacim olarak büyümesi. (Bahsi geçen büyüme dünya genelinde finansal piyasaların aktivitelerinde ve bu aktivitelerin oluşturduğu ödemelerde artış olarak yansımıştır.)
- b) Teknolojik gelişimlerin ödeme sistemleri üzerinde fonların daha hızlı akışına olanak sağlaması (Sheppard,1996: 7).

Ödeme sistemlerinin merkez bankalarının gündemlerinden operasyonel olarak önemli bir kavram olmaktan çıkıp yüksek düzeyde önemli politika kavramına dönüşmesinin önemli nedenleri arasında finansal sistemin istikrarı ve ödeme sistemlerindeki bir sorunun finansal sektör krizleri için en erken manifesto niteliğinde olması kaygıları yer almaktadır. Ödeme sistemlerinin istenen sonucu veren para politikaları üzerindeki etkileri de konuya merkez bankalarınca verilen önemin artmasına etken olmuştur (Masha, 2002:67).

Ödeme sistemlerinin kurulması, geliştirilmesi, işletimi ve denetimi süreçlerinde merkez bankalarının doğrudan rol almalarının nedenleri TCMB internet sitesinde aşağıdaki şekilde açıklanmıştır:

- Para politikalarının başarı ile yürütülmesi için sağlıklı işleyen bir ödeme sistemine gereksinim duyulması,
- Ülke ekonomisi yönünden yüksek stratejik önem taşıyan bu tür sistemlerde güvenlik ve denetimin sağlanması,
- Yüksek tutarlı fon ödemeleri ve menkul kıymet işlemlerinin merkez bankaları nezdinde tutulan hesaplar üzerinden yapılmakta olması,
- Denetim yetkisi ve mevzuat belirleyici konumu nedeniyle kredi riskinin ve sistemik riskin azaltılmasındaki rolü.

Günümüzde merkez bankalarının pek çok örnekte büyük meblağlı ödeme sistemlerinin sahibi ve işletmeni olduğu ve bu sistemleri düzenleyip gözettikleri görülmektedir.

2.4.1 Merkez Bankası Parası

Bugün merkez bankası dışındaki bütün bankalar geçici mevduatının belli oranını kanuni rezervler olarak ayırmak zorundadırlar. Fakat bu rezervleri muhakkak kağıt para şeklinde saklamak zorunlulukları yoktur. Müşterilerinin ani ihtiyaçlarını karşılamak için ayıracakları daha düşük orandaki kasa ihtiyatları dışında, bankalar genelde rezervlerinin bir kısmını merkez bankasında açtıracakları hesaplarda ve bunun da bir kısmını devlet tahvili olarak saklarlar. Gerek merkez bankası nezdinde bankalar lehine açılan bu alacaklı hesaplar, gerek devlet tahvilleri, arzu edildiği zaman derhal merkez bankasında paraya çevrilebilmektedir (Üstünel, 1983 :69).

Ödeme sistemlerinde mutabakat için merkez bankası nezdindeki hesaplar kullanılmaktadır. Gönderen bankanın hesabından düşülen tutarın alıcı bankanın hesabına eklenmesi ile mutabakat sağlanmaktadır. Likidite sıkıntısına düşülmesi durumunda merkez bankalarının sağladıkları krediler, kredi alan bankanın merkez bankasındaki hesabına yansıtılmaktadır.

2.4.2 Gözetim Fonksiyonu

Ödeme sistemleri merkez bankalarının temel amaçlarını üzerine inşa ettikleri temellerdir. Ödeme sistemlerinde oluşan bir sorun finansal istikrara ve para politikasına doğrudan yansiyacağı için, merkez bankaları ödeme sistemlerinin gözetim görevini üstlenmiştir (BoE, 2005: 8). Bilhassa Bank for International Settlement (BIS) temel ilkeler raporunun ardından merkez bankalarının ödeme sistemleri üzerinde oynadığı aktif rol daha iyi aydınlatılmıştır. Gözetimin amacı sistemik risklerin tanımlandığı ve ortadan kaldırılmaya çalışıldığı, sistem etkinliğinin ve güvenilirliğinin sağlandığı bir işletim yürütmektir.

2.4.2.1 Ödeme Sistemleri Gözetiminde Kilometre Taşları

6-8 Ekim 2003 tarihlerinde Alman Bundesbank tarafından Türkiye Cumhuriyet Merkez Bankası çalışanlarına verilen Ödeme Sistemleri Seminer notlarından yapılan derlemeye göre ödeme sistemleri gözetimindeki kilometre taşları şu şekilde listelenebilir :

- 1970 lerde iki gelişme olmuştur :

- Finansal işlemlerin genişlemesini yansıtır biçimde ödemelerin hacminde artış
 - Elektronik veri işleme ve telekominükasyon teknolojilerini kapsar biçimde yeni para transfer yöntemlerinin ortaya çıkması
- 1990 : Lamfalussy Raporuna uyum
- Sınır ötesi ve çoklu para birimi netleştirme adımlarının içermesi gereken 6 standart
 - Gözetim için sunulan 5 prensip
 - Pratikte standartlar kabul görmüş ve oldukça geniş bir şekilde uygulanmıştır
- 1993 : Avrupa Merkez Bankalarının “Ulusal Ödeme Sistemleri İçin Sağlanması Gereken Minimum Genel Özellikler (Minimum Common Features for Domestic Payment Systems) “ Raporu
- 10 prensip : Erişim koşulları, risk yönetimi politikaları, yasal konular, standartlar ve altyapılar, fiyatlandırma politikaları ve iş saatleri alanlarını kapsayan 10 prensip
 - 1. ana prensip “her katılımcı ülke yüksek hacimli ödemelerin gerçekleştirildiği bir RTGS sisteme sahip olmalıdır.”
- 1998 : Avro alanındaki tüm yüksek hacimli ödeme sistemleri Lamfalussy Standartlarına uyumluluk açısından incelenmiş ve uyumlu bulunmuştur.

- 1998 : Elektronik Para Raporu (Report on Electronic Money)
- 1999 : Trans European Automated Real-time Gross settlement Express Transfer (TARGET) sistemi hayata geçmiştir
- 2001 : Sistemik olarak önemli ödeme sistemleri için temel prensipler “Core Principles for Systemically Important Payment Systems” yayınlanmıştır.
- 2003 : Avro perakende Ödeme Sistemleri için gözetim standartları “Oversight Standards for Euro Retail Payment Systems”

2.5 Ödeme sistemleri ve finansal istikrar

Ödeme sistemleri reformu sadece finansal değerlerin ekonomide etkin ve güvenli aktarımını hedeflememiş aynı zamanda finansal piyasalarda probleme yol açacak ve sistemik risk ile sonuçlanacak likidite ve kredi risklerinin bulaşıcılığını da en aza indirmeyi de hedeflemiştir. Ödeme sistemlerinin finansal sektör istikrarı açısından önemi, ödeme sistemlerindeki sorunun sadece bir katılımcıyı etkilemekle kalmayıp yayılmacı bir etki ile sistemik risklere yol açabilme olasılığıdır (Pringle & Robinson: 2002).

2.6 Ödeme sistemleri ve para politikası

Ödeme sistemi kullanıcılarının “para” transferine olanak sağlayan düzenlemeler bütünüdür. Parayı teşkil eden parçaların ne olduğu ise para teorisinin temel sorusudur. Paranın kullanımı zaman içerisinde ve ülkeden ülkeye çeşitlenmiştir.

Pratikte, pek çok gelişmiş ülkede günümüzde “para” nakit (hükümet ya da merkez bankasınca basılmış bozuk para ya da banknotlar) ve kaydi olarak ayrılmaktadır (Bank of England, 2000 :4).

Para politikası ve ödeme sistemleri iç içe girmişlerdir. Merkez bankaları faiz oranlarını ve likidite politikalarını uygulayabilmek için etkin büyük meblağlı ödeme sistemlerine bağımlıdır. Para politikasının etkinliği nakit ve kaydi paradaki değişimlerle ilişkilidir.

Günümüzde, faiz oranlarının belirlenmesi ve kamuya açılan kredi tutarının doğrudan kontrol edilmesi gibi para politikası araçlarının yerine, bankaların rezerv ve likidite büyüklüklerini dolaylı olarak kontrol edildiği açık piyasa işlemleri (bankalararası para ve döviz piyasası işlemleri dahil) önem kazanmıştır. Açık piyasa işlemlerinin etkin bir şekilde gerçekleştirilebilmesi için aynı gün ödeme ve mutabakat işlemlerini yerine getiren, güvenilir ve etkin ödeme sistemlerine gereksinim duyulmaktadır. Belirtilen niteliklere sahip ödeme sistemleri, merkez bankalarının para politikalarının etkinliğini üç şekilde arttırmaktadırlar:

- 1) Etkin ödeme sistemleri, bankalar tarafından düzenli bir rezerv talebinin yaratılmasına katkıda bulunurlar.
- 2) Etkin ödeme sistemleri, kamu harcamaları ve döviz müdahalelerinin rezervler üzerindeki etkisinin ölçülmesine olanak sağlarlar.

3) Etkin ödeme sistemleri, derinliđi ve likiditesi olan bankalararası piyasaların kurulmasına yardımcı olurlar .

Aynı gn sonulandırma iřlemelerini gerekleřtiren ve tamamıyla otomasyona gemiř bir deme sistemi, arbitraj iřlemlerinin yardımıyla lkenin her tarafında faiz oranlarının birbirine eřitlenmesini sađlayarak lke bazında etkin bir para politikasının yrtlmesine olanak sađlamaktadır .

Etkin ve hızlı bir řekilde fon transfer ve sonulandırma iřlemlerinin gerekleřtirilemediđi deme sistemlerinde byk ve deđiřken tutarda yzen fonlar mevcuttur. deme sistemleri nedeniyle ortaya ıkan yzen fonların miktarının byk olması durumunda, bankacılık sisteminin likidite durumunu izlemek ve kontrol etmek olduka zorlařmaktadır. Yzen fon tutarının yksek olduđu deme sistemlerinde, bankalar merkez bankaları nezdinde tutulan mutabakat hesaplarında ihtiyat olarak geređinden fazla fon tutmak iin kendilerini zorlamakta ve merkez bankaları gn ii kredi kullanımlarını gecelik kredilere kolaylıkla dnřtrme ihtiyacı hissetmektedirler. Her iki durum da para piyasası aralarının ve bankalar arası piyasaların geliřimini engellemektedir (Ergin,2001: 54).

Merkez bankalarının ekonomik faaliyetler zerindeki etkisi kısa dnemli likiditenin, bilhassa bankaların bakiyelerin mutabakatı iin ihtiya duyulan demelerin, ulařılabilirliđi ve maliyeti ile iliřkilidir. Mutabakat merkez bankası rezervlerindeki hesaplardan gerekleřmektedir. Rezervlerde talep ve mutabakat iin bakiyenin yetmediđi durumlarda kredi nem kazanmaktadır. Para politikaları likidite ynetimi

ile donatılmış ÷lkelerde ödeme sistemleri programın amalarını gerekleřtirmekte birkaç nedenden dolayı önemli rol oynayacaktır:

Öncelikle, tekrar oluşturulmuş ve görelili olarak daha etkinleřtirilmiş bir ödeme sisteminde, rezerv taleplerinde bir kayma olacaktır. Para politikaları likidite yönetimine odaklı merkez bankalarının politika uygulamalarında daha esnek yaklaşımlara sahip olmaları gerekmektedir. Bilhassa RTGS sistemlerin kullanımında, likidite yönetimi piyasalardaki kısa dönemli faiz oranlarında, çoėu faaliyet para piyasalarına kaydığı için ikincil bir rol oynayabilir.

Bunu izleyen bir biçimde piyasa oranları mutabakat sisteminin işlemlerinden ve merkez bankalarınca zorlanan düzenleyici ortamdan kuvvetli bir biçimde etkilenebilir. Eğer bankalar arası piyasada geçici rezerv ihtiyaçları merkez bankaları tarafından karşılanırsa, bankalar arası oran durum bu olmadığında olacağından daha oynak olmayacaktır. Fakat merkez bankasına açılan olasılıklar finansal ajanların teminat karşılığı kredi alıp alamadığına baėlıdır.

RTGS sistemlerde dört likitide kaynaėı söz konusudur :

- Merkez bankasındaki hesaplar
- Diėer bankalardan gelen ödemeler
- Merkez bankasından alınan krediler
- Ve diėer bankalardan alınan borlar.

Merkez bankasındaki hesaplar istenen rezerv miktarı ve çeşitli nedenlerle tutulması gereken fazla rezervle ilişkilidir. Para politikası açısından, merkez bankalarının verilen kredi ek likidite verilmesini temsil etmektedir. Para piyasasından borç almak, para stoğunu önemli oranda arttırmaya da sistemde erişilebilir olan fonların yeniden dağıtımına neden olmaktadır. Bununla birlikte, bu durum faiz oranları üzerinde bir baskı oluşturabilmektedir. Para politikasının amaçlarının gerçekleştirilmesi doğrultusunda bankalar ek likidite zerk edilmesini göze alarak merkez bankasından kredi almayı mı, kısa dönemli faiz oranlarına etki olasılığı ile para piyasalarına yönelmeyi mi tercih etmelidir? Para politikasının kapsamı içinde, para yönetimi amaçlarını gerçekleştirmek doğrultusunda tartışılmalıdır.

Etkin olmayan ödeme sistemlerine sahip ekonomilerde likidite yönetimi, bilhassa etkin olmayan süreç ve teknolojilerde, bir problem olabilir. Etkin olmayan ödeme sistemlerinde ekonominin emici kapasitesinden daha fazla kredinin yaratılmış olması ihtimal dahilindedir (Masha:2002: 72).

ÜÇÜNCÜ BÖLÜM

3 EFT ve EMKT SİSTEMLERİ

Elektronik Fon Transfer (EFT) Sistemi Türk Lirası üzerinden ödeme işlemlerinin, Elektronik Menkul Kıymet Transfer (EMKT) Sistemi ise menkul kıymet aktarımlarının bankalar arasında elektronik ortamda, gerçek zamanlı olarak yapılmasını ve gerçek zamanlı mutabakatını sağlayan sistemlerdir. Uluslararası literatürde EFT Sistemi TIC-RTGS (Turkish Interbank Clearing - Real Time Gross Settlement System), EMKT Sistemi TIC-ESTS (Turkish Interbank Clearing-Electronic Security Transfer and Settlement System) adı ile anılmaktadır.

EFT Sistemi 1 Nisan 1992 tarihinde işleme açılmıştır. İşletim sırasında katılımcılardan gelen isteklere ve ortaya çıkan yeni gereksinimlere göre çeşitli iyileştirmeler yapılmıştır. 24 Nisan 2000 tarihinde yeni işlevlerin eklenmesiyle sistem yazılım ve donanımda önemli değişikliklerin yapıldığı ikinci kuşak devreye alınmıştır. EMKT Sisteminin ön çalışmalarına EFT Sisteminin kuruluşundan sonra başlanmış ve sistem 30 Ekim 2000 tarihinde işleme alınmıştır.

EFT2 sistemi hem müşteri bankacılığı işlemlerini hem de yüksek montanlı işlemleri bir arada gerçekleştiren bir ödeme sistemidir. Pek çok ülkede düşük ve yüksek meblağlı sistemler ayrılırken ülkemizde maliyetler, birden fazla sisteme bağlanmanın bankalarımıza getireceği yük ve komplikasyonlar düşünülerek iki görevi de üstlenen tek bir sistem kurulmuştur. EFT2 sisteminde yüksek ve düşük meblağlı işlemleri birbirinden ayırabilmek amacıyla toplu mesaj gönderimi denilen yapı tasarlanmıştır. Katılımcılara hissettirilmeyecek şekilde belli bir tutarın altındaki işlemler kısa

sürelerle gruplanarak merkez sisteme tek bir mesajmış gibi gönderilmektedir. Merkezde tek bir mesaj gibi işlem gören mesajlar alıcılara ayrıştırılarak gönderilmektedir. (Okay, 2001) .

EMKT sistemde devlet iç borçlanma senetleri ile birlikte Özelleştirme İdaresi ve Kamu Ortaklığı Fonu gibi diğer kamu kuruluşları tarafından ihraç edilen senetlere ilişkin işlemler yapılır. Menkul kıymetlere ilişkin bilgiler bu sistemde elektronik ortamda, kaydi olarak tutulmaktadır.

EMKT Sistemi temel olarak bir gerçek zamanlı ödeme karşılığı teslimat sistemidir. Bu sistemde teslimat ve ödemenin mutabakatı eş zamanlı olarak yapılır. Dolayısıyla bu işlemde kredi riski bulunmamaktadır.

TCMB bir katılımcı olarak EMKT Sistemine bağlıdır. Katılımcıların TCMB'deki çeşitli piyasalarda işlem yapmak için kullandıkları teminat depolarına giriş ve çıkışlar TCMB sistemine bilgi verilmesi ve onay alınmasıyla gerçekleşir.

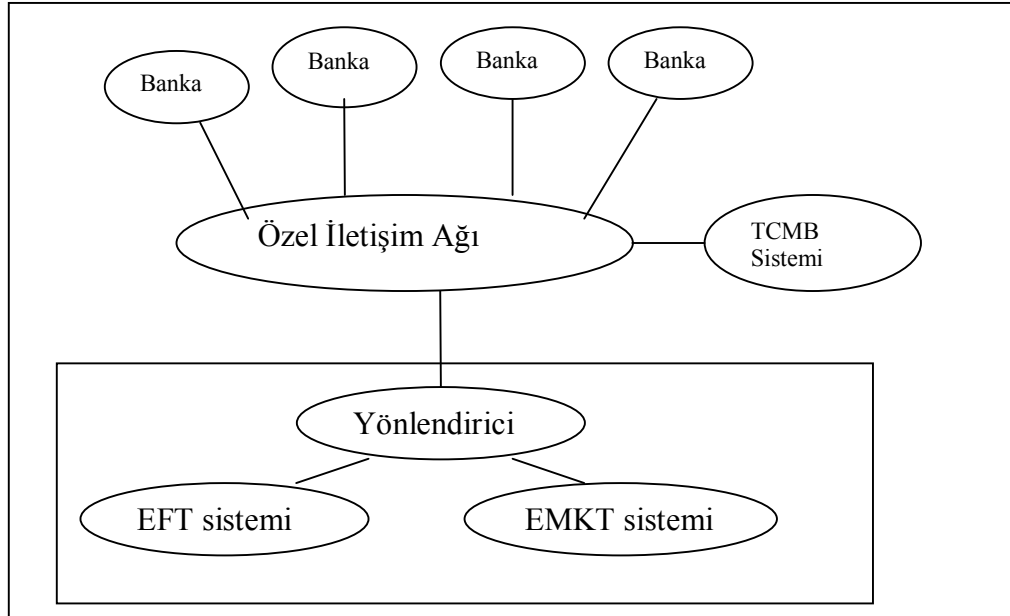
EMKT Sisteminin EFT Sistemi ile doğrudan bağlantısı bulunmaktadır. İki katılımcı arasında ödeme karşılığı teslimat koşuluyla fon ve kıymet aktarımı istendiğinde kıymet ve fon aktarımlarının eşzamanlı yapılması bu bağlantı sayesinde sağlanır.

Bankalar ve aracı kurumlar tarafından İMKB'de yapılan işlemlerin mutabakatının gerçekleştirildiği Takasbank bir banka olarak bu sisteme bağlıdır. Sisteme bağlı diğer katılımcılar ile Takasbank arasındaki menkul kıymet aktarımları EMKT Sistemi ile

yapılır. İMKB’de Devlet iç borçlanma senetlerine ilişkin yapılan işlemlerin mutabakat sonuçları da EMKT Sisteminde gerçekleştirilir. Ayrıca EMKT Sistemi katılımcısı olmayan aracı kurumlarına ilişkin aktarımlar da Takasbank aracılığıyla EMKT Sisteminde gerçekleştirilir (TCMB, 2002).

Şekil-6’da EFT – EMKT sistemlerinin yapısı görülmektedir. Bankalar özel iletişim aracılığı ile mesajlarını EFT EMKT merkezine göndermektedirler. Yönlendirici mesajın türüne göre mesajı EFT sistemine ya da EMKT sistemine yönlendirmektedir. İlgili sistem, mesajın başlığında bulunan alıcı bilgisine istinaden mesajı alıcı bankaya iletmektedir.

Şekil 6 - EFT – EMKT şeması



Kaynak : (TCMB, 2002 : 1).

EFT ve EMKT Sistemlerinin kesintisiz hizmet vermesini sağlamak üzere yedekli bir yapı kurulmuştur.

EFT Merkez Sistemi :

EFT Merkezi katılımcıların fon aktarımlarının ve mutabakatlarının yapılmasını, hesaplarının işlenmesini ve çeşitli raporların alınmasını sağlar. Merkezde; gün içinde katılımcıdan elektronik olarak gönderilen mesaj alınır, gönderen katılımcının EFT Merkezinde bulunan hesabı uygunsa eksiltir, alıcının hesabı artırılır ve alıcıya mesaj gönderilir. Gönderenin hesabı uygun değilse mesaj kuyruklanır, hesap uygun olduğunda otomatik olarak işlem yapılır. Mutabakat EFT hesapları üzerinden, mesaj alındığı zaman, gerçek zamanlı olarak yapılır. Gün sonunda katılımcılara ve TCMB'ye hesapların son durumları iletilir.

EMKT Merkez Sistemi :

EMKT Merkezi katılımcıların menkul kıymet aktarım ve mutabakatlarının yapılmasını, depo kayıtlarının işlenmesini ve çeşitli raporların alınmasını sağlar. Merkezde; gün içinde katılımcıdan elektronik olarak gönderilen mesaj alınır, gönderen ve alan katılımcının EMKT Merkezinde bulunan depo hesapları eksiltir/artırılır, alıcıya mesaj gönderilir. Mutabakat EMKT merkezinde tutulan depolar üzerinden, mesaj alındığı zaman, gerçek zamanlı olarak yapılır. Ödeme karşılığı yapılan kıymet aktarım istekleri için EFT Sistemi ile bağlantı bulunmaktadır. Gün sonunda katılımcılara ve TCMB'ye depoların son durumları iletilir.

Katılımcı Aktarıcı Bilgisayarı:

Bir katılımcının, EFT ve EMKT sisteminde mesaj alışverişi yapabilmesi için, üzerinde gerekli yazılım bulunan uygun aktarıcı bilgisayarı edinmiş olması gerekir. Aktarıcı bilgisayar üzerindeki yazılımlar TCMB'nin sorumluluğundadır. Yazılımlar üzerindeki her türlü değişiklik ve yükseltim TCMB tarafından yapılır. Katılımcı, aktarıcı bilgisayarı ile iletişim hatlarını kullanarak EFT ve EMKT merkezine erişir, herhangi bir katılımcıya göndermek istediği mesajı hazırlar, alıcıya iletmek üzere mesajı merkeze gönderir, kendisine gönderilen mesajları alır, gün içinde ve günsonunda anlık sorgulama yapar, raporlar alır, gönderdiği ve aldığı mesajları arşivler. Katılımcı yerel aktarıcı bilgisayar terminallerini kullanabileceği gibi aktarıcı bilgisayara uzaktan bağlı terminallerini de kullanabilir.

Katılımcı Anabilgisayarı:

Anabilgisayarı olan katılımcı tarafından istenirse özel protokol ile aktarıcı bilgisayar-anabilgisayar bağlantısı kurulabilir. Böylece aktarıcı bilgisayarın yanı sıra anabilgisayardan da yukarıda sözü edilen mesaj gönderme, mesaj alma, sorgulama işlemleri yapılabilir.

TCMB Sistemi :

TCMB sistemdeki tüm katılımcıların hesaplarını ve depolarını izler, sisteme fon aktarır. Gerekğinde katılımcı hesaplarından fon, depolarından kıymet doğrudan borçlandırması yapar,

Özel İletişim Ağı :TICNET

Katılımcıların sistemleri ile merkez sistemler arasındaki iletişim özel iletişim ağı (TICNET) üzerinden sağlanır. İletişim ağının kapsamı aktarıcı bilgisayarların iletişim hattına bağlandıkları modemden başlayıp, Ankara'daki merkez sistemin girişinde son bulur. Ankara ve İstanbul'da iletişim ağına giriş için birer özel sistem bulunmaktadır. Katılımcılar bu sistemler aracılığıyla EFT ve EMKT merkez sistemine ulaşırlar. TICNET kapsamında katılımcılar iletişim sistemlerine kiralık iletişim hatları ile bağlanırlar. Ankara ile İstanbul arasında özel kiralık hatlar ile iletişim kurulmuştur.

X.25 iletişim protokolü ile çalışan ağ altyapısı, 28 Kasım 2005 tarihinden bu yana TCP/IP iletişim protokolü ile çalışmaktadır.

EFT Sisteminin Amaçları:

- Nakit dolaşımını azaltmak
- Ödemelerin güvenli, güvenilir, hızlı ve risksiz gerçekleşmesini sağlamak
- Sağlıklı ve hızlı bilgi sağlamak
- Para politikasının etkin olarak uygulamasını kolaylaştırmak
- Elektronik bankacılık uygulamalarının gelişmesini sağlamak

EMKT Sisteminin Amaçları:

- Fiziksel basım ve değişimi azaltmak
- Maliyetleri düşürmek
- İşlem gerçekleştirmeyi kolaylaştırmak
- Sağlıklı ve hızlı bilgi sağlamak
- Piyasalarda gelişmeyi sağlamak

EFT ve EMKT Sistemlerinde katılımcılar arası iletişimde, iletişim birimi olarak "mesaj" olarak adlandırılan yapı kullanılmaktadır. Bir mesaj, başlık ve veri olmak üzere iki bölümden oluşur. Mesaj başlık bölümü: Mesaj türü, mesajı gönderen katılımcı, mesajı alacak katılımcı, aktarılacak para miktarı ve sistemler tarafından mesaj izlemede kullanılan sayım bilgilerini içerir. Her mesaj için başlık bölümü aynı yapıdadır. Mesaj veri bölümü ise yapılan işleme ait operasyonel açıdan gerekli ek bilgileri içerir. Her mesaj türü için içeriği farklılık gösterebilir (TCMB,2002).

T.C MERKEZ BANKASI'NIN YERİ

EFT ve EMKT Sistemlerinin sahibi olan TCMB aynı zamanda sistemlerin işletimini de yapmaktadır. TCMB, kendisine 25.4.2001 tarih, 4651 sayılı kanun ile değişen 1211 sayılı TCMB Kanununun verdiği yetkiyle ödeme sistemlerinin kullanımını yaygınlaştırmak, sistemlerin kesintisiz işlemlerini ve denetimini sağlayacak düzenlemeleri yapmak, sistemlerin güvenilirlik ve etkinliklerini artırmak ve sistemleri gereksinimler doğrultusunda geliştirmek amacıyla bu konudaki her alanda çalışmalarını sürdürmektedir. Bu çerçevede, EFT ve EMKT Sistemlerinin uluslararası ödemelerin mutabakatlarıyla ilgili üst kuruluş olan BIS tarafından saptanmış bulunan Temel İlkeler ile uyumlu olması için de çalışmalar yürütmektedir.

Türkiye Cumhuriyet Merkez Bankası da geliştirdiği ve denetlediği EFT ve EMKT Sistemi ile güvenilir ve etkin ödeme sistemi hizmetlerinin gelişmesinde öncülük görevini yüklenmiştir. RTGS sistemi ile fonların etkin olarak aktarımı amaçlanmış ve

işlevsel süreçler ile hak ve yükümlülükler TCMB ile katılımcı bankalar arasında yapılan özel anlaşma hükümleri çerçevesinde düzenlenmiştir.

TCMB'nin sistemle ilgili sorumlulukları sistemin işlemesinden ve katılımcılara gerek teknik, gerekse yardım masası desteği vermek, sistemin yasal ve işlevsel çatısını kurmak, sistemi bütünüyle kontrol etmek, katılımcıların gereksinimlerini ve sistemin geliştirilme gereksinimini sorgulamak ve sistemi geliştirmeye yönelik olarak bankacılık sektöründeki yeni eğilim ve gereksinimleri değerlendirmek olarak sıralanabilir. TCMB'nin bu sorumlulukları çerçevesinde müdahalesi daha önce bahsedilen gerek yasal, gerekse işlevsel anlamda görülebilecek olası riskleri ortadan kaldırmakta ve ödeme sisteminin güvenilirliğini artırmaktadır.

EFT Sisteminde, katılımcıların TCMB nezdinde bulunan EFT hesabında yeterli fonun bulunması şartıyla ödeme emirlerinin kabul edilmesi ise, kredi riskinin ortadan kalkmasına neden olmaktadır. Piyasadaki kur ve faiz oranlarında meydana gelebilecek dalgalanmalardan kaçınmak amacıyla likidite ayarlaması görevi de bulunan TCMB, bu sistemle ödeyememe riskini ortadan kaldırmış olmasının yanı sıra, istenmeyen likidite hareketlerinin piyasalarda meydana getirebileceği olumsuz sonuçları da önleyebilmektedir (TCMB, 2002).

Sisteme İlişkin Bilgiler

Sistemler resmi tatil günleri dışında 08:00-17:30 saatleri arasında açık bulunmaktadır. Gerekliği taktirde, TCMB tarafından sistemin çalışma saatleri uzatılabilir. EMKT sistemi EFT sisteminden önce kapatılmaktadır.

Başvurusu TCMB tarafından onaylanan, Rezerv Kontrol Sisteminde rezerv bulundurmakla yükümlü olan, Bankalar Kanunu uyarınca Türkiye’de faaliyette bulunan bankalar ile özel finans kurumları EFT ve EMKT Sistemlerinde katılımcı olabilir .

Katılımcıların EFT ve EMKT Sistemlerine bağlanmada kullandıkları aktarıcı bilgisayar donanım ve yazılımı ile iletişim sisteminin yatırımı ve giderleri Türkiye Bankalar Birliği'nin koordinasyonu ile katılımcılar tarafından karşılanmaktadır (TCMB, 2002). Sistemde mesaj ücretleri yıl bazında değişmektedir. 2006 yılı için haber mesajlarından 10 kuruş, 4000 YTL ye kadar tutar içeren ödeme mesajlarından 10 kuruş, 420,000 YTL üstü tutar içeren ödeme mesajları için 10,50 YTL alınmaktadır. 4000 YTL ile 420,000 YTL arasında tutar içeren ödeme mesajları için 0,0025 oranında masraf kesilmektedir. Belirtilen kapanış saatinden sonra mesaj göndererek kapanış saatini geciktiren katılımcılardan gönderilen her mesaj için ek ücret almaktadır. Çeşitli mesajlar için ücretlendirme yapılmamaktadır. Merkez bankasının belirli hesaplarına yapılan ödemeleri içeren mesajlar, ihalelere teklif sunulan MERB_HAZ1 mesajları da bu kapsamda bulunmaktadır.

Sistemlerde kuyruklama mekanizmaları bulunmakta ve TCMB tarafından gün içi likidite sağlanmaktadır.

Sistemde her biri 50 karakter içeren 10 satırlık mesajlarla iletişim kurulmaktadır. Mesajların ilk 4 satırı başlık bölümünü, 6 satırı ise veri bölümünü oluşturmaktadır. Mutabakatı yapılmış mesajların iptali söz konusu değildir. Merkez bankasına ait işlemler (Açık Piyasa, Döviz Efektif Piyasası ve TL piyasası işlemleri) MERB kodu ile başlayan mesajlarca gerçekleştirilmektedir.

Sistemin CPSIPS temel ilkeleri ile uyumlu olduđu belirtilmektedir (TCMB ,2002).

Sistem ödeme sistemleri amalarını gerekleřtirmekte ve etkin bir řekilde alıřmaktadır.

Sistemin 09.07.2006 tarihi itibariyle 49 katılımcısı bulunmaktadır.

DÖRDÜNCÜ BÖLÜM

4 BAZI ÖDEME SİSTEMLERİNE GENEL BİR BAKIŞ :

4.1 RTGSplus – Almanya

Rahat ve etkin günüçi likidite yönetiminin giderek daha önem kazanması Bundesbank'ın entegre, likidite kazançlı, gerçek zamanlı RTGS sistemini oluşturmasına neden olmuştur. RTGSplus sistemi ile Almanya TARGET sistemine bağlanmaktadır(BIS, 2003:162).

Alman RTGSplus sistemi Avrupa Birliği'ndeki ödemelerin hem işlem hem de tutar hacmi olarak pek çoğunu gerçekleştirmektedir. RTGSplus yeni karma sistemler kategorisinde bulunmaktadır. 2001 yılında hayata geçen sistem, netleştirme sistemlerinin likidite avantajlarını, RTGS sistemlerin iyi özellikleriyle harmanlayarak karma bir sistem oluşturmuştur. RTGSplus RTGS sistemlere yeni, ek özellikler de sunmuştur. Katılımcıların likidite akışlarını etkin olarak denetleyebilecekleri kontrol mekanizmaları yaratılmıştır (Iivarinen, 2004:..27). RTGSplus sisteminde kuyruklar ve kuyruklar içinde ofset netleştirmeler ile mutabakat sağlanmaktadır.

RTGSplus katılımcılarına gerçek zamanlı bilgi sunmakta ve katılımcılarının modern internet teknolojilerini bilgi ve kontrol sisteminde (ICS) kullanarak kontrol parametrelerin değiştirmelerini sağlamaktadır (BIS,2003:162).

Ayrıca RTGSplus katılımcılarına gerek duydukları bireysel kontrol kombinasyon opsiyonlarını sunmaktadır. Her katılımcı, iki yönlü veya çok yönlü gönderici limitini seçebilir. İki veya çok yönlü limit tam bir likidite kontrolü oluşturmak için tasarlanmıştır. İki yönlü limit katılımcının başka bir katılımcıya göndereceği limiti belirtirken çok yönlü gönderici limiti ise tüm katılımcılara gönderilebilecek limiti belirler. Bu yöntemle gönderici katılımcı likidite akışlarını etkin olarak kontrol edebilmektedir (Iivarinen, 2004:28).

4.2 Fedwire and CHIPS- Amerika

Fedwire Amerika Birleşik Devletleri'nde da kullanılan RTGS sistemidir. Fedwire sistemi 12 bölgesel Federal Reserve Bankası tarafından sahiplenilmiş ve işletilmektedir. Fedwire genellikle büyük hacimli ve zaman kritik ödemeler için kullanılmaktadır (Iivarinen, 2004:).

Fedwire sisteminden günde ortalama 460,000 yaklaşık 1.7 milyar hacimli ödeme geçmektedir (Iivarinen, 2004:32) .

Fedwire sistemi ulusal ödemeler için kullanılırken sınır ötesi ödemeler CHIPS (Clearing House Interbank Payment System) sistemi tarafından gerçekleştirilmektedir. Dünya çapında ülkeler arasında dönen dolar ödemelerinin %95 i bankalar tarafından sahiplenilen bu sistemde gerçekleşmektedir. Sistem aynı zamanda bankalararası ödemeleri ve müşteri ödemelerini de gerçekleştirmektedir (Iivarinen, 2004:32).

CHIPS 1970'lerde mevcut kağıt tabanlı ödeme sisteminin elektronik muadili olarak oluşturulmuştur. Önceleri çoklu netleştirme mutabakat sistemi olan CHIPS 2001 yılından bu yana karma bir sistem olarak hizmet vermektedir (BIS,2003 :444-445).

Karma Chips sisteminde, çoklu netleştirme sürekli olarak rol almakta ve ödemelerin çoğunun sabah saatlerinde mutabakatı sağlanmış olmaktadır. Sistem gün boyunca ortalama 250,000 işlem gerçekleştirmekte ve bu ödemelerin hacmi 1.2 trilyon doları bulmaktadır (Iivarinen, 2004:32).

4.3 BOJ-Net - Japonya

BOJ-NET (Bank of Japan Financial Network System) Japonya'da kullanılmakta olan RTGS sistemidir. 1988 yılında mutabakat için DNS ve RTGS biçimleri sağlanarak tanıtılmıştır. Fakat DNS sistemlerdeki riskler göz önünde bulundurularak yeni bir RTGS sistem 2001 başlarında oluşturulmuştur. Yaklaşık tüm ödemeler RTGS esasına göre gerçekleşmektedir. Ödemelerin bazıları iki yönlü netleştirme esasına göre katılımcılar ve merkez bankası arasında netleştirilmektedir. Mutabakatlar gün boyunca belirlenmiş saatlerde eş zamanlı olarak gerçekleşmekte ve ödemeler işlendiğinde kesinleşmektedir (Iivarinen, 2004:33).

2001'de BOJ-NET de 77 trilyon japon yeni hacminde işlem gerçekleştirilirken 2000 yılında 142,7 trilyon japon yeni işlem gerçekleştirilmiştir. İşlem hacmindeki bu keskin düşüşün nedeni 2001 yılındaki RTGS sistem değişikliğidir (Iivarinen, 2004:33-34).

Japon merkez bankası BOJ-NET'in hem sahibi hem de işleticisidir.

Japon Merkez Bankası, 3 Şubat 2006 tarihinde internet sitesinde yeni bir projeye başladıklarını duyurmuştur. Yeni proje, yeni nesil RTGS projesi(RTGS-XG) olarak adlandırılmaktadır. Proje iki ana değişiklik içermektedir. Bu ana değişikliklerden ilki, BOJ_NET ödeme sistemine likidite tasarrufu özelliklerinin eklenmesi, ikincisi ise özel sektör tarafından işletilen iki gecikmeli mutabakat ödeme sisteminin yeni RTGS sistem ile bütünleştirilmesidir.

4.4 SIC – İsviçre :

1987 yılında işlemlerine başlayan Swiss Interbank Clearing System (SIC) en eski RTGS sistemlerden biridir. Sistem üç temel prensibe dayanmaktadır : gün içi krediye izin verilmemektedir, kuyruklama mekanizması kullanılmaktadır, ödeme işleme ve mutabakatında FIFO (first in, first out: ilk giren ilk çıkar) yaklaşımı benimsenmektedir. 1990'larda FIFO kuralı bankaların ödemelerini önceliklendirmelerine imkan tanınarak gevşetilmiştir.

1999 yılında İsviçre merkez bankasının katılımcılarına faizsiz günüçi likidite sağlaması ile gün içi kredi de sağlanır olmuştur. CLS ödemelerine verilen özel önem nedeni ile zaman kritik ödemelerin artması gün içi kredi sağlanmasını sağlamıştır.⁶

SIC hesap sistemi özel bir yapıdadır. Katılımcıların iki hesabı bulunmaktadır. Biri ana hesap hesap diğeri ise SIC hesabıdır. Fonları SIC hesabına yansıtmak

⁶ CLS : Continuous Linked Settlement ilerleyen bölümlerde detaylıca açıklanacaktır.

mutabakat döngüsünü başlatır. Katılımcı hesapları arasında özgürce aktarım yapabilmektedir. Gün sonunda SIC hesaplarındaki bakiyeler ana hesaplara aktarılmaktadır.

SIC sistemine bir ödeme emri valör tarihinden beş gün öncesine kadar girilebilmektedir. Mutabakat 22-saat döngüsü boyunca gerçekleştirilmektedir. Ödemeler sistem tarafından çalıştırıldığında kesin ve geri dönülmez şekilde işlenir. Hesaplarda yeterince bakiye bulunmadığında ödeme otomatik olarak beklemeye alınır. Kuyruklarda bekleyen mesajların mutabakatı otomatik olarak yapılmaktadır. Aynı zamanda kuyruklarda bekleyen mesajları iptal etmek de olanaklı kılınmıştır. Kuyruklamaya ek olarak iki yönlü ofsetleme fonksiyonu sistemde yer almaktadır. Gönderenin bakiyesinin yetmediği durumlarda sistem alıcının kuyruğunun başında göndericiye gönderdiği ofsetleme yapabileceği mesaj olup olmadığına bakar.

SIC sisteminde gittikçe artan bir fiyatlandırma mekanizması bulunmaktadır. Bu yöntem kilitlenme sorunlarını ortadan kaldırmak için uygulanmaktadır. Alınan ücretler gün ilerledikçe artmaktadır. Burada hedef katılımcıların ödemelerini olabildiğince erken göndermelerini sağlamaktır. Ayrıca küçük ve büyük ödemeler için de farklı fiyatlandırmalar söz konusudur (Iivarinen, 2004:34-35).

4.5 PNS - Fransa

Paris Net Settlement (PNS) sistemi büyük meblağlı Fransız RTGS sistemi TBF ile çalışan bir ödeme sistemidir. 10 banka tarafından oluşturulan CRI (Centrale des règlements interbancaires) sistemin sahibidir. PNS müşteri ve bankalar arası kredi

ödemelerini gerçekleştirir. TBF sisteminden ve TBF sistemine likidite transferlerini de sıklıkla gerçekleştirir. Günbaşında bankaların TBF hesaplarından PNS sistemindeki hesaplarına likidite aktarımı yapması gerekmektedir. PNS sisteminde ödemeler için her hangi bir alt ya da üst sınır bulunmamaktadır.

PNS netleştirme mekanizmalarını ödemelerin gerçek zamanlı mutabakatının sağlanması ile bir arada tuttuğu için bir karma sistem olarak tanımlanabilir. Ödemeler birer birer süreklilik esası ile işlem görmektedir. Mutabakat kriterlerini sağlayan her ödemenin anında mutabakatı sağlanmaktadır. Diğerleri ise mutabakat uygunluğu için sürekli taranan kuyruklara aktarılmaktadır.

Sistemin ana risk kontrol mekanizması sistemin merkez bankası parası üzerinden geri dönüşü olmayan mutabakat sağlamasıdır. Kullanıcılar kredi ve likidite risklerini azaltacak olanaklara sahiptir. Her banka diğerlerine , onlardan ödeme almadan önce yapacağı en fazla ödemeyi belirleyebilir. Ayrıca iki yönlü limitlerin belirlenmesi de söz konusudur.

2003 yılında 30,000 işlem 70-80 milyar avro hacim ile PNS sisteminden geçmiştir (Iivarinen, 2004:39-40).

4.6 SPI /SBLE – İspanya

SPI İspanya’da İspanyol RTGS sistemi SLBE ile yan yana çalışmaktadır. (SBLE ispanya merkez bankasının sahibi olduğu RTGS ödeme sistemidir. İspanya’nın TARGET ile bağlantısı SBLE ile gerçekleşmektedir.) Katılımcılar sistemin sahibidir.

SPI’da mutabakat gören ödeme türleri diğer ulusal büyük meblağlı ödeme türlerinden farklılık göstermektedir. Ödemelerin çoğuna sınır ötesi ödemeler gözü ile bakılabilir.

SPI sisteminde ödemelerin mutabakatı sağlanır ve katılımcıların net pozisyonları gün boyunca sürekli hesaplanır. Eğer bir ödeme kuyruğa aktarılmışsa iki taraflı ya da çok taraflı optimizasyon prosedürleri mutabakatın sağlanması için uygulanabilir. Mutabakat gün sonunda eksi “short” ya da artı “long” pozisyonlar hesaplanıp mutabık kalındıktan sonra gerçekleşir.

İki değişik limit, kredi ve likidite risklerini engellemek için kullanılmaktadır : iki yönlü kredi limiti ve çok yönlü borç limiti. İki yönlü kredi limiti bir katılımcının başka bir katılımcıdan kabul edebileceği en büyük kredi pozisyonunu belirlemektedir. Çok yönlü limit ise bir katılımcının sahip olabileceği toplam borç pozisyonunu belirtir (Iivarinen, 2004:40-41).

4.7 POPS/Bof-RTGS – Finlandiya

POPS Fin bankalar arası sistemidir. Katılımcı bankalar sistemin sahibi ve işleticisidirler. Katılımcı bankalar POPS sisteminde mesajları iki yönlü olarak merkezi bir yapı olmadan gönderip almaktadırlar.

POPS, gerçek zamanlı, verinin iki yönlü değiş tokuşuna olanak tanıyan merkezi olmayan bir fon transfer sistemidir. Katılımcı bankalar ödeme talimatlarını doğrudan birbirlerine göndermektedirler. Ödemelerin mutabakatı Fin RTGS sisteminde (BoF-RTGS) gönderilen ödemenin miktarına göre gross ya da netleştirme esasına göre

gerçekleşmektedir. (BoF-RTGS sistemi Finlandıyanın TARGET sistemine bağlantısını gerçekleştirmektedir.) İki yönlü gönderilen ödemelere göre gün içinde iki yönlü borç ve alacak pozisyonları sürekli günlenmektedir. İki yönlü anlaşılan limite ulaşıldığında, netleştirme yükümlülüklerini zorlayan ödeme BoF-RTGS sisteminde gerçekleştirilir. Geri kalan iki yönlü yükümlülükler günsonunda netleştirilir. İki yönlü limitlerle her banka diğer katılımcılar karşısındaki net pozisyonlarını kontrol edebilir. İki çeşit limit kullanılmaktadır : RTGS limiti ve kredi limiti. RTGS limiti iki yönlü kredi limitinin yarısıdır. Limitler bankalar arası ikili görüşmelerle belirlenmektedir. RTGS limiti netleştirme esasına göre mutabakatı sağlanan (RTGS limitinden büyük ödemelerin “gross” esasına göre mutabakatı sağlanmaktadır) tekil ödemelerin en fazla büyüklüğünü belirlemektedir. Aynı zamanda RTGS limiti iki yönlü net bakiyelerin gün boyunca mutabakatı tetikleyecek sinyal işlevini de görmektedir. İki yönlü kredi tutarı RTGS limitini aştığında günüçi mutabakat yordamı devreye girmektedir. Borçlu taraf mutabakat işlemini RTGS sistemine gönderir. Günüçi mutabakat işlemleri her zaman RTGS limitlerine karşılık gelen aynı boyuttur. Kredi limiti iki yönlü net bakiyenin aşamayacağı tutarı belirlemektedir. Eğer kredi limitine ulaşırsa, risk alan banka net bakiyeyi arttıran işlemleri kabul etmeyecektir.

1. günüçinde iki yönlü net pozisyon RTGS limitini aştığında
2. günüçinde tekil ödemeler RTGS limitini aştığında
3. günsonunda iki yönlü bakiyeler sıfırlandığında

POPS ödemelerinin mutabakatı RTGS sisteminde gerçekleşmektedir.

Pratikte gün içi iki yönlü net kredi pozisyonları sıfır ila RTGS limiti arasında değişkenlik göstermektedir. Her hangi bir banka tarafından alınan toplam en fazla kredi riski kabul edilen iki yönlü limitlerin toplamı kadardır. Sürekli netleştirme esasına göre oldukça düşük bir risk sözkonusudur. Bunun sebebi ise iki yönlü pozisyonların gün içinde borç tarafından alacak tarafına sürekli olarak değişmesidir (Iivarinen, 2004:41-42).

4.8 CHAPS – İngiltere

CHAPS 1984 yılında elektronik bankalararası sistem olarak, kesin, garanti ve koşulsuz sterlin kredi transferlerini gerçekleştirmek amacı ile kurulmuştur. Kesin mutabakatın gün sonunda çoklu netleştirmeye dayandığı bir sistem olarak hayata geçmiştir. 1996 nisanında RTGS bir sistem olarak tasarlanmış yeni hali devreye girmiştir. Ve bankalararası yaklaşık tüm büyük meblağlı sterlin ödemeleri CHAPS üzerinden gerçekleşmektedir. 1999 yılında Avro ödemelerini sağlayacak ikinci CHAPS sistemi çalışmaya başlamıştır. CHAPS-Euro TARGET sistemine bağlı olarak çalışmaktadır. Toplam 20 banka CHAPS Euro'nun katılımcıdır. Bu bankalardan 12 tanesi (İngiltere Merkez Bankası da dahil olmak üzere) aynı zamanda CHAPS Sterling'in de katılımcıdır.

2001 Ağustos ayında gelişmiş NewCHAPS olarak isimlendirilen RTGS servislerinin tanıtılması ile CHAPS Sterling ve CHAPS Euro ortak bir teknik platform üzerinde çalışmaya başlamıştır.

İki CHAPS sistemi de yüksek hacimli ödemeler için tasarlanmış olmasına rağmen, sistemde geçebilecek ödemeler için her hangi bir alt ya da üst sınır bulunmamaktadır (BIS, 2003:407-408).

Tablo-2 ile açıklanan ödeme sistemleri karşılaştırılmıştır.

Tablo 2 – AB Ülkeleri Ödeme Sistemlerinin ve Türkiye Ödeme Sistemi EFT Sisteminin Karşılaştırılması

<i>Sistem</i>	<i>CHAPS Euro</i>	<i>RTGSPlus</i>	<i>Fedwire</i>	<i>BoJ-Net</i>	<i>PNS</i>	<i>SPI</i>	<i>POPS</i>	<i>SIC</i>	<i>EFT</i>
Ülke	İngiltere	Almanya	Amerika	Japonya	Fransa	İspanya	Finlandiya	İsviçre	EMKT
Katılımcı Sayısı	19	127	7134	363	496	157	10	306	49
Türü	RTGS	Karma	RTGS	RTGS	Karma	RTGS	RTGS	RTGS	RTGS
İşlemler için Kapanış ssatı	17:00	18:00	18:30	19:00	16:00	*	*	16:15	17:30
Sahibi	B+MB	MB	MB	MB	MB+B	MB	MB	MB+B	MB
TARGET Bağlantısı	Var	Var	Yok	Yok	Yok	Yok	Yok	Yok	Yok
Yıllık İşlem hacmi (milyar)	40,820 milyar dolar	156,996 milyar dolar	469,899 milyar dolar	188,800 milyar dolar	21,718 milyar dolar	217,70 milyar avro	459,91 milyar avro	33,762 milyar dolar	3,99 trilyon dolar

- İle gösterilen alanlara ilişkin veri derlenememiştir.

Kaynak : BIS,2006 :sayfa 47 , ECB,2006 ve TCMB internet sitesinden derlenmiştir.

4.9 SWIFT - Society for Worldwide Interbank Financial Telecommunication

1970'lerin ortalarından itibaren uluslararası finansal iletişimde ortak bir dil oluşturmak üzere kurulan SWIFT, üye bankaları ve aracılığı ile üyelerin kendi ve müşterilerinin ihtiyaçlarını karşılamaya yönelik olarak tüm finansal piyasalar arasında mesaj alış verişi ve arayüz yazılımı ile hizmeti sağlayıcısıdır. Sistem dünya genelinde sürekli olarak hizmet vermektedir (Kuzu, 2003: 67).

SWIFT finansal endüstri tarafından sahiplenilmiş, güvenli ve standart mesajlaşmayı sağlayan bir kooperatiftir. 7800 finansal kuruluş ve 200 ülkede kullanılmaktadır. Türkiye'de bankalar 1986 yılından itibaren SWIFT sistemini kullanmaya başlamışlardır. SWIFT sisteminde mutabakat bir ödeme sistemi veya muhabir bankacılık ilişkileri kanalıyla sağlanmaktadır (Kuzu, 2003: 68).

SWIFT dünya çapında bir standart olmuştur. SWIFT web sayfasından alınan bilgiye göre günde ortalama 10,041,009 adet mesaj sistemden geçmektedir. Bu rakam SWIFT'in bir standart oluşunun en bariz göstergesidir.

Ödeme ağları farklı ağ topolojileri kullanılarak kurulabilir. En yaygın olanı merkezileşmiş yıldız tipi (centralized star-type) ve iki taraflı (bilateral) ağ yapılarıdır. Yıldız ödeme ağı tipinde merkezde merkez sistem bulunmakta ve her katılımcı tüm işlemlerini merkeze göndermekte, merkezden almaktadır. İki taraflı ağda ise her katılımcı diğer katılımcılarla bağlantılıdır. İki yapının da avantajları ve dezavantajları vardır. Merkezileşmiş yapı daha elverişli iken her zaman iki iletişim

ayağının olması, ve merkez sistemin tıkanıklık, maliyet ve risk kaynağı olması açısından sıkıntı yaratır. İki taraflı ağda iletişim etkinken, pek çok sayıda bağlantının olması bilhassa ortak standartların olmadığı durumlarda sıkıntı oluşturmaktadır.

Modern ağ teknolojileri bu iki yapının karışımının oluşturulmasına olanak sağlamaktadır. Basit işlemler iki taraflı ağda gerçekleştirilirken, sistem merkezileştirilmiş fonksiyonlarla kontrol edilmekte ve desteklenmektedir. Geleneksel SWIFT altyapısı karma ağ yapısı için ilk adım olarak görülebilir. SWIFT standartları ve adresleme araçları (bank identifier code – BIC) ile merkezileşmiş yıldız yapısı üzerine iki taraflı ağı kurar, sakla ve yönlendir (store and forward) süreci ile merkezi sistemde bilgilerin tutulmasını da sağlar (Leinonen,2000:22).

4.10 TARGET

Avrupa para birliği kapsamında, tek para birimi “euro” ya geçiş sürecinin üçüncü aşaması olan “euro” kullanımına 1999 tarihinde başlanması planlanmıştır. Bu kapsamda tek para birimi kullanımı ve ülkeler arası ödemelerin verimliliğini arttırmak amacıyla, ödeme sistemlerinde yeni düzenlemelere ihtiyaç duyulmuştur. Merkez Bankaları Avrupa Sistemi (ESCB: European system of Central Banks) bu düzenlemelerin, Avrupa Para Birliği’nin (EMU: European Monetary Union) üçüncü aşamasında uygulamaya alınmasını talep etmiştir.

Mayıs 1995 tarihinde, Avrupa Para Kurumu (EMI:European Monetary Institute), gerçek zamanlı ulusal mutabakat sistemleri arasında bağlantıyı sağlayacak yeni bir

sistemin kurulmasına yönelik ilk raporunu hazırlamıştır. Bu sistem TARGET (Trans-European Automated Real-Time Gross Settlement Express Transfer) olarak adlandırılmıştır. Bu raporda, ödemelere ilişkin olarak EMU'nun üçüncü aşaması için gerekli düzenlemelerin tanımı yapılmıştır.

Temmuz 1996 tarihinde, sistemin detay spesifikasyonları tamamlanmış, birinci raporda tanımlanan düzenlemeler daha detaylandırılmış, ayrıca ulusal RTGS sistemlerinde bulunması gereken ortak özellikler, bu sistemlerle Avrupa Merkez Bankası arasındaki transferleri sağlayacak olan "interlink" sisteminin teknik özellikleri gibi konuları içeren teknik detaylar belirlenmiş ve "First Progress Report on the TARGET Project" ile "Technical Annexes to First Progress Report on the TARGET Project" adlarıyla iki ayrı rapor hazırlanmıştır (Uzdil,1997:1).

TARGET Avrupa Birliği merkez bankalarının aralarındaki ödemeleri gerçekleştiren RTGS bir sistemdir. 16 ulusal ödeme sisteminin ve Avrupa Merkez Bankasının ödeme mekanizmasının tek bir sistem oluşturmak üzere birbiri ile bir ağ üzerinde bağlanması ile oluşmuştur. TARGET sisteminde 2004 verilerine göre 50,800 kredi kuruluşu birbirine Avro bazlı ödemeler yapmaktadır. 4 Ocak 1999 tarihinden bu yana hizmet vermekte olan TARGET bankalar arası ödemeler ve müşteri ödemelerini gerçekleştirmektedir. Avrupa Merkez Bankası işlemleri dışında merkezi olmayan bir yapıda yani *decentralized* olarak tanımlanmış olan TARGET sisteminin günbaşı ve günsonu işlemleri Avrupa Merkez Bankası tarafından gerçekleştirilmektedir (ECB,2005).

TARGET sisteminin kurulmasının amaçlarını Avrupa Merkez Bankası şu şekilde sıralamaktadır (ECB,2005:5):

- Avro ödemelerinin RTGS tabanlı mutabakatının güvenli bir biçimde sağlanması
- Avro alanında, üye ülkelerin ödemelerinin etkinliğini arttırmak, ve en önemli amaç
- Avrupa Merkez Bankasının para politikasının gereksinimlerini sağlamaktır.

Tam otomasyon için TARGET, SWIFT standartlarını kullanmaktadır. TARGET sistemini Avrupa Birliği'ne üye ülkeler kullanabilmektedir.

Avrupa Merkez Bankası verilerine göre TARGET sistemine üye ülkeler ve ulusal ödeme sistemleri alfabetik olarak şu şekilde sıralanmaktadır (ECB,2005):

- Almanya (RTGSplus),
- Avusturya (Artis) ,
- Belçika (ELLIPS),
- Danimarka (KRONOS) ,
- Finlandiya (BoF-RTGS),
- Fransa (TBF),
- Hollanda (TOP),
- İngiltere (CHAPS),

- İrlanda (IRIS),
- İspanya (SLBE),
- İsviçre (ERIX),
- İtalya (NewBIREL),
- Lüksemburg (LIPS_Gross),
- Polonya (SORBN ET_EURO),
- Portekiz (SPGT),
- Yunanistan (Hermes)

Avrupa para birliğine üye 12 ülke (Almanya, Fransa, Belçika, Hollanda, Lüksemburg, İrlanda, İspanya, Portekiz, İtalya, Yunanistan, Finlandiya ve Avusturya) ve üye olmayan Danimarka, İsviçre, İngiltere ve Polonya'da bankalararası (MT202) ve müşteri ödemeleri (MT103) için TARGET kullanılmaktadır.⁷ TARGET gönderilecek tutar miktarı için alt ya da üst sınır koymamaktadır (ECB,005:6). Para Birliği'ne üye olmayan ülkeler TARGET üzerinden sadece avro ödemelerini yapabilmektedir.

Çeşitli ulusal RTGS sistemleri ulusal kullanım amacıyla geliştirilmiştir. Uluslararası TARGET ödemeleri ulusal RTGS sistemlerince gerçekleştirilmektedir. Bu sistemler alıcı RTGS sistemlerine ödemeleri doğrudan göndermektedir. Birbirinden farklı RTGS sistemlerinin iletişim kurmasını bağlantı modülleri sağlamaktadır. Farklı RTGS sistemlerinin işletim zamanı, uluslararası ödemelerin fiyatlandırılması ve gün

⁷ MT202 ve MT103 SWIFT mesaj türleridir. MT202 bankalararası ödemeler MT103 ise müşteri ödemeleri için tanımlanmıştır.

içi kredi provizyonu özellikleri harmanlanmıştır diğer özellikler aslını korumuştur (Iivarinen, 2004:18-19).

Tablo 3 - TARGET üyesi ülkelerde ulusal ve uluslararası ödemeler (Tutar Bazında)

Ülke Adı	Ulusal Ödemelerin Tutarı (Milyon AVRO)	Uluslararası Ödemelerin Tutarı (Milyon AVRO)	Toplam Ödemelerin Tutarı (Milyon AVRO)	Uluslararası Ödemeler/ Toplam Ödemeler
Belçika	3331	10227	13558	75.4
Lüksemburg	1513	3242	4755	68.2
Portekiz	1280	1975	3255	60.7
Hollanda	9494	11871	21365	55.6
Avusturya	2374	2803	5177	54.1
Yunanistan	1724	1620	3343	48.4
Finlandiya	2142	1503	3645	41.2
İrlanda	3360	2142	5502	38.9
İtalya	16303	8458	24761	34.2
Almanya	92711	35833	128544	27.9
Fransa	77081	19246	96327	20.0
İspanya	65081	5128	70208	7.3
İngiltere	7362	23818	31180	76.4
İsviçre	73	18241	897	96.1
Danimarka	42	3166	3208	98.7

Kaynak : Iivarinen, 2004

Tablo-3’de Belçika, Lüksemburg ve Portekiz’de sınır ötesi ödemelerin yüksek olduğu görülmektedir. İspanya da ise durum tam tersi gözükmemektedir, ulusal ödemeler RTGS sistemin ana yapısını oluşturmaktadır. Para Birliği üyesi olmayan İngiltere, İsviçre ve Danimarka’daki değerlerin yüksekliği Para Birliği üyesi olan Belçika, Lüksemburg ve Portekiz ile kıyaslanmamalıdır. Çünkü ilk gruptaki ulusal ödemeler ayrı RTGS sistemlerde gerçekleşmektedir (Iivarinen, 2004:26).

TARGET'ın başarılarının yanında heterojen sistem tasarımı kaynaklı sıkıntıları da bulunmaktadır. Avrupa Birliği'nin gelişmesi gibi ortamdaki değişiklikler nedeniyle Eurosystem (avro alanının merkez bankası sistemi) yeni nesil TARGET sistemini geliştirmektedir. Yeni nesil TARGET2 olarak adlandırılmaktadır. Yeni sistemin 2007 yılının ikinci yarısında devreye alınması planlanmaktadır. Yeni nesil genel bir teknik platform üzerinde daha fazla güvenlik seviyeleri ve etkinlik sağlamayı planlamaktadır. Mevcut sistemin yeteneklerinin artırılarak sürdürülmesi sistemin hedefleri arasında bulunmaktadır (The Eurosystem, 2005).

4.11 CLS Continuous Linked Settlement

Dünya FX piyasasında uygulanan klasik mutabakat yöntemlerinin global sistemin sağlamlığını tehdit edebilecek sistemik bir risk oluşturduğu, aralarında merkez bankalarının da bulunduğu çeşitli kuruluşlar tarafından uzunca bir süredir dile getirilerek bu riskin ortadan kaldırılması, FX işlemlerinin daha hızlı, güvenli ve daha az likiditeye ihtiyaç duyacak şekilde gerçekleştirilebilmesi için bir çalışma başlatılmıştır.

Gerçekleştirilen çalışmalar sonucunda önde gelen, 7 merkez bankasının (ABD, Avrupa, Japonya, İngiltere, İsviçre, Kanada ve Avusturya) RTGS ödeme sistemlerini birbirine bağlayan Continuous Linked Settlement (CLS) sistemi 9 Eylül 2002 tarihinde işleme geçmiş bulunmaktadır.

CLS, yaklaşık 300 yıldan bu yana aynı yöntemle yapılmakta olan ve bir dereceye kadar karşılıklı güvene dayalı sınır ötesi FX ödemelerine radikal bir değişiklik getirmiştir.

CLS, mevcut ödeme sistemlerini kullanarak yapılan FX işlemlerinin mutabakatında söz konusu olan mutabakat riskinin ve bağlantılı risklerin (operasyonel risk, sistemik risk) bertaraf edilmesi ya da azaltılması amacıyla özel bankaların girişimleri ve G10 merkez bankalarının önerileri ile kurulan yeni bir küresel mutabakat sistemidir.

CLS işlemlerini gerçekleştirmek için özel amaçlı bir banka olan CLS Bank kurulmuştur. Bankalar CLS sistemine hissedar olarak doğrudan ya da dolaylı üye olabilmektedirler. Sadece mutabakat üyeleri CLS Bank'ta hesap bulundurabilmekte ve bu banka nezdindeki çoklu hesapları aracılığı ile mutabakatı yapılacak işlemlerden oluşacak net bakiyeyi CLS Bank'a ödemektedirler (TCMB, 2003: 3) .

Geleneksel olarak bir FX'e ilişkin iki ödeme ayrı olarak işlem görmektedir. İki katılımcıdan birinin ödediği parayı alamayabilir. Bu durum mutabakat riski olarak adlandırılmaktadır (Iivarinen, 2004:44). CLS sisteminde kullanılan döviz türleri için bu risk ortadan kalkmaktadır.

Mutabakat bildirimleri CLS Banka 6:30'a (CET) kadar bildirilmektedir. Her katılımcıya döviz türü için çok yönlü olarak net pozisyonlar CLS Bank tarafından hesaplanmaktadır. Yapılacak ödemeler ulusal RTGS sistemlerince CLS bankın hesabına aktarılmaktadır(Iivarinen, 2004).

CLS'in řu anda 691 katılımcısı bulunmaktadır ve gnlk iřlem hacmi ortalama 2 trilyon Amerikan dolarına ulařmıřtır.

CLS'in kazandırdıkları:

- ❖ Sınır tesi FX iřlemlerini daha gvenli hızlı ve etkin, iřlemlerin bařarısızlık ihtimalini ortadan kaldırarak gerekleřtirir.
- ❖ Karřılıklı deme talimatlarındaki riski mutabakatın aynı gn gerekleřmesi ile ortadan kaldırır.
- ❖ Hangi iřlemlerin mutabakatının saęlandıęını gerek zamanlı olarak sunarak yelerinin daha iyi likidite ynetimi yapmasını saęlar.
- ❖ Hergn gerekleřtirilen mutabakat iřlemlerinin %7 sini CLS kapsamaktadır. Bu rakamlar CLS'in daha fazla iřletimsel etkililięe liderlik edeceęinin gstergesidir.
- ❖ Azaltılan kredi riski ile CLS yesi bankalar aracılıęıyla tarafların iřlem hacimlerini bytmesi sz konusudur.
- ❖ Tam otomasyon saęlanmış srelerin tm yararlarına sahip olunmaktadır.

- ❖ Mutabakat üyesi kurumların kredi yönetimini ve likidite konsolidasyonunu arttırır.
- ❖ Fonların uygunluğunu ve akışını geliştirir.
- ❖ Bankaların iş sistemlerinin CLS ile bütünleşmesine olanak verir.
- ❖ CLS sisteminde eşleşen net pozisyonlar söz konusu olduğundan yapılan binlerce işleme karşılık gönderilecek sınırlı sayıda ödeme emrinin bankaların işlem maliyetlerini önemli ölçüde azaltacağı öngörülmektedir.
- ❖ CLS sisteminde işlemlerin mutabakatının yapılması nedeniyle sadece net pozisyonlar fonlandığı için bankaların gün içi likidite ihtiyaçlarında azalma olması beklenmektedir.

CLS’de kullanılan para birimleri şu şekilde sıralanabilir :

- Kanada Doları,
- Danimarka Kronu,
- Avro,
- İngiliz Sterlini ,
- Hong Kong Doları,
- Japon Yeni,

- Kore Wonu,
- Yeni Zelanda Doları,
- Norveç Kronu,
- Singapur Doları,
- Güney Afrika Randı,
- İsveç Kronu,
- İsviçre Frankı ,
- Amerikan Doları

BEŞİNCİ BÖLÜM

5 ÖDEME SİSTEMLERİNDE RİSK

Ödeme sistemleri finansal yapının önemli bir parçasıdır. Piyasa ekonomilerinde her bir işlem bir ödeme içerir. Ödeme sistemlerinde dönen meblağların büyüklüğü ve ödeme sistemlerinin ekonomilerdeki etkileri göz önünde bulundurulduğunda ödeme sistemlerinin teknik olarak güvenilir ve güvenli olmaları gerekmektedir. Risklerin tanımlanması ve önlenmesine yönelik çalışmalar yapılması ödeme sistemlerine güven duyulmasını sağlamak ve sürdürmek açısından önem arz etmektedir.

5.1 Risk grupları

Ödeme sistemlerinde oluşabilecek riskler BIS tarafından 2001 yılında şu şekilde sınıflandırılmıştır:

5.1.1 Kredi Riski

Katılımcılardan herhangi birinin sistem içerisindeki finansal yükümlülüklerini hiçbir zaman karşılayamadığı zaman oluşacak risktir.

Kredi riski ikiye ayrılmaktadır. Piyasa riski (“*market risk*”), yapılan bir işlemde karşı tarafın yükümlülüklerini yerine getirememesi ve arada geçen süre içinde işleme konu kıymetin fiyatında meydana gelebilecek aleyhte değişimler nedeniyle ortaya çıkan

risktir. Örneğin; yapılan bir döviz işleminde karşı tarafın taahhüt ettiği döviz gönderememesi ve bu arada dövizin fiyatının yükselmesi sonucunda piyasa riski ortaya çıkmaktadır. Piyasa riski, yerine koyma riski (*“replacement cost risk”*) olarak da adlandırılmaktadır.

Anapara riski (*“principal risk”*) olarak da adlandırılan ikinci tür kredi riskinde yapılan yatırımın tümünü kaybetme olasılığı vardır. Örneğin; gerçekleştirilen bir döviz işleminde karşı tarafa taahhüt edilen fonların gönderilmesi, buna karşılık karşı tarafın taahhüt ettiği döviz gönderememesi durumunda söz konusu risk ortaya çıkmaktadır (Ergin, 2001:31-32).

5.1.2 Likidite Riski

Katılımcılardan herhangi birinin sistem içerisindeki finansal yükümlülüklerini beklendiği zamanda karşılayamaması fakat ileriki bir zamanda karşılayabilecek olması durumunda oluşan risktir. Ödeme sistemlerinin sınıflandırılması başlığında bahsi geçen T yapıdaki ödeme sistemleri kredi ve likidite risklerine mutabakat bilgisinden önce ödeme bilgisi alıcı bankaya ulaştığından dolayı açıktır.

5.1.3 Yasal Risk

Zayıf hukuki çerçeve ya da hukuki belirsizlik durumları kredi ya da likidite riskine yol açabilir.

5.1.4 Operasyonel Risk

Operasyonel sebeplerle kredi ya da likidite riskleri oluşabilmektedir. Operasyonel risk ödeme sistemlerinin bilgi sistemlerinde, işletim ve yönetiminde yapılan hatalarla oluşabilecek bir risk türüdür.

Bu risk modern ödeme sistemlerinin omurgası olan bilişim teknolojileri ile yakından ilgilidir. Ödeme sistemlerinin teknik karmaşıklığı arttıkça sistemlerin kırılganlığı da artmaktadır. Ayrıca kriminal riskler de operasyonel risk çerçevesinde değerlendirilmelidir. Sistemlerin zayıf noktalarını öğrenen suçlular bu noktaları kolaylıkla kırabilmektedir (Iivarinen, 2004:14).

Günümüzde finansal sistemler ve ödeme sistemleri sürekli bir değişim içerisinde bulunmaktadır. Değişen koşullara denetim ve düzenleme fonksiyonları hızla uyumu sağlanmak zorundadır. Hızlı değişim ve uyum sağlama çalışmaları ise başlı başına risk oluşturmaktadır (Khiaonarong,2003:14).

Normlar ve standartların belirlenmesi, olağandışı durum planlarının hazırlanması , ve teknolojik yeniliklerin sistemlere aktarılması ile ödeme sistemlerinin güvenilirlikleri arttırılabilir (Johnson vd., 1998 :2).

5.1.5 Sistematik Risk

Sistemdeki katılımcılardan birinin yükümlülüklerini yerine getirememesi ya da sistemin kendisinde oluşabilecek bir sorun nedeniyle diğer katılımcıların da yükümlülüklerini yerine getirememesi durumudur. Diğer bir deyişle, bir katılımcının yükümlülüğünü yerine getirememesinin, ödeme sisteminin işleyişini etkileyecek şekilde yaygınlaşmasıdır.

Ödeme sisteminin herhangi bir katılımcısının maruz kaldığı kredi, likidite ya da operasyonel risklerin ödeme sisteminin genelinde ve hatta finansal sistemin bütününe yayılması şu şekilde gerçekleşmektedir. Ödeme sistemi katılımcılarından birinin yükümlülüklerini yerine getirmekte zorlanmasının, sistemdeki diğer katılımcılar tarafından fark edilmesi ile birlikte diğer katılımcılar kendilerini güvence altına almak amacı ile pozisyonlarını sağlamlaştırmaya çalışacaklardır. Sorun yaşanan katılımcıdaki fonlarını çekmeye ve söz konusu katılımcıdan para gelmeden onun adına transfer işlemi yapma taleplerini reddetmeye başlayacaklardır. Likidite sıkıntısı daha da artan katılımcı, likidite bulmak için elinde bulunan varlıklarını zararına satmaya başlayacak, bu durum finansal pozisyonunun daha da kötüleşmesine yol açacaktır. Diğer katılımcılar, sorun yaşayan katılımcının yükümlülüklerini yerine getirememesinden dolayı likidite sıkıntısı yaşayacak ve ellerinde bulunan varlıkların değerinde azalmalarla karşı karşıya kalacaklardır. Piyasada oluşan belirsizlik tarafların birbirlerine tanıdıkları kredi oranlarının kısılmasına yol açacaktır. Sonuçta ödeme sistemindeki herhangi bir sorun ekonominin geneline yayılarak sistematik bir soruna dönüşecektir (Akan, 2004 : 56).

5.2 Risk Açısından RTGS ve DNS sistemler:

Katılımcı bir bankanın gönderimden sonra fakat mutabakattan önce darboğaza girmesi halinde alıcı banka beklediği fonları alamayacaktır. Bir katılımcıdan kaynaklı bu tarz sorunlar diğer katılımcıları da etkileyebilecektir (McAndrews ve Trundle, 2001:127). Mutabakatın anlık olarak yapılmadığı gecikmeli mutabakat sistemlerinde kredi riski söz konusudur.

Bankalar arası ödemelerin hacmi 1980'lerden 1990'lara geçişte hızlı finansal yenilikler ve finansal marketlerin globalleşmesi sebebiyle hızla artmıştır. Bu artışa paralel bilgi teknolojilerindeki gelişmeler gerçek zamanlı mutabakat sistemlerini önemli bir alternatif olarak sunmuştur.

RTGS sistemlerde gerçek zamanlı işlem yapılması nedeni ile kredi riski yoktur. Gecikmeli Mutabakat sistemlerden gerçek zamanlı sistemlere geçişle kredi riski likidite riskine kaymıştır (Manning ve Willison, 2006: 6). RTGS sistemlerin yoğun olarak bilgi teknolojilerini de kullanması, kredi riskinden likidite riski ile birlikte bilgi teknolojileri risklerine kaymayı da beraberinde getirmiştir.

Ödeme sistemlerinin tasarımı para politikalarının verimliliğini, ekonominin tümünün işleyişini etkilemektedir. Finansal sektör reformlarının programlarında ödeme sistemi reformları da yer tutmuştur. (Örneğin İtalya 1989/90; Malezya 1986/89 ve Tayland 1995) Geçiş sürecindeki tüm ekonomilerde ödemeleri hızlandırmak, nakit olmayan ödemelerdeki riski ve belirsizliği azaltmak, para politikasının dolaylı

enstrumanlarına adaptasyonunu sağlamak, riski azaltmak ve finansal piyasaların gelişimini çabuklaştırmak amacı ile ödeme sistemlerinde reformlar gündeme gelmektedir. Bu bağlamda Avrupa Para Birliği'nde tekil bir para politikasının oluşturulması sürecinde de TARGET anahtar rol oynamıştır. (Johnson vd.,1998 :1).

Ödeme sistemlerindeki riskleri değerlendirebilmek için risklerin oluşma koşullarını ve oluştuklarında verebilecekleri zararları tanımlamak gerekmektedir. Ödeme sistemlerindeki risklerin ölçümünde en genel sorun daha önce yaşanmış deneyimlerden sistematik veri toplanmamış olmasıdır (Khiaonarong, 2003:14).

5.3 Temel İlkeler

Sağlam ve etkin ödeme sistemleri finansal sistemin iyi çalışması açısından kritik önem taşımaktadır. Sistemik açıdan önemli ödeme sistemleri şokların ulusal ve uluslararası sistem ve marketlere taşınmasında önemli bir aktarım kanalı olabilmektedir. Sağlam sistemler finansal istikrarın sürdürülmesi ve arttırılması için anahtar bir gerekliliktir. Bu doğrultuda uluslararası standartları ve deneyimleri tasarım ve işletimlerinde kullanacak sağlam sistemlerin oluşturulması hususunda uluslararası düzeyde bir anlaşmaya varılmıştır (BIS, 2001 :1).

2001 Ocak Ayında 23 ülke, IMF ve Dünya Bankasının elemanlarından oluşan grup risklerin giderilmesi amacı ile (“Core Principles for Systemically Important Payment Systems (CPSIPS)“) sistemik açıdan önemli ödeme sistemleri için temel ilkeler raporunu yayınlamıştır. Temel ilkeler, sistemik açıdan önemli ödeme sistemlerinin

riskleri ortadan kaldırmak için uyması gereken 10 ilkeyi ve merkez bankalarının 4 sorumluluğunu belirlemektedir.

Bir ülkedeki tüm ödeme sistemlerinin temel ilkelere uyması şart değildir. Ancak mali sistem bakımından önemli olarak tanımlanan ödeme sistemlerinin temel ilkelere uyması, mali sistemin etkin çalışması açısından büyük önem taşımaktadır. Temel ilkeler, bu tür ödeme sistemlerinin tasarımcılarını, işleticilerini, gözetimcilerini doğrudan; katılımcılarını ise dolaylı olarak ilgilendirir.

Bir ülkede birden çok ödeme sistemi bulunabilir. Çalışmaması halinde

- Ulusal mali sistem çapında bir riske yol açabilen, ve
- Ülke ekonomisini anında etkileyen

ödeme sistemleri “mali sistem açısından önemli” olarak nitelendirilir .

5.3.1 Temel ilkelerin ana başlıkları:8

I. Sisteme ilişkin sağlam bir hukuksal altyapının bulunması :

Sistemin kuralları ve yordamları uygulatılabilir ve sonuçları tahmin edilebilir olmalıdır. Yasal olarak sağlam olmayan ya da yasal kavramları anlaşılır olmayan bir sistem risklere her zaman açıktır. Sınır ötesi elemanları

⁸ Ana başlıklar TCMB internet sayfasından <<http://www.tcmb.gov.tr>> 10 Mart 2006 tarihinde alınmış , açıklamalar ise “core principles for systemically important payment systems” BIS 2001 raporundan derlenmiştir.

barındıran ödeme sistemlerinde nerenin kanunlarının ne durumlarda nasıl tabi olunacağına açıklık getirilmelidir.

II. Sisteme ilişkin risklerin kurallar ve yordamlar aracılığıyla açıkça tanımlanması :

Katılımcılar, sistem operatörleri sistemdeki finansal riskleri ve nedenlerini açık bir biçimde anlamalıdır. Sistemin kural ve yordamları risklerin nerelerden doğduğunun en önemli saptayıcısı olacaktır. Sistem kuralları ve yasal ortamın diğer bileşenlerin ilişkisi net bir biçimde anlaşılmış ve açıklanmış olmalıdır.

III. Sistemdeki kredi ve likidite risklerinin etkin yönetilmesi :

Risklerin nereden doğduğunun tanımlanması sistemik açıdan önemli ödeme sistemleri için yeterli değildir. Aynı zamanda bu risklerin yönetimi ve bastırılması için sistem kural ve yordamları ile sorumlulukların atanmış olması da gerekmektedir. Analitik ve işletimle ilgili yordamlar risk yönetimi için söz konusu olabilir. Analitik yordamlar katılımcının sistemde ortaya çıkarabileceği kredi ve likidite riskinin sistemin sürekli izlenmesi ve analiz edilmesini içerir. İşletimle ilgili yordamlarsa, teminatlandırma anlaşmaları ile limitler konması, işlem kuyruklarının tasarım ve yönetimi gibi konuları kapsar. Pek çok sistem için risk yönetimi süreçlerinin gerçek zamanlı kullanımı, bu maddenin sağlanması için anahtar rol oynayacaktır.

IV. Mutabakatın ödeme gününde kesinleşmesi:

Ödemelerin sisteme kabulü ve kesin mutabakat işlemi arasında geçen sürede katılımcılar kredi ve likidite riskleri ile yüzleşebilirler. İlgili otoritelerin müflis kuruluşları kapatmaları iki iş günü arasında yaşandığı için mutabakat işleminin iş gününden sonraya kalması bu riski katlamaktadır. Kesin mutabakat valör gününün sonunda gerçekleştirilmiş olmalıdır.

V. Çok taraflı netleşmelerde mutabakatın gününde tamamlanması :

Çoğu çok taraflı netleştirme sistemi katılımcıların yükümlülüklerini ertelemektedir. Çoklu netleştirme sistemlerinde bir katılımcı mutabakat yükümlülüklerini yerine getiremediğinde diğer katılımcılar da likidite ve kredi riski ile karşı karşıya kalacaklardır. Sistem en büyük mutabakat yükümlülüğüne sahip katılımcının yükümlülüklerini gerçekleştiremediği durumda bile günlük mutabakatın zamanında yapılmasını sağlayacak yeterlilikte olmalıdır.

VI. Mutabakat parasının güvende olması:

Mutabakat için kullanılan varlıkların merkez bankası güvencesinde olması tercih edilmeli, diğer varlıkların kullanılması halinde kullanılan varlıklar az ya

da hiç kredi ve likidite riski taşınmalıdır. Mutabakat varlığı sistemdeki tüm katılımcılarca kabul edilmiş olmalıdır.

VII. İleri düzeyde güvenlik ve işlemler açısından güvenilirlik sağlanması:

Piyasa katılımcıları finansal piyasa işlemlerini ödeme sistemleri üzerinden gerçekleştirmektedirler. Bu işlemlerin doğruluk ve bütünlüğünü sağlamak için sistemlerin geçerli güvenlik standartlarını tahsis etmiş olması gerekmektedir. Sözü edilen standartların teknolojik gelişmelerle güncellenmesi gerekmektedir. Sistem aynı zamanda günlük işlemleri gerçekleştirmek için yüksek seviyede operasyonel esnekliğe sahip olmalıdır. Bu yeterli teknolojinin kullanılması, tüm donanım, yazılım ve ağ elemanlarının yedeklerinin alınmasından ibaret değildir. Sistemler aynı zamanda iş prosedürlerine, iş prosedürlerinin doğru uygulandığını denetleyebilecek ve sistemin doğru ve etkin çalışmasını sağlayacak çalışanlara sahip olmalıdır.

VIII. Sistemin pratik ve verimli olması:

İşletmenler, kullanıcılar ve sistemi gözetenlerin hepsinin sistemin etkin çalışması konusunda ilgileri vardır. Bu kişiler kaynakları israf etmek istememektedirler. Kaynakları etkin kullanırken güvenliği de en fazla oranda sağlamak istemektedirler. Bu ihtiyaçları karşılama doğrultusunda sistem tasarımı kaynak maliyetlerini sistemin özel durumlarında pratikliği ve tüm ekonomiye etkilerini gözетerek sağlamalıdır.

IX. Adil katılım hakkı sağlanması:

Katılımcıların arasındaki rekabeti sağlayacak katılım kriterleri sistemin daha etkin ve düşük maliyetli çalışmasını sağlayacaktır. Bu avantaj sistemi yasal, finansal ve işletimsel risklere sokacak katılımcıların sisteme dahil edilmesi olasılığı ile dengelenmelidir. Erişimle ilgili tüm sınırlamalar nesnel olmalı ve erişim kriterleri üzerine kurulmalıdır.

X. Sistem yönetiminin etkin ve saydam olması:

Ödeme sistemleri yönetim düzenlemeleri sistemin sahipleri ve katılımcıları arasındaki ilişkiyi çerçevelemektedir. Sistemik olarak önemli ödeme sistemlerinin daha geniş finansal ve ekonomik alanı etkileme güçleri olduğundan sistemler ister merkez bankaları ister özel sektör tarafından yönetilsin daha etkin, sorumlu ve şeffaf yönetime ihtiyaçları vardır.

5.3.2 Temel ilkeleri uygulamada merkez bankalarının görevi nedir?

Temel ilkelerin mali sistem bakımından önemli olan ödeme sistemlerine uygulanmasında merkez bankalarına düşen görevler şunlardır:

- A. Ödeme sistemlerinin hedeflerini belirlemek ve açıklamak
- B. İşlettikleri sistemlerin temel ilkelerle uyumluluğunu sağlamak
- C. İşletmedikleri sistemlerin de temel ilkelerle uyumluluğunu denetlemek

D. Diğer ilgili ulusal ve uluslararası yetkili taraflarla işbirliği yapmak ⁹

⁹ TCMB internet sitesinden <<http://www.tcmb.gov.tr>> ilgili maddeler 10 Nisan 2006 tarihinde alınmıştır.

ALTINCI BÖLÜM

6 Bilgi Teknolojileri Riskleri

Kullanıldıkça tükenmeyen bir kaynak olan bilgi, günümüzde mal ve hizmet üretim süreçlerinde önemli bir girdi haline gelmiştir. Bilginin öneminin artması ile birlikte, elde edilmesi ve üretim süreçlerinde kullanılacak hale dönüştürülmesi ihtiyacı doğmuştur. Bu ihtiyaca cevap vermek amacı ile süren çalışmalar, Bilgi Teknolojilerini (BT) geliştirmiştir. Bilgiyi toplama, işleme ve dağıtma görevini üstlenen teknolojiler, Bilgi Teknolojileri olarak adlandırılmaktadır.

Bilgi teknolojileri günümüzde, sosyal yaşamın ayrılmaz bir parçası olmuştur. Söz konusu teknolojilerin dünya genelinde uygulama alanı hızla artmaktadır, dolayısıyla bu gelişimin dışında kalma şansı bulunmamaktadır. Güvenilir bilgi teknolojileri, çok fazla birbirine bağlanmış sistem ve fonksiyonel bilgi teknolojileri işleyişine ihtiyaç duyulması nedeniyle, toplumlar ve ekonomiler için önem arzetmektedir .

Bilgi teknolojilerindeki hızlı gelişim ve bilgi teknolojileri portföyündeki ürünlerinin fiyatlarındaki hızlı düşüş (1996 1998 yılları arasında %8 lik bir düşüş gözlenmiştir) ekonomi üzerinde önemli bir etki yaratmıştır (Vlatko, 2000:1). İstatistiklere göre 1995’de \$1,963 BT maliyeti ile yapılabilen işler 2004’de \$1,000 BT maliyeti ile gerçekleştirilebilir olmuştur (Mark,2005:2). Fiyatlardaki hızlı düşüş bilgi teknolojilerinin iş süreçlerine dahil edilme oranını arttırmıştır.

Bilgi teknolojilerinin, dünya genelinde hızla artan uygulama alanlarından biri de ödeme sistemleridir. Bilgi teknolojilerindeki hızlı gelişme, ödeme sistemlerinde kağıt tabanlı sistemlerden elektronik ödeme sistemlerine geçişi sağlayarak yapısal değişikliklere neden olmuştur. Yaşanan geçiş pek çok değişimi ve yeni teknolojiyi de beraberinde getirmiştir. Bu geçiş sadece iş süreçlerinin elektronik ortama aktarılması şeklinde gerçekleşmiştir. Bir sonraki adım, yeniden mühendislik (re-engineering) çalışmalarıyla, elektronik süreçlerin yeniden tanımlanması şeklinde olacaktır. Bilgi teknolojilerinin sunduğu olanaklar, ödeme sistemlerinin etkinliğini ve verimliliğini arttırmaktadır. Bilgi teknolojilerinin katkıları göz önüne alındığında ve yeniden mühendislik çalışmaları kapsamında, ödeme sistemlerinin kendilerini teknolojik olarak yenilemeye devam edeceği görülmektedir.

Teknoloji geleneksel yapıda olmayan pek çok riski bünyesinde barındırmaktadır. Teknoloji riskleri yazılım, donanım, elektronik aletler, çevrimiçi ağlar ve telekomünikasyon sistemlerinin kullanımından ya da bu sistemlere olan güvenden oluşan zarar, kayıp, düzensizlik ya da hatalarla ilişkili risklerdir. Bu riskler aynı zamanda sistem göçmeleri, işleme hataları, yazılım kusurları, işletim yanlışları, donanım arızaları, kapasite yetersizlikleri, ağ kırılganlıkları, kontrol süreçlerindeki zayıflıklar, güvenlik eksiklikleri, kötü niyetli ataklar, saldırı (hacking) olayları, dolandırıcılık eylemleri ve yetersiz yeniden elde etme kapasiteleri ile birlikte de düşünülmelidir (The Central Bank of The Bahamas, 2006).

Ödeme sistemleri, bünyesinde ağırlıklı olarak bilgi teknolojileri risklerini barındırmaktadır. Bilgi teknolojileri kaynaklı oluşacak riskler sistemde tıkanmaya, bozulmaya ve hatta sistemin durmasına neden olabilmektedir. Oluşan sonuçlar, sonrasında likidite riskini ve sistemik riski doğurabilmektedir.

Çalışmanın daha önceki bölümlerinde ödeme sistemlerinin amaçları, globalleşen ve hacmi artan finans işlemleri ile birlikte kullanımlarının arttığı, mevcut sistemlerin yenilenmeye başlandığı, merkez bankalarının gündeminde ödeme sistemlerinin önemli yer tuttuğu ve ödeme sistemlerinin gözetimini üstlendikleri, ödeme sistemlerinin para politikası yürütülmesi ve finansal istikrarın sağlanmasına katkısı olduğu, ödeme sistemlerinde işlem gören parasal miktarların gaysi safi milli hasılların çok üzerinde olduğu bilgileri aktararak ödeme sistemlerinin önemi vurgulanmaya çalışılmıştır. Riskler başlığı altında ise ekonomideki önemleri nedeniyle teknik olarak güvenli ve güvenilir olmaları gerektiğine değinilerek ödeme sistemleri için söz konusu olan riskler gruplanmıştır.

Çalışmanın bu bölümünde, ilgili otoritelerce operasyonel riskler başlığı altında incelenen bilgi teknolojileri riskleri ve bu risklerin ödeme sistemleri ilişkisi irdelenecektir.

6.1 Bilgi Teknolojileri Riskleri Nelerdir

Günümüzde teknolojinin gelişimi için bilgi teknolojileri lokomotif rol üstlenmektedir. Bilgi teknolojilerindeki hızlı değişim, teknoloji geçişlerini bir tercih olmaktan çıkarıp zorunluluk haline getirmiş bulunmaktadır (Valerdi & Kohl:2004). Ödeme sistemleri ve bilgi teknolojileri arasındanki kuvvetli bağın bir zorunluluk olduğu dikkate alınarak, bilgi teknolojileri risklerini tanımlamak, riskleri ortadan kaldıracak çözümler aramak gerekmektedir.

Elektronik ödeme sistemlerinin, kağıt tabanlı ödeme sistemlerine oranla daha fazla kırılganlıkları bulunmaktadır. Elektronik ödeme sistemleri öncesinde müşteriler, işlemler süresince belirli bir uzaklıkta bulunmaktaydılar ve finansal kuruluşlar tüm süreçleri kontrol etmekteydiler ve korumaktaydılar. Kağıt tabanlı sistemlerde paranın akış hızının az olması da güvenlik açıklarının oluşmamasına katkı sağlamaktaydı. Elektronik ödeme sistemleri ile birlikte müşterilerin sistemle mesafelerinin ortadan kalkması ve fonların hızlı hareket etmesi güvenlik sorunlarını beraberinde getirmiştir. Bu açıkların yanında elektronik ödeme sistemlerinin elektronik bilgi işleme, bilgi saklama ve aktarma gibi bilgi teknolojilerine dayalı kırılgan noktalarının da bulunması risk içermektedir (United States. Congress. Office of Technology Assessment, 1982).

Ödeme sistemleri için bilgi teknolojileri risklerine göz attığımızda risklerin iki farklı niyetle oluşabileceğine görmekteyiz:

1. Bilinçli olarak, planlanarak yaratılmış aksaklıklara yol açmaya, para çalmaya, sistemi darboğaza sokmaya, firmanın itibarını zedelemeye yönelik yasadışı eylemler
2. Bilinçsiz olarak iş süreçlerinde aksaklıklar sonucunda oluşmuş sorunlar

Her ne şekilde olursa olsun, bilgi teknolojileri riskleri, ödeme sistemlerinin amaçlarının gerçekleşmemesine, etkinliğinin ve güvenilirliğinin zedelenmesine sebep olacaktır.

Mutabakat işleminin geçikmesi, bilgi teknolojileri nedeniyle oluşabilecek risklerin neden olabileceği sonuçlardan biridir. Mutabakat gecikmesinin hem gönderen hem de alıcı katılımcıya maliyetleri, dolaylı olarak da ekonomiye maliyeti söz konusudur.

Bilgi teknolojileri riskleri ile yanlış veri üretilmesi, eksik veri üretilmesi, verinin üretilmesinde aksama ve sistemin tamamen çalışamaz hale gelmesi gibi sonuçlar meydana çıkabilir. Fakat tüm olası sonuçlarda, verilerin bütünlüğü (yanlış ya da eksik olmadığı) gözden geçirilmelidir. Verinin bütünlüğünün sağlanamadığı durumlarda, tutarsızlığın kaynağını bulmak çok zor, belki de imkansız olabilir. Para transferleri söz konusu olduğu için, tutarsızlığın olduğu adımda transfer edilen parayı geri alamama ihtimalinin olması da dikkate alınarak bilişim risklerinin oluşturulmaması yönünde azami çaba sarf edilmelidir.

Bilgi teknolojileri riskleri sonucunda, katılımcı sistemlerde ya da merkez sistemde mesaj akışının yavaşlaması ya da durması söz konusu olabilir. Akış düzeninin

bozulması likidite riskine yol açabilir. Likidite riskinin aşılamadığı durumlarda sistemik riskin oluşması söz konusu olabilir.

Bilgi teknolojileri risklerinin ortadan kaldırılması için öncelikle risklerin tanımlanması gerekmektedir. Bilgi teknolojileri riskleri, bilgi güvenliği, internet bankacılığı, yeni teknolojilerinin gelişmesi, ağ yapıları, yazılım ve donanım, olağanüstü durumlar, standartlar ve risk doğurabilecek diğer nedenler altında tanımlanmıştır.

6.1.1 Bilgi Güvenliği

Bilgi teknolojileri, bilgiyi işleme, saklama, iletme işlemlerini gerçekleştirmektedir. Bu işlemler gerçekleştirilirken bilgi güvenliği sağlanamadığı müddetçe riskler söz konusu olacaktır. Bilgi güvenliğine ilişkin çözümler kullanılabilirlik, veri bütünlüğü, yetki verilmesi, yetkilerin doğrulanması, veri gizliliği başlıkları sıralanabilir.

Kullanılabilirlik

Bilgi sadece yetkili birimlerce erişilebilir ve kullanılabilir olmalıdır. Kritik görevler (tasks), ne önce ne de sonra, tam gerekli olduklarında gerçekleştirilmelidir. Kritik olmayan görevler zaman kritik olarak tanımlanmamalıdır. Kaynaklara erişim ihtiyaç halinde olanaklı olmalı, gereksiz ve yetkisiz erişimler önlenmelidir. Sistem hatalarını meydana çıkarmalı ve kayıpları en aza indirgeyecek hata telafi yordamlarını içermelidir (Leinonen vd. 2002:74).

Veri Bütünlüğü

Süreçler arasındaki veri geçişleri, veri değişikliğine yol açmayacak biçimde sağlanmalıdır. Sistem, veri parçaları arasındaki ilişkinin doğruluğunu tahsis edecek ve sürekli kılacak fonksiyonlara sahip olmalıdır. Ayrıca verinin kaybedilmesi, günlendi ya da olmayan verinin eklenmesi olasılıklarını önlemek amacıyla verilerin hangi süreçlerden, hangi kullanıcılardan, ne zaman geçtiğini belirleyecek yapıyı sistem barındırmalıdır. Ödeme mesajının gönderen, alıcı, tutar ve valör gibi kritik veri alanlarının değiştirilmesine izin verilmemelidir (Leinonen vd. 2002:74). Bilhassa bankacılık işlemleri ile ilişkili oluşturulan veya kritik alanların otomatik olarak oluşturulabileceği ödeme mesajlarında kritik alanların (örn. valor, alıcı, tutar bilgileri) değiştirilmesine programlar izin vermemelidir.

Yetki Verilmesi

Önemli ve uygun izin sadece tasarlanmış amaçlar için verilmelidir. Kullanıcılar ve kullanımlarındaki süreçlerin yetki ve gereksinimleri dışındaki bilgi ve kaynaklara erişimleri engellenmelidir. Aynı şekilde bilginin yetkisiz ellerce yaratılması ve değiştirilmesi de engellenmelidir. Sistem erişim bilgilerinin listesini ve kurallarını tutan fonksiyonları içermelidir (Leinonen vd. 2002:74) .

Yetkilerin Doğrulanması:

Sistem kaynaklarına erişme yetkileri olan öğelerini (kullanıcıları, bilgisayarları, süreçleri ve diğer bileşenleri) tanımlayacak ve kontrol edecek nitelikte olmalıdır (Leinonen vd. 2002:74).

Veri Gizliliği:

Herhangi bir bilgi yetkisiz bireylere, varlık ve sürece açık olmamalıdır. Kıymetli veriler iç ve dış yetkisiz erişimlere karşı korunmalıdır. Çeşitli tür erişimleri engelleyecek yöntemler geliştirilmeli, veri maskeleye sağlanmalıdır (Leinonen vd. 2002:74).

Denetlenebilirlik:

Güvenlik açısından tehdit oluşturabilecek tüm olaylar kayıt altına alınmalıdır. Verilerin geçtikleri süreçler, kullanıcılar ve kullandıkları programların adımları da kayıt altına alınmalıdır (Leinonen vd. 2002:74).

Bilişim teknolojilerin her noktasında bilgi güvenliğinin sağlanması riskleri azaltacaktır bir yaklaşım olacaktır.

6.1.2 İnternet Bankacılığı

Bilgi teknolojilerinin ekonomi üzerindeki güçlü etkisi bilgisayar ağlarındaki ve internetteki gelişimlerden kaynaklanmıştır. Bu etki iş pratiklerini yeniden şekillendirilmesine etken olmuştur. İnternet, şirketlerin yeni çevrimiçi (online) iş modelleri geliştirmelerini, müşteriler ve diğer firmalarla iletişimlerini güçlendirmelerini, yeni ürün ve hizmetler sunmalarını, etkin ve global işler ortaya çıkarmalarını sağlamıştır (Vlatko, 2000:1). İnternet bankacılığı, gelişen çevrimiçi iş modellerinden birisi olmuştur ve büyük yaygınlık kazanmıştır.

Bankalara maliyet ve prestij açısından olumlu etkiler yaratan internet bankacılığı, yarattığı güvenlik açıkları nedeni ile aynı zamanda sıkıntılar da oluşturmaktadır. Elektronik ödeme sistemleri için müşteri ile mesafenin ortadan kalktığı en gelişkin örnek internet bankacılığıdır. İnternet bankacılığı ile birlikte, her erişim güvenlik açısından bir açığı da beraberinde getirmektedir ve sahtecilik yöntemlerinde bu açıklar kullanılmaktadır. Kullanılan en yaygın sahtecilik yöntemi Phishing (Olta) saldırıları olarak adlandırılmaktadır. Bir banka adına art niyetlilerce gönderilen bir mailde, bankanın web adresinin linkinin verilmesi, bir yeniliğin reklamının yapılması ve linke tıklanarak işlem hakkında bilgi edinilmesi istenmektedir. Linke tıklandığında arka planda çalışan bir programla başka bir sayfa, bankanın internet giriş sayfasının birebir kopyası olarak kullanıcının karşısına gelmekte, kullanıcının şifreleri alındıktan sonra ise teknik arıza nedeniyle hizmet veremiyoruz türünden bir mesajla işlem sonlandırılmaktadır. Bu süreçte kullanıcının tüm şifreleri ve bilgileri ele geçirilmektedir. Bir başka yaygın yöntem olan keylogger adı verilen, klavye ve ekran görüntülerini kopyalayabilen programlar vasıtasıyla, kullanıcıların bilgileri ve kullandıkları şifreler elde edilmektedir. Sahtecilikle elde edilen bilgiler ve şifrelerle kullanıcının hesaplarına erişilmekte ve hesaplardan ödeme sistemleri kullanılarak yapılan para transferleri ile hesaplar boşaltılabilmektedir.

Ekrandan girişi istenen hesap numarası alanına, hesap numarası yerine kötü niyetle girilecek bir yazılım parçası (script) ile veri tabanındaki bilgilerin silinmesini/değişmesini sağlayacak, internetten bilgisayar sistemlerine yasadışı bir şekilde ulaşarak, sistemlere zarar verecek saldırılar gerçekleştirilmektedir. Bu saldırılar ödeme sistemlerinin kullandığı veri tabanlarını da risk altına almaktadır.

Bu yollarla pek çok hırsızlık olayının ve saldırının gerçekleşmesi üzerine bankalar, kendi adlarına gönderilmiş e-postalardaki linklere tıklanılmaması yönünde müşterilerin uyarılması, şifrelerin ekranda beliren sayısal klavyelerle alınması, her erişimde farklı bilgilerin istenmesi, kullanıcıların interaktif hesaplarının kullanımları için belirli limitler tanınmasına olanak sağlanması, büyük meblağlı para aktarım işlemlerinde kullanıcıdan telefonla teyit alınması, kullanıcıların internet üzerinden yapılabilecek sahteciliklerle ilgili bilgilendirilmesi, ekrandan alınan veri alanlarının uygunluğunun kontrol edilerek, yazılım parçalarının enjekte edilme girişimlerinin engellenmesi, firewall olarak isimlendirilen araçları kullanarak yasadışı erişimlerin engellenmesi ve kontrol edilmesi gibi güvenlik önlemlerini kullanıma almışlardır.

Önlemler alındıkça, yeni dolandırıcılık teknikleri geliştirilmektedir. İnternet bankacılığı yetkisiz kullanıcıların ödeme sistemlerine erişimine açık kapı bırakmaktadır. Ödeme mesajlarına eklenecek internet bankacılığınca oluşturulmuş mesaj bilgisi, bu tarz mesajlarda ekstra kontrollerin yapılmasına olanak sağlayarak riskleri en aza indirgeyebilir. Örneğin internet bankacılığı ile oluşturulan bir mesaj alındığında, ilgili hesaba parayı hemen aktarmak yerine, hesabın karapara listelerinde olup olmadığı kontrol edilebilir.¹⁰

Hesabın ödeme kaynağı bilgisini içeren mesajlar 29 Mayıs 2006 tarihinde Türkiye ödeme sistemi EFT’de uygulamaya alınmıştır. Bu bilgiyle sistemdeki ödeme mesajlarının ne kadarının internet tabanlı olduğu, risk oluşturan ya da oluşturma

¹⁰ Karapara aklama işlemlerinde, yasadışı faaliyetlerin ve terör eylemlerinin finansmanının sağlanmasında ödeme sistemlerinin kullanılmaması amacı ile yasaklı isimlerin tutulduğu karapara listeleri oluşturulmaktadır. Daha önce bu suçu işleyenler ya da işlemesi olası isimler bu listelerde tutulmaktadır.

potansiyelli mesaj görüldüğünde sorunun nerden kaynaklandığına ilişkin istatistiki bilgiler elde edilerek çözüme katkı sağlanması söz konusudur.¹¹

6.1.3 Yeni Teknolojiler

Teknolojinin yenilenme hızı da kendi başına bir risk unsurudur. Eskimiş teknolojilerde kalmak yeniliklerin sunduğu fırsatlardan yararlanmayı engellerken, yeni teknolojileri kullanmaya başlamak edinme maliyeti, adaptasyon süreci, yeni güvenlik kontrolleri gibi süreçleri ve risklerini beraberinde getirecektir.

Bilgi teknolojileri belli bir süreden sonra ömrünü tamamlamakta, yerini bir başka teknolojiye bırakmaktadır. Bilgi teknoloji geçişlerinde, en uygun zamanın seçilmesi ve geçişin mevcut sisteme uyumunun ve güvenliğinin sağlanması önemli noktalardır. Sistemlere yararı olmayan teknolojilere geçilmesi, ölmeye mahkum teknolojilerin sistemlere dahil edilmesi, ödeme sistemlerinde aksamalara yol açabilir. Ve aksamaların giderilmesi için teknolojilerin sistemlerden ayıklanması, ya da uyarlamalarla sorunun giderilmesi gibi maliyetli çözümler söz konusu olabilir. Geçişin yapılacağı bilgi teknolojisi pahalı bir teknoloji ise, bütçeleme konusunda sıkıntılar yaşanabilmektedir. Bilhassa yaşanan krizlerde yatırımların askıya alınması gündeme gelmektedir.

Yeni teknolojilere örnek olarak XML (Extensible Markup Language) olarak isimlendirilen standart verilebilir. XML veri taşınabilirliğine olanak sağlayan yeni

¹¹ Türkiye örneğinde internet üzerinden kredi kartı ödeme ve hesaba aktarım işlemlerini gerçekleştiren KRED-KART , NORM ve KRED isimli mesajları üretilmektedir.

bir bilgi formatıdır. Değişik bilgisayar sistemlerinin herhangi bir özel dosya aktarım programı ya da arayüzü oluşturmaya gerek kalmadan veri değişimi yapmasını mümkün kılmaktadır. Teknik olarak XML platform bağımsız, genişletilebilir, tek başına ya da başka çözümlere gömülü olarak kullanılabilen bir yapıdır.

Uluslararası bir standart olan XML, ödeme sistemleri konusunda yapılan çalışmalarda da ilgi odağı olmaya başlamıştır. The International Standards Team harmonisation (IST) çalışma grubu genel XML ödeme standartlarını oluşturmak üzere 2003 sonbaharında çalışmalarına başlamışlardır. Yakın gelecekte XML tabanlı mesajlar ödeme sistemleri üzerinde akışlarına başlayacaklardır. Mevcut mesaj formatlarından XML tabanlı mesaj formatlarına geçiş oldukça köklü değişiklikleri de beraberinde getirecektir.

Yeni teknolojilere geçişlerde sıkıntı yaşanmaması için önerilebilecek yaklaşımlardan biri eski ve yeni teknolojinin bir müddet paralel olarak çalıştırılmasıdır. Bu yaklaşım her teknoloji değişiminde söz konusu olamayabilir. Eski ve yeni teknolojilerin bir arada kullanıldığı bir örnek olarak SWIFT ağ yapısı SWIFTNet'in protokol değişikliği gösterilebilir. SWIFT ağ yapısının X.25 protokolünden TCP/IP (Transmission Control Protocols/Internet Protocols) protokolüne dönüştürme sürecinde, 2003 yılında geçişe imkan sağlanmış, 2004 yılında ise tamamen TCP/IP yapıya geçilerek eski yapıyı devre dışı bırakılmıştır. Bu süre boyunca iki sistem de devrede tutulmuştur. Geçişler ülkeler bazında gerçekleştirilirken, ülkeler içinde de katılımcılara farklı zamanlarda sisteme dahil olma şansı sunulmuştur. 2004 yılının

belli bir diliminden sonra yeni yapıya geçmeyen katılımcıları hızlandırmak amacı ile eski ağdan gönderilen her mesaj için daha fazla ücret talep edilmiştir.

6.1.4 Ağ Yapıları

Geçmişte bilginin korunması fiziksel güvenlik, fiziksel ortam ve çalışanların motivasyonu ile ilgili bir konu olarak tanımlanmıştır. Kasalar bulundurmak, kuryelerle verinin iletilmesi güvenli sayılan yöntemler arasında sıralanmıştır. Bilginin radyo kanallarıyla iletmeye başlanması koruma yöntemlerinde bir başkalaşımı da beraberinde getirmiştir. Bilgisayarların işlem gücü arttıkça veri manyetik ya da optik ortamlarda saklanmaya, veri transferi yerel ve global telekomünikasyon ağları üzerinden gerçekleşmeye başlanmıştır. Bilgisayarlarda işlenmekte olan ve ağlar üzerinden transfer edilen veriler pasif ve aktif ataklara karşı daha kırılgan hale gelmiştir. Bu tür tehditler bilhassa finansal işlemler ve elektronik ticaret için tehlike arz etmektedir. Elektronik ortamdaki veri kağıt ortamdaki veriden daha kolayca ve iz bırakmadan değiştirilebilmektedir (Preeneel, 1998).

Ağ yapılarının genişlemesi ile ağlar üzerinde veri dinlenmesi, yetkili olmayan birimlerin veri aktarımına müdahale etmesi gibi riskler de oluşmaya başlamıştır. Bu risklerin ortadan kaldırılması amacı ile Public Key Infrastructure (PKI) olarak adlandırılan bir yapı geliştirilmiş ve bir standart haline gelmiş bulunmaktadır. PKI, kullanıcılarına ağlar üzerinde güvenilir otoritelerce sağlanan özel şifreli anahtar çiftiyle güvenli veri iletişimi olanağı sağlamaktadır. Ağ üzerinde güvenli iletişime olanak sunan sayısal sunucu ve istemci sertifikalar ile verinin ağ üzerindeki yolcuğunda erişilmesi engellenerek, riskler ortadan kaldırılmaya çalışılmaktadır.

Türkiye ödeme sisteminde bu yapı, 28 Kasım 2005 tarihinden itibaren kullanılmaya başlanmıştır.

Transfer edilen verinin şifrelenerek yetkisiz kişilerce görünmesinin engellenmesi ve transferi sırasında bozulmadığının garanti edilmesini sağlayan bütünlük algoritmaları da kullanılarak ağ üzerinde veriye müdahale riskleri ortadan kaldırılmaya çalışılmalıdır.

Mesajların ağda dolaşımı sırasında değişmediklerini garanti etmek amacı ile belirlenen formüllerle mesajları referans edecek değerler mesaj başlıklarına eklenebilmektedir. Mesaj alıcılarınca bu referans değerinin uygunluğunu kontrol edilebilmekte, aynı referanstan bir mesajın tekrar gelmesi durumunda mesaj göndericisine iade edilebilmektedir. Bunun yanı sıra, mesajı gönderen terminal ve gönderen banka kodları ilişkisi, mesajın içerdiği gün bilgisi gibi bilgiler de kontrol edilerek ağ dolaşımının güvenli bir biçimde sağlandığı garanti edilebilmektedir. SWIFT, mesaj aktarım sistemine bağlanan her katılımcısına bir oturum numarası vermektedir. Ve her katılımcının gönderdiği mesaja gönderen banka, gönderilen iş günü, oturum numarası, oturum içi sıra numarası bilgilerinden oluşan bir referans bilgisi iliştilmektedir. Bu referansı içeren sadece bir mesaj sistemden geçebilmektedir.

Ağda tanımlı olmayan bir katılımcıya mesaj göndermeye çalışmak, mesajın alıcısına geri iade edilmesine ve mesajın hedefine ulaşamaması nedeniyle ağ trafiğini gereksiz arttırmasına neden olacaktır. Ağda tanımsız bir kullanıcıya mesaj gönderme,

gönderen katılımcının veritabanındaki sistem katılımcıları bilgilerinin güncel olmamasından kaynaklanmaktadır. Bu nedenle ödeme sistemleri katılımcı bilgilerini güncel tutacak yöntemler sunmaktadırlar. Türkiye örneğinde, 2. nesil sistemin devreye alınmasından sonra duyulan ihtiyaç nedeniyle HABR-BKOD ve HABR-SKOD mesajları geliştirilmiştir. HABR-BKOD mesajı banka kodları, isimleri adresleri gibi bilgileri güncellerken, HABR-SKOD mesajı bankaların şube bilgilerine ilişkin güncellemeler yapmaktadır. HABR-BKOD mesajı sadece merkez bankası tarafından üretilirken, HABR-SKOD mesajı şubesi değişiklik görececek banka tarafından yayınlanmaktadır. Mesajlar katılımcılara ulaştığında, katılımcı sistemleri mesajları otomatik olarak işleyerek veritabanlarını güncellemektedirler.

Ağ yapılarının dinlenmesi dışında bir bilişim riski de, ağlarda sorun oluşması sonucu iletişimin kesilmesidir. Bu riski ortadan kaldırmak için ağ yapıları yedeklemeler yapılmaktadır. SWIFTNet, SWIFT mesajlaşma trafiğini sağlayan ağ yapısıdır. SWIFT ağı güvenli yapısı ile bir standart olmuş durumdadır. SWIFT ağının birincil ağ olarak kullanılması ya da, ikincil yedek ağ olarak kullanıldığı örnekler yaygın olarak görülmektedir. Örneğin CHIPS, Avrupa birliği ülkeleri ve TARGET SWIFTNet'i birincil ağ olarak kullanmaktadır. Bilhassa 11 Eylül saldırılarından sonra, Amerika ödeme sistemi Fedwire'in SWIFTNet'i yedek ağ olarak kullanması gündeme gelmiş bulunmaktadır. 2004 yılında Atlanta'da gerçekleşen SIBOS konferansında, Federal Reserve Bank (FED) of New York adına yetkili Gary Berton SWIFTNet'in Fedwire bünyesinde kullanılmaya başlanacağını ifade ettiği bilgisi SWIFT resmi internet sitesinden edinilmiştir. Amerika'daki öncü bankalardan oluşan ve FED New York tarafından desteklenen "The Payments Risk Committee"

tarafından hazırlanan raporda (2004), Fedwire'nin ağı Fednet'in kullanılmadığı durumlarda SWIFTNet'in devreye alınmasına yönelik çalışmalara 2004 yılında başlandığı ifade edilmiş bulunmaktadır. Türkiye ödeme sistemi SWIFTNet'i kullanmamaktadır. Türkiye ödeme sistemi için de ağın kendi içinde yedeklenmesi söz konusudur.

6.1.5 Yazılım ve Donanım

Ödeme sistemlerinde kullanılmakta olan yazılımın ve donanımın, sistemlerin geliştirme süreçlerinde iyi analiz, tasarım, test süreçlerinden geçmesi ve devreye alındıklarında uygulanmalarında sorunlar yaşanmayacak biçimde bakımlarının yapılıyor olmaması gerekmektedir. Aksi durumlarda bilgi teknolojileri riskleriyle karşı karşıya kalınması söz konusu olabilir.

Operasyonel güvenlik ve bilgi garantisi sağlamak için tasarlanan kanunlar, gereksinimler ve politikalar, yazılım geliştirilirken oluşabilecek riskleri tam olarak adreslememektedir (United States General Accounting Office,2004: 8). Bu nedenle yazılım geliştirilirken uluslararası düzeyde kabul görmüş metodolojiler takip edilmelidir.

Ödeme sistemleri yazılımlarını geliştirecek ekibin teknik açıdan güçlü bir ekip olması gerekmektedir. Ödeme sistemleri için yazılımlar, katılımcı yazılımları ve merkez sistem yazılımları olarak ikiye ayrılmaktadır. Katılımcılar yazılımlarını, ortamları doğrultusunda kendi bünyelerinde geliştirilirken, merkez yazılımların sistemin sahibi organizasyonlar tarafından geliştirilmesi gerekmektedir. Geliştirme

işlemi kurum personelleri tarafından yapılabileceği gibi, dış kaynaklardan (outsourc) da yararlanmak söz konusudur.

Türkiye Bankalar Birliği'nin (TBB) Mart 1998 de yayınladığı Elektronik bankacılık ve Elektronik para faaliyetleri için risk raporunun 6. sayfasında dış kaynaklardan faydalanma konusunda şu saptamalarda bulunulmuştur :

“Çoğu bankaların, elektronik para ve elektronik bankacılık faaliyetlerinin gerçekleştirilmesi, işletilmesi ve desteklenmesi için harici hizmet sağlayıcılar ve uzmanlara dayanması muhtemeldir. Bu tür bir dayanma arzu edilebilir, çünkü bankanın ekonomik olarak kendisinin sağlayamayacağı elektronik bankacılık ve elektronik para faaliyetlerinin bazı özelliklerinin dışarıya yaptırılmasını sağlar. Ancak, dışarıya yaptırmaya dayanmak, bankayı operasyonel risklere maruz bırakır. Hizmet sağlayıcılar banka tarafından umulan hizmetlerin sağlanması için gerekli uzmanlığa sahip olmayabilirler veya teknolojilerini zamanında yenileyemeyebilirler. Hizmet sağlayıcının operasyonları sistem çökme veya mali zorluklar nedeniyle durabilir, bu da bankanın ürün ve hizmetleri sunma yeteneğini tehlikeye sokar.

Bilgi teknolojisini karakterize eden hızlı değişim, bankalara sistem işe yaramazlığı riski getirir. Örneğin, elektronik bankacılık ve elektronik para ürünlerinin müşteriler tarafından kullanılmasını kolaylaştıran yazılımın güncelleştirilmesi gerekir fakat yazılım güncellemelerinin dağıtılma kanalı, suçlu veya kötü niyetli şahısların müdahale edebilmesi ve yazılımı değiştirebilmesi nedeniyle, bankalar için risk doğurur. İlaveten, hızlı teknolojik değişim personelin

banka tarafından kullanılan yeni teknolojinin mahiyetini tamamen anlamasını önleyebilir. Bu da yeni veya güncelleştirilen sistemlerle operasyonel problemlere neden olabilir.”

TBB’nin de dile getirdiği üzere bankaların kendi bünyelerinde bilişim teknolojileri birimleri barındırmamaları dış kaynaklardan yararlanmaları bankaları risklere açık hale getirmektedir. Günümüzde pek çok banka temel yeteneklerine ilişkin bilişim konularında dış kaynaklar barındırmayı tercih etmemektedir.

Merkez sistem yazılımlarında ise, daha kapsamlı bir sistem kurulması söz konusu olduğu için konusunda uzmanlaşmış global firmalar, ülkelerin sistemlerini geliştirmektedir. Birleşik Kral’lık kökenli BT firması LogicaCMS’in CAS isimli ürünü Azerbeycan, Şili, Bosna-Hersek, Sırbistan, Avusturya, İrlanda, Litvanya, Lüksemburg, Filipinler, Slovenya, Sri Lanka, Trinidad-Tobago ve Türkiye merkez bankalarının sistemlerinde ve TARGET sisteminde kullanılmıştır. ABD kökenli BT firması Motran, Hollanda, Bulgaristan, Ermenistan, Kuveyt ve Romanya RTGS sistemlerini geliştirmiştir. ABD kökenli BT firması CMA Libya, Makedonya ve Serbia RTGS sistemlerini geliştirmiştir. Fransa kökenli BT firması Diamis, Ürdün RTGS sistemini geliştirirken, İtalya tabanlı BT firması SIA, İtalya RTGS sistemini geliştirmiştir (Okay, 2004:40). SIA web sitesinde İsviçre RTGS sistemi SIC 2. nesil çalışmalarını geliştirmek üzere İsviçre ile 2005 yılında anlaşmaya vardığını yayınlamıştır.

Gelişmekte olan ülkelerin bazılarında ödeme sistemleri sıfırdan geliştirilirken, ödeme sistemlerine sahip ülkeler gelişen koşullarla birlikte ödeme sistemlerini

yenilmektedirler. Örneğin Türkiye, 24 Nisan 2004 tarihinde 1992 yılından beri kullanılmakta olan EFT birinci nesil sistemi devre dışı bırakarak, EFT ikinci nesil sisteme geçmiştir. Birinci nesil ve ikinci nesil sistemler arasında oldukça büyük farklar bulunmasına rağmen, EFT geçişi başarı ile tamamlanmıştır. Türkiye ödeme sistemi değişikliği başarılı bir geçiş örneği olarak gösterilirken, literatürde geçiş sırasında yaşanan sorunlara rastlanmaktadır. Örneğin İtalya RTGS sisteminin BIREL'den New BIREL'e geçişinden birkaç ay sonra yazılım problemi nedeniyle sistem kesintiye uğramıştır (IMF, 2004:23). Bilhassa bu boyuttaki büyük geçişlerde test süreçleri büyük bir titizlikle gerçekleşmeli, geçişin tatil günlerine denk getirilmesi sağlanarak olası sorunların çözümü için daha fazla zaman şansı yaratılmalı, geçiş sonrasında sistemler oturana dek sistemler sürekli izlenmeli, ilgili elemanların o dönemde izinli olmamasına özen gösterilmeli, büyük sorunlar yaşanıp sistemin çalışırılığının sağlanamadığı durumlarda eski sistemlere dönüş mümkün kılınmalıdır.

Uygulamaların geliştirildiği sistemler gerçek sistemlerin bire bir kopyası olamamaktadır. (Maliyetler nedeniyle test ortamlarında daha düşük kapasiteli donanım kullanılmaktadır, gerçek verilere erişim kısıtlaması nedeniyle test ortamlarında test verileri bulunmaktadır.) Bu nedenle geliştirme ortamından üretim ortamına geçişlerde uygulamaların doğru ve etkin çalışmaları açısından her zaman risk bulunmaktadır. Mesajların içerisine eklenecek mesajın test mesajı olduğunu belirtecek alanlar ile gerçek sistemlerde testi olanaklı kılmak bu riski azaltacak bir çözüm olarak düşünülebilir.

Sistemlerin ağırları ve donanımlarına oranla yazılımları çok daha fazla değişikliklere uğramaktadır. Donanım ve ağırlar bilginin saklanması, iletilmesi gibi işlevleri sağlarken yazılımlar verinin oluşturulması ve işlenmesini gerçekleştirmektedir. Değişiklik oranının fazlalığı, veri değişikliğine kolay olanak vermesi nedeniyle yazılımlar görece olarak daha fazla risk unsurudur.

Kişisel hesaplardaki kayıplar küçük olduğu zaman sahiplerince fark edilmeyebilir. Araya sıkıştırılan yasadışı yazılımlarla her hesaptan çalınacak bir kuruş ya da cent hesap sahibinin dikkatini çekmezken, ödeme sistemleri üzerinde gerçekleşen işlem hacmi düşünüldüğünde suçun farkına varılmadan büyük bir hırsızlık gerçekleştirilebilir (OTA, 1982: 47). Ülkemiz ödeme sistemi üzerinden bir örnekleme yapacak olursak: TCMB elektronik veri dağıtım sisteminden elde edilen bilgilere göre, 22.05.2006 tarihinde 502,400 adet ödeme işlemi gerçekleşmiştir. Her işlemde bir kuruşun art niyetli kişilerce yapılan düzenlemelerle çalınması halinde 5,024 YTL tutarlı bir hırsızlığın bir günde gerçekleştirileceği hesaplanmaktadır. Daha büyük işlem hacmine sahip ödeme sistemlerinde ve yapılan hırsızlığın uzun müddet farkına varılmadığı durumlarda ise ilgili tutar çok daha fazla olacaktır. Bu riski ortadan kaldırmak için bankalar, bünyelerindeki hesapların işlem görme sayılarını günlük olarak ve belirlenen periyotlarla izleyerek olağandışı işlem gören hesapları inceleme altına alabilirler. Ödeme sistemlerinde mesaj tutarına bir alt limit konması ya da belirli limitin altında tutar içeren mesajların alıcı bilgilerin tekrar edip etmediğinin kontrol altına alınması bu tarz yolsuzlukları ortadan kaldırmak için birer çözüm olabilir.

Yazılımlarda veri alanlarının kontrol edilmemesi, ve veri giriři sırasında veri alanına yazılan bir script ile veri tabanındaki bilgilerin tahrip edilmesi, bir ödeme mesajı içinde yapılacak deęişikliklerle (örneğin alıcı, valör tarihi ya da tutar alanı) büyük miktarlarda paranın çalınması söz konusu olabilmektedir.

Yazılımlar içerisinde koşulların doğru kontrol edilmemesi, döngülerden çıkılamamasına ve işlemin tekrar tekrar gerçekleşmesine neden olabilir. Bir kere yapılmak istenen bir ödeme işlemi, hesapta para tükenene kadar yinelenebilir. Eksi bakiye oluşmasına rağmen ödeme yazılımlar ödeme işlemini gerçekleştirebilir.

Bir yazılımın yanlış zamanda çalışması, sistem parametrelerindeki deęişiklikler nedeniyle sistemlerin çalışmaması, çalışan yazılımların veritabanı kaynaklarının kilitlenmesine ya da veri tabanından veri silinmesine sebep olması, yetki tablolarının silinmesi gibi nedenlerle de ödeme sistemlerinde sıkıntılar oluşabilmektedir.

Yazılımlardan kaynaklanacak riskleri engellemek için, önemli modüllerin yazılımlarının en az iki kiři tarafından gerçekleştirilmesi (pair programming), yazılım ve test ekiplerinin ayrıştırılması, yazılımların versiyonlamasının yapılması, yazılım deęişikliklerinin kayıtlarının tutulması, gerçek ortamda yazılım üzerinde deęişiklik yapılmasına olanak verilmemesi, yazılım deęişikliklerinin geliştirme ve test ortamlarında yapıldıktan sonra onay dahilinde gerçek ortamlara yansıtılması, uygulama geliştiricilerin gerçek ortamda veriyi deęiřtirme yetkisinin olmaması, süreçlerin ve yazılım kalitesinin denetlenmesi gibi önlemler alınabilir.

Donanımların arızalanması, donanımlara yetkisiz erişimlerle sistemlere zarar verilmesi, donanımı satan firmanın ürüne desteğini kesmesi ihtimalleri risk barındırmaktadır. Donanımlarda ortaya çıkabilecek riskleri ortadan kaldırmak amacı ile, donanımların bakımlarının düzenli yapılmasının, donanımlara erişimlerin yetki dahilinde olmasının sağlanması gerekmektedir. Ürüne ilişkin alımların detaylı araştırılmaların yapılarak gerçekleştirilmesi durumunda donanım kaynaklı problemler azaltılabilecektir.

6.1.6 Olağandışı Durumlar

Elektronik ödeme sistemlerinde bilgi kayıpları kasıtlı olabileceği gibi donanım yazılım ve ağ yapılarında oluşabilecek bir sorun nedeniyle kazara da oluşabilmektedir. Bu nedenle sistemler sürekli yedeklenmelidir.

İşlemlerin tamamıyla elektronik ortama aktarılmış ve işlem boyutlarının artmış olması, elektronik yapının çökmesi durumunda işlerin elle yürütülmesini imkansız kılmaktadır. Bu nedenle olağandışı durum planlarının oluşturulması yedek merkezlerin oluşturulması ve bu merkezlere gerçek sistemdeki tüm işleyişin kopyalanması bir gereklilik boyutundan çıkıp zorunluluk olmuştur. Yedekleme eşzamanlı olarak yapılmalı ve aktif sistemin çalışmasını etkilememelidir.

Olağandışı durum senaryoları yazılmalı, sıklıkla güncellenmeli ve test edilmelidir. Testler gerçek sistemler çalışırken yedek merkezlerde olağandışı durum senaryoları adım adım gerçekleştirilerek yapılmalıdır. Yedek sistemlerin test edilmesi amacı ile

yılın belli günlerinde gerçek sistemler devredışı bırakılarak yedek sistemler üzerinden çalışılmalıdır.

Olağandışı durum planlarının her şeyden önce, konuyla ilgili birimlerin bir araya geldiği bir grup tarafından oluşturulması gerekmektedir. Olağandışı durum planlarının oluşturulmasının ilk adımı, işin sürekliliğini engelleyebilecek olayların listelenmesidir. Bunun ardından, bu olaylar olası etkilerine göre derecelenmelidir. Olağandışı durum planının temel amacı herhangi bir kriz durumunda, öncelikle işin sürekliliğini sağlayacak düzenlemeleri yapmak ve sorun çözüldükten sonra operasyonların günlük akışında devam etmesini sağlamaktır. Olağandışı durum planlarında hangi işlerin daha kritik olduğu ve bu işlerin hangi sırayla yapılması gerektiği belirlenmiş olmalıdır. Oluşturulan olağandışı durum planlarının test edilmesi, ilgili personelin eğitilmesi ve bu planların periyodik aralıklarla gözden geçirilerek iş akışlarında meydana gelen değişikliklerin plana yansıtılması, planların işler olması açısından önem taşımaktadır (Akan,2004:67-68).

Veri merkezleri veri kaybında veriyi tekrar elde edecek yapıları kapsayacak şekilde oluşturulmalıdır (IMF, 2004 : 24).

6.1.7 Standartlar

Ödeme sistemlerinde mesajların müdahaleye gerek kalmadan, tam otomasyon süreci içinde sistem içerisinde dolaşması riskleri ortadan kaldıracaktır.

Ödeme sistemlerinde işlemlerin, müdahaleye gerek kalmadan tam otomasyon süreci içerisinde gerçekleşmesi için uluslararası düzeyde kabul görmüş standartlar söz konusudur.

SWIFT dünya çapında kabul görmüş ve pek çok önemli ödeme sisteminde kullanılmakta olan standartları bünyesinde barındırmaktadır. SWIFT standartlarının kabulü pek çok önemli sistemle aynı dili konuşmayı sağlayacaktır. Ortak bir ödeme sistemi dilinin varlığı ise operasyonel riskleri en aza indirecektir.

Hesaba aktarım mesajlarında, işlemlerin otomatik olarak gerçekleşmesi nedeniyle, mesaja yanlış hesap numarası girilmesi durumunda, para yanlış hesaba aktarılacaktır. IBAN : international Bank Account Number (uluslar arası banka hesap numarası), para transferlerinin yanlış hesap numarası ile yapılmasını önlemek amacıyla ilk olarak Avrupa Birliği ülkelerinde ortaya çıkmış bir hesap numarası standardıdır.

Avrupa Birliği Standardı çerçevesinde en fazla 34 basamak uzunluğunda olan IBAN'ın ilk iki hanesi, tüm ülkelerde standart olmak üzere ait olduğu hesabın ülke kodunu ve iki haneli kontrol rakamını içermektedir. Kontrol rakamları, IBAN'ın içerisinde bulunan diğer rakamlar üzerinde bir takım hesaplamalar yapılarak ulaşılabilen rakamlardır. Bu hesaplamalar standart ve herkesçe bilinen bir yöntem ile yapılmaktadır ve IBAN kullanan bütün ülkeler kontrol basamaklarını bu hesaplama standardına uygun şekilde hesaplamaktadır. Bu nedenle, IBAN'ın içerisindeki basamaklardan biri veya fazlası yanlış veya eksik yazılırsa, yukarıda sözü edilen

standart hesaplama yapıldığında IBAN'ın içerisindeki kontrol rakamından farklı bir rakama ulaşılacak ve IBAN'ın yanlış olduğu anlaşılacaktır

34 basamak uzunluğunu aşmamak ve ilk 4 hanede ülke kodu ile kontrol basamaklarını içermek koşulu ile her ülke kendisine ait IBAN'ların basamak sayısı ve biçimini gösteren ülke IBAN standardını serbestçe belirleyebilmektedir. Ülkeler, belirledikleri IBAN basamak sayısı ve biçimini IBAN kullanan diğer ülkelere duyurmaktadır. Bu sayede, her ülke diğer bir ülkeye ait IBAN'ın uzunluğunu da kontrol edebilmektedir.

Bu özellikleri sayesinde IBAN, para transferi talebi gönderici bankaya ulaştığında alıcı bankaya transfer mesajını göndermeden kendi içerisindeki özel ve standart hesaplama yöntemi ile kontrol edilebilmekte ve yanlış bir IBAN ile yapılmak istenen para transferi başlamadan engellenmiş olmaktadır.

IBAN, var olan hesap numaralarının yok edilmesini ya da bu numaraların para transferinde kullanılmamasını gerektirmemektedir. Uygulamada para transferine konu olan her hesabın numarasının yanı sıra bu hesaba bir de IBAN üretilmektedir. Para transferlerinde IBAN'ın kullanılması durumunda yukarıda sözü edilen avantajlar elde edilmektedir. Ancak –IBAN kullanımının zorunlu tutulduğu ülkelerin dışındaki- müşteriler istedikleri takdirde IBAN kullanmaksızın mevcut hesap numarası ile para transferi yapabilirler.

IBAN, sağladığı bu tür faydalar nedeniyle Avrupa Birliği ülkelerinin yanı sıra diğer bazı ülkeler tarafından da kabul görmüştür ve uygulanmaktadır. Bazı ülkeler, IBAN'ı yurtiçi para transferi işlemlerinde de kullanmaya karar vermişler; bazı ülkeler de aralarındaki ve kendi sınırları dahilindeki para transferleri için IBAN kullanımını zorunlu hale getirmişlerdir. (İş Bankası :2006).

Türkiye'de, 27 Haziran 2005 tarihinde ödeme sistemleri altyapısı uygun hale getirilerek, 1 Eylül 2005'ten bu yana IBAN standartları kullanılmaya başlanmıştır. Zorunlu kullanıma geçilmemiş olup, Merkez Bankası ve Bankalar Birliği ortak çalışmalarına devam edilmektedir.

6.1.8 Bilgi Teknolojileri Risklerini Doğarabilecek Diğer Durumlar

Günümüzde iş değiştirmek eskiye oranla daha sık yaşanan bir durumdur. İş değişikliklerinde çalışanlar deneyimlerini de beraberlerinde götürmektedir. Eğer gerekli dokümantasyon yapılmamış ise, ilgili elemanın sisteme ilişkin sorumluluklarının sonlanması nedeni ile sözel destek de sağlanamayacağından sorunların çözülmesi vakit alacaktır. Dolayısı ile yapılan çalışmaların dokümantasyonu hiçbir biçimde ihmal edilmemelidir.

Yaşanan olumsuzlukların küçük ya da büyük olmasına bakılmaksızın bir merkezi kayıt sisteminde tutulması da problemlerin tekrar yaşanması halinde çözümün önceki seferlerden daha hızlı olmasını sağlayacaktır.

Sistemlerin hızlı cevap verebilir olması, işlemlerin hızlı gerçekleştirilmesi açısından önem arz etmektedir. Bu nedenle sistemlerin darboğaza girmesine engel olacak yaklaşımlar sergilenmelidir. Bu yaklaşımlardan biri toplu mesaj gönderimidir (bulk payment). Katılımcıların toplu gönderilmesinde sakınca görmedikleri ödeme mesajları aktarıcı bilgisayarlarda bekletilmekte, alıcısı aynı olan mesajlar birleştirilerek tek mesaj olarak merkezi sisteme gönderilmektedir. Örneğin 10 ayrı toplu gönderilebilecek mesaj tek mesaj olarak gönderilmişse, merkez sistemde 10 ayrı işlem yerine(mesajın mutabakatı, ağda aktarımı vb.) tek işlem gerçekleşmektedir.

Sistemlerin bakımları göz önünde bulundurulduğunda, karmaşık sistemlerde yapılan bakımların daha fazla risk içerdiği göz önünde tutularak işlevi olmayan ögeler sistemlerden ayıklanmalıdır.

Kurumların çalışanlarının bilişim riski oluşturma olasılığı, sistemlere erişimleri olduğu için ve yaptıkları suç içeren işlemleri yasal işlerinin arkasına saklayabilecekleri için oldukça yüksektir (OTA, 1982: 48). Çalışanların sistemlere erişimleri mutlaka yetki dahilinde olmalıdır. Önemli işlemler birkaç onaydan geçerek gerçekleştirilerek, yasal işlerin arkasına suçların gizlenmesi engellenmelidir.

Ödeme sistemlerinde mesajların gönderen - merkez sistem, merkez sistem - alıcı rotası boyunca yolculuğunda, ağ trafiğini azaltmak amacı ile mesaj içerisindeki boşluk karakterleri sıkıştırılmaktadır. Mesajlar gönderen katılımcının uygulamalarıyla uygulama formatında oluşturulmaktadır. Merkez sisteme gönderilirken iletişim formatına dönüştürülmekte, merkez sistemde tekrar uygulama

formatına dönüştürülmektedir. Sonrasında ilgili katılımcıya gönderilmek üzere tekrar iletişim formatına dönüştürülmektedir ve alıcısına ulaştığında uygulama formatına dönüştürülerek mesaj iletişimi sonlandırılmaktadır. Bu sıkıştırma ve dönüştürme işlemleri sırasında mesaj içeriğinde bozulma riski söz konusu olabilir. Sistemler geliştirilirken ilgili tüm kombinasyonlarla mesajlar oluşturularak sisteme aktarılmalı, alanların sorunsuz sıkıştırıldığı ve dönüştürüldüğü gözlenmelidir.

Bir mesaj sistemin bir ögesinden çıktıktan sonra, varacağı ögede oluşan bir sorun nedeniyle, ilk ögede gönderilmiş görünmesine rağmen, ikinci ögede alınmamış olabilir. Bu nedenle sistem içerisinde mesajların alınıp alınmadığına dair geri bildirimler sağlanmalıdır. Ayrıca gün içinde belirli zamanlarda ve gün sonunda katılımcılar ve merkez sistem arasında, gönderilen ve alınan mesajların sayılarının tutarlılığı kontrol edilmelidir.

6.2 Temel İlke VII: İleri düzeyde güvenlik ve işlemler açısından güvenilirlik sağlanması¹²

Ödeme sistemleri için risklerini engellemek amacıyla yayınlanan sistemik açıdan önemli ödeme sistemleri için temel ilkeler raporunun VII. ilkesini (“ileri düzeyde güvenlik ve işlemler açısından güvenilirlik sağlanması”) sistemlerin operasyonel risklere karşı korunmalarının sağlanmasını amaçlamaktadır. Operasyonel riskler bünyelerinde bilgi teknolojileri risklerini de barındırdığı için, bu madde bilişim risklerini engellemeyi de kapsamaktadır.

¹² 6.2 başlığı altındaki bilgiler BIS tarafından 2001 yılında yayınlanan raporun, 37. ve 41. sayfaları arasından derlenmiştir.

BIS'in , 10 temel ilkeyi açıkladığı raporunda VII. maddeye ilişkin yorumları bu başlık altında aktarılacaktır. Sonrasında daha önceki bölümlerde tanıtılan ödeme sistemleri, VII. ilke çerçevesinde değerlendirilecektir.

Sistemik açıdan önemli ödeme sistemleri yüksek güvenilirlik ilkesine göre tasarlanmalı ve işletilmelidir. Ödeme sistemlerinde kullanılan teknolojiler oldukça karmaşık ve hızla değişen yapıdadır. Bir ödeme sistemi pek çok farklı işlev ve bileşenden oluşmaktadır. Bu işlev ve bileşen zinciri en zayıf halkası kadar güçlüdür. Sistemin operasyonel güvenilirliği bileşenlerinin (donanım, yazılım, telekomünikasyon ağı, işletim personeli) operasyonel güvenilirliğine bağlıdır. İşletim sisteminin tasarımcıları ve işletim sorumluları sadece merkez sistemin bileşenlerinin güvenliği ve operasyonel güvenilirliği ile değil sistem katılımcılarınıninki ile de ilgilenmeli, katılımcıların gerekli kurallara uymaları sağlanmalıdır.

İşletim sorumluları, sistemin güvenlik politikalarını ve operasyonel hizmet düzeylerini karşılayıp karşılamadığını izlemelidirler. Bu sürekli ve kapsamı geniş bir adım olarak iç ya da dış denetçileri de kapsayan bir süreç olarak gerçekleştirilmelidir. Bu süreçler bilhassa normal iş saatlerinde, katılımcılar için de gerçekleştirilmelidir. Eğer bir katılımcının performansı diğer katılımcılar ya da ödeme sistemi için gereksiz risk oluşturuyorsa katılımcının ilgililerinin dikkati bu noktaya çekmeli, önem arzeden kritik durumlarda ise sistem gözetimcisi bilgilendirilmelidir.

Bankacılık ve ödeme sektörü için uluslararası ve ulusal pek çok standart, kılavuz ve tavsiyeler bulunmaktadır. Bu standartlara uyma yüksek düzeyde güvenlik ve operasyonel güvenilirliği sağlamada yardımcı olacaktır.

Bahsi geçen standartlar:

International Organization for standardization (ISO),

The International Electrotechnical Commission (IEC),

The International Telecommunication Union (ITU),

The International Engineering Task Force (IETF),

The European Committee for Banking Standards (ECBS),

The American National Standards Institute (ANSI),

The British Standards Institution (BSI) tarafından oluşturulmaktadır.

Standartlardan örnek verecek olunursa :

Güvenlik:

ISO/ IEC TR 13335	Bilişim teknolojilerinin güvenlik yönetim kılavuzu
ISO TR 13569	Bankacılık ve ilişkili finansal hizmetler – Bilgi güvenliği kılavuzu
BSI 7799: 1999	Bilgi güvenliği yönetimi

ISO/ IEC 15408	Bilişim teknolojileri güvenliği değerlendirme kriterleri
ISO/IEC PDTR 15446	Koruma profilleri ve güvenlik hedefleri üretim kılavuzu

Kalite:

ISO 9000	Kalite yönetimi standartı
----------	---------------------------

Veriler:

ISO 9364	Bankacılık telekomünikasyon mesajları – Banka Tanımlama Kodu(BIC)
ISO 13616	Uluslararası Banka Hesap Numarası (IBAN)

Ödeme sistemi yeterli sayıda eğitimli, sistemi güvenli ve etkin biçimde işletebilecek ve bu süreçte operasyon ve risk yönetimi yordamlarını olağan ve olağandışı durumlarda izleyecek personele sahip olmalıdır. Personelin bir kısmı operasyon ve güvenlik yöneticisi gibi davranmalı ve üst düzey bilgi birikimine, deneyime ve yetkiye sahip olmalıdır. Personelin eğitimi doğru kararların alınmasını sağlayacak ödeme sistemleri ve önemine ait ufkun genişliğinin bir ürünüdür. Personel teknik ve operasyonel sorunları (mesai saatlerinin dışında da) çözebilecek yetkinlikte olmalıdır.

Bir ödeme sisteminin güvenlik politikaları ve operasyonel hizmet seviyeleri zaman içinde, ödeme sistemleri piyasalarındaki değişime ve daha güvenli, etkin, hızlı ve az maliyetli süreçler sağlayacak teknolojik gelişime, artan talep ve yeni katılımcılara bir cevap olarak değişmektedir. Bu değişim sistem tasarımı ve işletiminin değişikliklere uygun olduğu yapılarda daha kolay olabilmektedir. Bir önemli gelişme TCP/IP gibi internet tabanlı teknolojilerin, özel IP ağlarının ve internetin kullanıma alınması ile yaşanmıştır. Bu yeni teknolojiler bilgi ve kaynakların ortak kullanımına yönelik sağladıkları avantajlar nedeniyle giderek daha popüler hale gelmektedir. Her yeni değişimde sisteme etkileri iyi anlaşılmalı ve tanımlanmalıdır.

Güvenlik amaçları ve politikaları net bir biçimde tanımlanmalı, dokümanite edilmeli ve detayları ödeme sisteminin kapsamı, katılımcılarının ihtiyaçlarına göre oluşturulmalıdır. Yapılan işin önemi ve ödemelerin bütünlüğünün korunması gerekliliği göz önünde bulundurulduğunda sistemik açıdan önemli bir ödeme sisteminin güvenliği diğer pek çok sistemden daha üst düzey olmalıdır. Güvenlik politikaları ve amaçları sistem işletmenlerine ve katılımcılarına uygulanmalı, tasarım sırasında oluşturulmaya başlanmalı, düzenli olarak ve bilhassa sistem ve bileşenlerinde önemli bir değişim olduğunda gözden geçirilmelidir. Güvenlik adımları sık sık denenmelidir.

Güvenlik amaçları ve politikaları sistem mimarisi ve sahibinden etkilenmektedir. Örneğin yüksek derecede merkezileşmiş bir sistem (merkezi bileşenler, ağ, katılımcıların yerleşkelerindeki bileşenlerin bir birim tarafından sahip olduğu ve yönetildiği yapılar) oldukça merkezileşmiş güvenlik amaçları ve politikalarına sahip

olabilirler. Dağıtık yapılarda ise genel güvenlik amaçları ve politikaları üzerinde anlaşılmalı, sorumlulukların net tanımı yapılmalı, bileşenler arasında sistemin kontrol ve denetimini aksatmayacak koordinasyon sağlanmalıdır.

Güvenlik amaç ve politikaları sistem (donanım, yazılım ve ağı) ve verilerine, yetkili ve yetkisiz birimlerin fiziksel ve mantıksal erişimlerine ilişkin kontrolleri içermelidir. Güvenlik politikalarının düzenli analizlerinin tanımlanmış ve yapılandırılmış metodolojileri kullanmak gibi önemli bir misyonu vardır. Bu analizler sistem tasarımı başlamalı, sistemin iş gereksinimleri değiştiğinde, sistemin yapısında değişiklik olduğunda ve normal işleyiş sürecinde düzenli aralıklarla gözden geçirilmelidir.

Teknolojik gelişmeler zaman içerisinde sistemlerde açıkların olma olasılığını da arttırmaktadır. Bu gelişmeler için yeni güvenlik noktaları ve kontrolleri söz konusu olmalıdır. Sistem işleticileri, teknolojik gelişmeleri izleyerek sistem güvenliğinin güncel tutulduğunu kontrol etmelidir.

Güvenlik Risk Analizinin Temel Argümanları :

- Sistem güvenlik amaç ve politikalarını gözden geçirmek
- Sistem fonksiyonlarını, bileşenlerini, sınırlarını ve sorumluluk alanlarını tanımlamak
- Olası tehditleri ve etkilerini tanımlamak

- Varolan ve potansiyel kurtarıcıları tanımlamak (fiziksel araçlar, güvenlik yazılımları, örgütsel ve işletimel yordamlar)
- Her tür risk ve kırılganlığı tanımlamak
- Son iki adımı sistem risk ve kırılganlığı güvenlik amaç ve politikalarınca kapsanana kadar tekrar etmek
- Sistem kurtarıcılarını risk analiz süreçlerine katmak

Deprem, sel gibi olağandışı durumlar da göz önünde bulundurularak sistemin olağanüstü durum yordamları hazırlanmalıdır. Hata toleranslı ya da yedeklenmiş donanım elemanları kullanılmalıdır. Bilgisayar ve telekomünikasyon araçlarının düzenli bakımları yapılmalıdır. Yangın farketme ve bilgilendirme sistemleri kurulmalıdır. İş süreçlerine ve teknik yapıya ilişkin dokümanlar sürekli güncel tutulmalıdır. Sistem sürekli test edilmelidir. Verilerin ve değişiklik olduğunda yazılımların kopyasının alınması sağlanmalıdır. Telekomünikasyon kesintileri için fiziksel ortamdaki verinin katılımcılar arasında değiştirilebilmesini sağlayacak yordamlar tanımlanmalıdır.

6.3 Bilgi Teknolojileri Riskleri ve Seçilmiş Örnekler

Avrupa Merkez Bankası 2004 yılında Avrupa'daki büyük tutarlı ödeme sistemlerinin temel prensiplere uygunluğunu gözden geçirdiği bir rapor hazırlamıştır. Bu raporda ülkelerin TARGET sistemine bağlandıkları ödeme sistemleri 10 temel ilke çerçevesinde gözden geçirilmiş ve sonuçta Tablo-4 elde edilmiştir.

Sistemler RTGS esasına göre çalıştığı için netleştirme esasına ilişkin 5. ilke değerlendirme dışında tutulmuştur. Elde edilen sonuçlardan, sistemlerin 7. ve 8. ilkeler dışındaki ilkeleri tamamıyla gerçekleştirmiş bulundukları gözlenmektedir. Operasyonel riskleri irdeleyen yedinci madde, bilişim risklerini de içermektedir. Görülmektedir ki, ödeme sistemleri dünyasında önemli sayılan ödeme sistemleri için de bilişim riskleri söz konusu olmaktadır.

Avusturya, Belçika, Avrupa Merkez Bankası, Yunanistan, İrlanda, Hollanda, Portekiz ödeme sistemlerinin ana ve yedek merkezlerinin arasındaki uzaklık 1 kilometreden daha az olduğu için temel 7. ilkeyi tamamen sağlayamamıştır. Fransa'nın ödeme sisteminin merkezleri arasındaki uzaklık makul olmasına rağmen, sisteminin ve yedekleme yordamlarının karışık olması ve bu karışıklığın risk barındırması nedeniyle temel ilke 7. ilkeyi karşılayamadığı belirtilmiştir. Sistemlerin tümünde güvenlik politikası bulunmaktadır. Avrupa Merkez Bankası, Yunanistan, İtalya, Lüksemburg kendi ulusal metodolojilerinin yanında TARGET risk yönetimi metodolojilerini de kullanmaktadırlar.

Tablo 4 – TARGET Üyesi Sistemlerin CPSIPS İlkeleri ile Uyumu

Temel İlke	Tamamıyla Gözlenmiş	Geniş Ölçüde Gözlenmiş	Kısmen Gözlenmiş
1	16	-	-
2	15	1 (Fransa)	-
3	15	1 (İsviçre)	-
4	16	-	-
5	-	-	-
6	16	-	-
7	8 (Almanya,Danimarka, İspanya,Finlandiya, İtalya, Lüksemburg, İsviçre,İngiltere)	8 (Avusturya,Belçika,Avrupa Merkez Bankası, Fransa, Yunanistan,İrlanda, Hollanda, Portekiz)	
8	1 (İspanya)	14	1 (Avrupa Merkez Bankası)
9	16	-	-
10	16	-	-

Kaynak: ECB ,2004

Çalışmanın bu bölümünde daha önceki bölümlerle tanıtılan ödeme sistemlerine ilişkin bilişim riskleri ülke başlıkları altında incelenecektir. Örneklemeler IMF'nin gerçekleştirdiği Financial System Stability Assessment (FSAP) çalışması raporlarının ödeme sistemleri ile ilgili bölümlerden, TARGET yıllık raporlarından ve ülkelerin sistemlerini değerlendirdikleri yıllık raporlardan derlenmiştir.

6.3.1 RTGSPlus – Almanya

Yedek merkezin ana merkeze görelî yakınlığı dışında, sistem son derece güvenilir olarak tanımlanmıştır (IMF, 2003a: 45,46).

6.3.2 Fedwire – Amerika

FED tarafından 2001 yılında hazırlanan “Fedwire Fund Transfer System, Self-Assessment of Compliance with the Core Principles for Systemically Important Payment Systems” raporundan derlenen bilgiler doğrultusunda :

Fedwire, Federal Reserve’ün bilgi güvenliği mimarisini kullanmaktadır. Bilginin gizlilik ve bütünlüğünü ve operasyonların devamlılığını sağlayacak yordamlar içeren bilgi güvenliği politikası, ilgili mimarinin bir parçasını oluşturmaktadır.

Fedwire güvenliği sağlamak için çeşitli güvenlik araçları kullanmaktadır. Bu araçlar mantıksal erişim kontrolleri, şifreleme, gün sonu kıyaslamaları, kullanıcı kodu çalışma istasyonu tutarlılığı, off-line (çevrimdışı) işlemlerin iki taraflı kontrolü, mesaj sorumluluğu ve değişim kontrollerini içermektedir.

Fedwire katılımcıları, fedwire ile iletişim kurdukları iç sistemlerin güvenliğinden sorumlu tutulmaktadır. Fedwire sistemine doğrudan erişen katılımcılar için erişmelerinin şifre ve tanımlayıcı kod ile sağlanması, gönderilen mesajların şifrelenmesi, güvenlik yordamlarının dokümente edilmesi söz konusudur. Yerel bir güvenlik yöneticisi, katılımcının bağlantıyı sağlayan sistemindeki güvenlik ayarlarını yapmak için katılımcı tarafından belirlenmektedir.

Fedwire sisteminde mesaj şifreleme dışında, mesaj merkez sisteme ulaştığında giriş tarihi, giriş sıra numarası ve geldiği terminal bilgileri mesaj bilgisiyle birlikte tutulmaktadır. Mesaj katılımcı tarafından alındığında, tarihin doğruluğu, sayının beklenen sıra numarasından büyük olmadığı, terminal bilgilerinin geçerliliğinin de kontrolü yapılarak mesajın doğruluğu saptanmaya çalışılır. Kontrolleri geçemeyen mesaj alıcısına geri gönderilir.

Fedwire sisteminin %99.85 oranında bir bir çalışır konumda olma istatistiği bulunmaktadır.

Düzenli olarak iş sürekliliği testleri yapılmaktadır. Fedwire, 3 veri merkezi ile çalışmaktadır. Biri ana veri merkezi, diğeri ana merkezin anlık olarak kopyalandığı yedek merkez, üçüncüsü ise kopyalamaların anlık yapılmadığı 2. yedek merkezdir. Tüm merkezlerin arasında yüzlerce millik mesafeler bulunmaktadır. Acil durumlarda ya da istendiğinde 1. yedek merkezin çalışmaya başlaması en fazla 30 dakika içinde gerçekleşmektedir. 2. yedek merkeze günlük loglar ve veri tabanı değişiklikleri dosyalarla iletilmektedir. 3. merkezin amacı acil durumda ya da istendiğinde aynı gün içerisinde sistemin 3. merkezden ayağa kaldırılmasıdır. Her merkezde normal akışta ve olağan dışı durumlarda hizmet verebilecek kapasitede personel bulundurulmaktadır. Ana merkez için yılda 4-6, yedek merkezler için ise 4 test gerçekleştirilmektedir. Aynı zamanda fedwire iç ve dış olmak üzere çeşitli denetimlerden geçmektedir.

Fedwire sisteminin yıllar ve aylar bazında çalışırılık oranları Tablo-5 ile gösterilmiştir. Sistemin en düşük çalışırılık oranına 11 Eylül saldırıları nedeniyle ulaştığı görülmektedir.

Tablo 5 – Fedwire Sistemi Yıllar Bazında Çalışırılık Oranları

Ay/Yıl	1997	1998	1999	2000	2001
Ocak	%99.85	%100	%100	%100	%100
Şubat	%100	%100	%100	%100	%100
Mart	%100	%100	%100	%100	%100
Nisan	%100	%100	%100	%100	%100
Mayıs	%100	%100	%99.88	%100	%99.84
Haziran	%100	%100	%99.86	%100	%100
Temmuz	%99.92	%100	%99.93	%100	%100
Ağustos	%100	%100	%100	%100	%100
Eylül	%100	%100	%100	%100	%97.85
Ekim	%100	%100	%100	%100	
Kasım	%100	%100	%100	%100	
Aralık	%100	%100	%100	%100	
Ortalama	%99.98	%100	%99.97	%100	

Tablo-6 Fedwire sistemindeki kesintilerin detaylarını göstermektedir. Görülmektedir ki çoğu kesinti bilgi teknolojileri sistemlerindeki sorunlardan kaynaklanmıştır.

Tablo 6 – Fedwire Sisteminde Kesintilerin Detayları

Tarih	Süre (dk.)	Sebep
09.01.1997	19	Bir iş, güvenlik veritabanına erişimi kısıtlamıştır
01.07.1997	11	Veritabanı bir hata nedeniyle durmuştur
25.05.1999	25	Otomatik başlaması gereken bir işte sorun olmuştur
14.06.1999	34	Bir yazılım problemi veritabanının açılmasını engellemiştir.
27.07.1999	14	Yanlışlıkla çalışan bir iş, uygulamaları durdurmuştur.
30.07.1999	2	Yanlışlıkla çalışan bir iş, uygulamaları durdurmuştur.
14.05.2001	39	Terminallerdeki sistem tanımlarının değişmesi nedeniyle bir kaç iş normalindeşinde durmuştur.
12.09.2001	65	Taşan çalışma saatleri nedeniyle problemler olmuştur.
13.09.2001	230	11 Eylül nedeniyle problemler olmuştur.
14.09.2001	173	Sistemin geç açılması nedeniyle sistem çalışmamıştır

11 Eylül saldırılarından Fedwire ve CHIPS sistemleri merkezleri Aşağı Manhattan'da olmadığı için doğrudan etkilenmemiştir. Fakat katılımcılarının etkilenmesi sistemleri etkilemiştir. Asıl ve yedek merkezlerin çok yakın konumda olması ve iki sistemin birden zarar görmesi katılımcıların sıkıntıya sokan durumların başında gelmiştir (Institute for security technology studies at dartmouth college ,2003 :14).

6.3.3 SIC – İsviçre

SIC güvenlik paketinin güçlendirmek için çalışmaların sürdüğü, sistemin 15 yıldan uzun bir süreden beri bir saldırıya uğranmadığı, 1999 yılında bir güvenlik paketinin SIC bünyesine dahil edildiği, testlerin düzenli olarak yapıldığı FSAP raporlarında ifade edilmiştir (IMF,2002: 66).

6.3.4 PNS- Fransa

Sisteminin 3 farklı platformu bulunmaktadır. Platformlar arası iletişim için farklı iletişim protokolleri mevcuttur. Sistemler karmaşıklıkları nedeniyle, teknik hatalara karşı kırılgandırlar. 2001 ve 2002 yıllarında teknik sorunlar ortaya çıkmış ve bir tanesinin giderilmesi uzun zaman almıştır. Yeterli uzaklıkta yedek merkezler bulunmakta ve sistem testleri düzenli olarak yapılmaktadır. SWIFT ve telefon gibi iletişim ağlarının ve merkezlerin çalışmadığı durumlarda floppy disklerle verinin taşınarak kritik mutabakatların gerçekleşmesini sağlayacak “Plan de Secours de Place” senaryosu bulunmaktadır. Veri bütünlüğünü sağlayacak önlemler alınmıştır. Firewall ile sistemler korunmaktadır. Yeni geliştirilen yazılımların kalitesi ölçülmekte, yeni sürümler test edilmektedir. Sistemin çalışabilirliği Mayıs 2001 ve Mayıs 2004 arası %99.94 oranındadır. Fransa ödeme sistemi için verilen bilgiler ve sistemlerin incelenmesi sonucunda FSAP Fransa raporunda, sistemin sadeleştirmeye çalışılması, bu doğrultuda gereksiz işlevlerin ayıklanması tavsiye edilmiştir (IMF,2005)

6.3.5 SBLE – İspanya

SBLE sisteminin bilgi teknolojileri alt yapısı, Banco de España (BE) tarafından hazırlanan güvenlik politikasını kullanmaktadır. Sistemdeki tüm olayların kaydı, izlenmesi ve analizi gerçekleştirilmektedir. İletişim kanalları şifrelenmekte ve sistem firewall aracılığı ile korunmaktadır. Sistemin 2005 yılı ağustos ayına kadarki dönemde çalışırılık oranı %99.94 olarak ölçülmüştür. Sistem iç ve dış denetimlere tabi tutulmaktadır. 2 saatten daha az bir sürede yedek merkezi ayağa kaldırmak mümkündür. Sistemde büyük çaplı bir bilişim sorunu oluşmamıştır. Düzenli testlerle sistem sınanmaktadır. Sistemde çıkacak sorunları aşmak için programcılar sürekli iş başındadırlar ve sorunları 15 dakikadan az sürede çözmek üzerine geliştirilmektedirler. İspanya ödeme sistemi için verilen bilgiler ve sistemlerin incelenmesi sonucunda FSAP İspanya raporunda, sistem göçmelerindeki yordamların daha net biçimde tanımlanması gerektiği ve katılımcıların iç testlerine ilişkin eksikliklerin bulunduğu ve BE'nin katılımcıların bilgi teknolojileri altyapılarını operasyonel riskleri ortadan kaldırmak amacı ile denetlemesi gerektiği belirtilmiştir. (IMF,2006).

6.3.6 CHAPS-İngiltere

Yaşanan birkaç problemin sistemin yüksek çalışırılık oranını düşürdüğü fakat sistemin 7. maddeye büyük oranda sağladığı ifade edilmiştir. (IMF,2003c :82).

2005 yılında CHAPS %99.95 lik bir çalışırılık oranına sahip bulunmaktadır. Yaşanan iki büyük sorundan biri 20 dakika diğeri 1.5 saat süresince sistemin çalışamamasına neden olmuştur. Ülkedeki diğeri bir ödeme sistemi olan Protected Payments System

(PPS) 7 Temmuz 2005'deki bombalı saldırılardan ana merkezinin etkilenmesi üzerine, yedek merkezinden çalışmalarını problemsiz sürdürmüştür. (BoE,2005)

6.3.7 POS-Finlandiya / BOJ-Net Japonya

POPS sisteminin tüm temel ilkelere uyumlu olduğu belirtilmiştir (IMF,2001:52).. FSAP kapsamında yapılan değerlendirmelerde BoJ-Net sistemi son derece güvenilir bulunmuştur. (IMF ,2003b).

6.3.8 TARGET

Avrupa Merkez Bankasının hazırladığı 2002, 2003 ve 2004 yılı TARGET raporlarından sistemlerdeki bilgi teknolojileri kaynaklı sorunlar derlenmiştir.

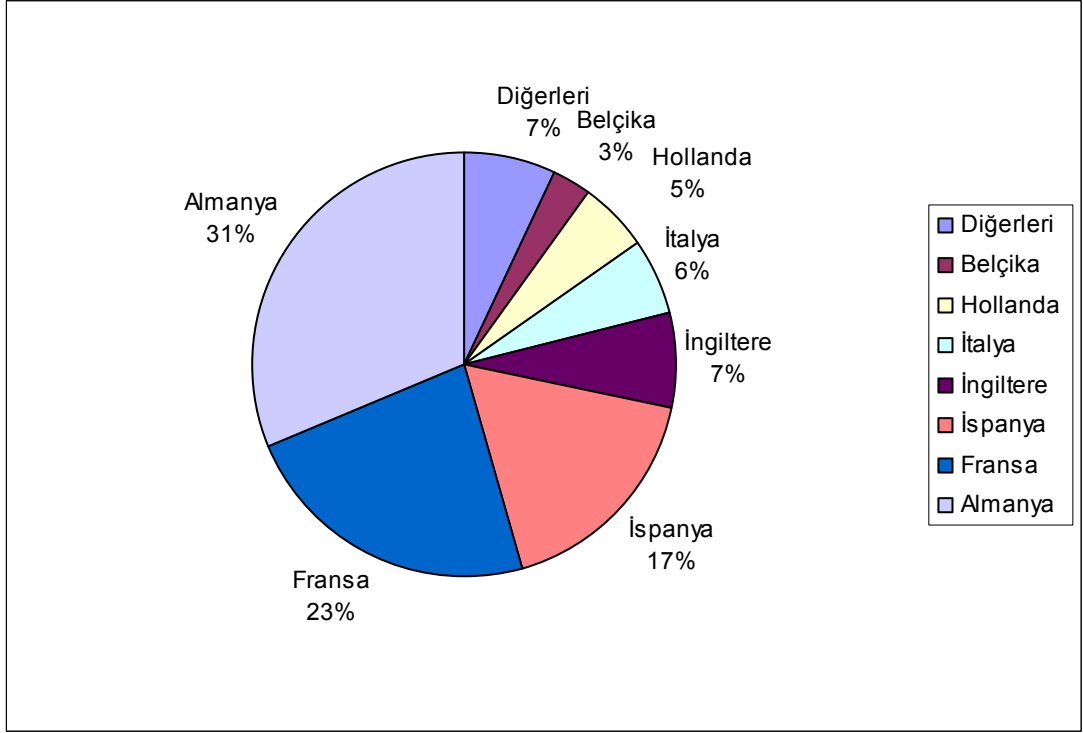
2004 yılı değerlendirmelerinde sistemin çalışırılık oranı %99.81 olarak elde edilmiştir. 20 Eylül 2004'te Bundesbank'ın yaşadığı bir yazılım sorunu nedeniyle Target sistemi 30 dakika geç kapanmıştır.

2003 yılı değerlendirmelerinde sistemin çalışırılık oranı %99.79 olarak elde edilmiştir. 11 Nisan 2003'te De Nederlandsche Bank'ın yaşadığı yazılım sorunu nedeniyle TARGET saat 19:00'da kapanmıştır. 1 Eylül 2003'de Sveriges Riskbank Banka tanımlama kodu (BIC) SWIFT veritabanından kazara silindiği için 3 saat boyunca adreslenememiştir. 15 eylül 2003'te Bank of England gönderilen TARGET mesajlarının onaylanmasıyla ilgili yazılım sorunu yaşamış, aşılması 4.5 saat sürmüştür. 30 eylül 2003'te De Nederlandsche Bank'ın yaşadığı donanım sorunu nedeniyle TARGET 19:00'da kapanmıştır.

2002 yılı deęerlendirmelerinde sistemin alıřırılık oranı %99.75 olarak elde edilmiřtir. 4 Ocak 2002'de Bank of England SWIFT'e baęlantı sorunu nedeniyle TARGET 18:30'da kapanmıřtır.18 Kasım 2002'de bir yazılım hatası Bank of England sisteminin 7 saat boyunca yavaşlamasına neden olmuřtur. 5 aralık 2002'de Bundesbank'ın yařadıęı yazılım sorunu bankanın eriřiminin kesilmesine, dolayısıyla TARGET sisteminin 19:00'da kapanmasına neden olmuřtur. 20 aralık 2002'de De Nederlandsche Bank'ın SWIFT networküne baęlanamaması TARGET sisteminin 20:00 de kapanmasına neden olmuřtur.

řekil-7 Avrupa Birlięi lkelerindeki RTGS sistemlerinin tutar bazında ulusal ve uluslararası alanda gerekleřtirdikleri demelerin 2003 yılı oranlarını gstermektedir. Grlmektedir ki, Almanya %31 oranıyla dięer lkelere aık ara bir fark yaratmaktadır. demelerin %71'i Almanya, Fransa ve İspanya tarafından yapılmıřtır. Bu  lke sonrasında Belika, Hollanda, İngiltere gelmektedir. Dięer lkelerin demeleri ise birleřtirilerek dięerleri bařlıęıyla sunulmuřtur.

Şekil 7 – AB Ülkelerinde Tutar Bazında Ulusal ve Uluslar arası Ödeme değerleri



Kaynak : (Iivarinen, 2004: 22)

Yüksek bir hacme sahip olan Fransa'nın ödeme sistemi, karmaşıklık nedeni ile riske açık bulunmuştur, en yüksek orana sahip Almanya'nın ödeme sisteminde yazılım sorunları yaşanmıştır. Bank of England'ın TARGET sisteminin çalışırılığının azalmasına neden olan sistem sorunlarının kaydına rastlanmaktadır. Hollanda'nın De Nederlandsche Bank adı altında hata kayıtları bulunmaktadır. Görülmektedir ki Avrupa ülkelerinde bile bilgi teknolojileri sorunlarına rastlanmaktadır. Gelişmekte olan ve az gelişmiş ülkelerin ödeme sistemlerinde daha fazla bilişim riskine rastlanması olasıdır.

YEDİNCİ BÖLÜM

7 ÖDEME SİSTEMLERİNİN GELECEĞİ

Farklı ödeme sistemlerinin incelenmesi ile de görülmektedir ki ödeme sistemlerinde pek çok farklı yaklaşım, pek çok farklı çözüm söz konusudur. Bu çeşitlilik nedeni ile ödeme sistemleri endüstrisinde pek çok değişikliğin olacağı da aşıkardır.

Bu değişiklik seçenekleri açık olmakla birlikte, bir takım öne çıkan yaklaşımlar gözlenmektedir. Bütünleşme süreci sürmektedir ve bu bütünleşme hem büyük meblağlı hem de küçük meblağlı ödeme sistemlerinin birleşmesine liderlik edecektir. Birleşme ve bütünleşme sonrasına daha az ödeme sistemi, fakat bu sistemlerde işlenen daha fazla mesaj sayısı ve daha fazla hacim olarak yansıyacaktır. Bu büyük sayılarsa gözetimin önemini arttıracaktır. (Iivarinen, 2004:46).

Büyük ve küçük ödeme ayrımları silinirken ödeme türlerine göre kategorize edilmiş ve özelleşmiş sistemler söz konusu olacaktır (örneğin bankalar arası ödemeler TARGET2, FX ve CLS, müşteri ödemeleri ACH; PEACH) (Iivarinen, 2004:46).

Globalleşme ve ekonomik entegrasyonun ödeme sistemleri alanına pek çok etkisi olmaktadır ve bu etki varlığını arttırarak devam ettirecektir. Sınır ötesi banka birleşmeleri arttıkça yeni ihtiyaçlar söz konusu olmaya başlayacaktır. Birleşmeler sonucu pek çok ülkede işlem yapan bankalar, pek çok ülkede eş zamanlı çalışacak operasyonel maliyetlerini düşürecek ödeme sistemleri çözümlerine ihtiyaç duymaya

başlayacaktır. Burada ihtiyacı cevaplayacak olan yine ödeme sistemlerinin uluslararası olması ve bütünleşmesidir (Iivarinen, 2004).

Avrupa Birliği'nde düzenleyici ortamın hızla değişmesinin ödeme sistemlerine etkisi söz konusudur. Önemli değişimlerden biri de “Basel Capital Accord –II”¹³ önerisidir. Sermaye elverişliliği gereksinimleri için bu yeni genel çerçeve ödeme sistemlerini de kapsamaktadır. Bu çerçeve bankaların operasyonel risklerini sermaye yeterliliği alanında kapsayacak şekilde tasarlanmıştır. Ödeme ve mutabakat sistemlerindeki risklere genel olarak operasyonel riskler gözüyle bakılmıştır. Bu bağlamda ödeme sistemlerinde operasyonel riskler hakkında daha fazla bilgi ve denetim kavramlarına vurgunun yapılacağı görülmektedir (Iivarinen, 2004:47).

Avrupa Komisyonu tarafından öne sürülen bir başka düzenleme değişimi ise Avrupa birliği için yasal bir çerçeve hazırlamaktan geçmektedir. Bu yeni çerçevenin tüm alanda yasal temelleri harmanlaması beklenmektedir. Sözü edilen çaba, alan içindeki tüm ödeme sistemlerine yeni gereksinimler doğuracak ve sistemlerin yapılarının yeniden şekillenmesi gerekecektir (Iivarinen, 2004:47).

Bilişim teknolojilerindeki daha sade, etkin ve güvenli ödeme sistemleri sağlayan hızlı değişim gelecekte de ödeme sistemleri üzerindeki etkisini sürdürmeye devam edecektir. Örneğin ağ teknolojileri ödeme sistemlerini daha gerçek zamanlı ve etkin kılarken yeni şifreleme teknikleri güvenliği arttırmaktadır. Yeni teknolojiler modüler

¹³ Basel Capital Accord – II için daha detaylı bilgiye Basel Committee on Banking Supervision tarafından hazırlanan The New Basel Capital Accord raporundan , rapora ise <http://www.bis.org/publ/bcbsca03.pdf> adresinden erişilebilir.

düzenleme imkanları ile sistemlerin yeniden yapılandırmasını kolay kılmaktadır. Bu da yeni tasarımlar yapmayı, eski tasarımları elden geçirmeyi kolaylaştırmaktadır (Iivarinen, 2004:47). Ödeme sistemlerinde bilgi teknolojileri kullanılarak sunulan çözümler daha da artacaktır. Sistemlerin bütünleşmesi ile birlikte kullanılan donanım ürünlerinin kapasitesinin artması gündeme gelecektir.

Avrupa Birliği'ne 2004 yılındaki yeni katılımlar mevcut ödeme sistemleri üzerinde baskı oluşturmuştur. Yeni katılımcılar mevcut ödeme sistemlerini kullanmak yerine (ki çoğu örnekte modern sistemler söz konusudur) Avrupa Birliği ortamına daha iyi uyan yeni ödeme sistemleri sahibi olmayı isteyebilirler. Bu durumda Avrupa Birliği'ndeki tüm ödemeleri kapsayacak etkin ve güvenli sistemlere ihtiyaç duyulacaktır. Bu ihtiyaç merkez bankalarını ve bankaları teknolojik bilgi açısından geride bırakacak yeni ürün sunacak yeni aktörlerin doğmasına olanak sağlayacaktır. Pazar daha harmanlandıkça farklı sistemler arasındaki rekabet artacak ve en sonunda konsolide sistemlerin oluşmasına önderlik edecektir.

7.1 Ulusal Sistemlerden Uluslararası Sistemlere Geçiş

Ülkeler arası ticari işlemlerin artması, piyasalar arasındaki sınırların yok olması ile ülkeden ülkeye yapılan ödemeler artmaktadır. Bahsi geçen artış ödeme sistemlerinin artan bir hızla globalleşmesine, ulusal ve uluslararası sistemler arasındaki ayrımların silinmeye başlamasına zemin hazırlamıştır. Bu süreçte güvenlik ve işlem hızını arttıracak standartlar, uçtan uca tümüyle elektronik süreçleri karşılayacak etkin otomasyon süreçleri söz konusu olmalıdır. Bilişim Teknolojileri bu süreçlerin

sağlanmasına olanak verirken veri işleme saklama ve telekomünikasyonda maliyetlerin düşürülmesini de sağlamaktadır.

Ulusal ödeme sistemleri ve uluslararası ödeme sistemlerinin bütünleşmesi sürecinde farklı yaklaşımlar sözkonusu olabilmektedir :

Farklı ulusal standartlar arası dönüştürme :

Ulusal sistem ve standartların kullanıldığı bu yöntemde, yerel işlemlerde ulusal standartlar kullanılmakta, global işlemlerde ise iletişimin sözkonusu olacağı sistemin standartına dönüştürme yapılmaktadır. İletişim halinde olunacak her sisteme dönüşümün sağlanabilmesi sistemin gereklerindendir. Oldukça maliyet içeren bu yöntem ödeme/bankacılık endüstrilerinin koordinasyonu sağlayamadığı durumlarda kullanılır.

Ulusal standartların genel bir standarda dönüştürülmesi:

Ulusal sistem ve standartların kullanıldığı bu yöntemde, yerel işlemlerde ulusal standartlar kullanılmakta, global işlemlerde ise genel standarda dönüştürme yapılmaktadır.

Tüm ulusal sistemlerde aynı standartları kullanma:

Ulusal sistemlerin kullanıldığı bu yöntemde, yerel ve global işlemlerde genel bir standart kullanılmakta dönüşüm söz konusu olmamaktadır.

Ulusal sistemleri tek bir genel sisteme entegre etme :

Ulusal sistemlerin kullanılmadığı bu yöntemde, tek bir genel sistem söz konusudur

7.2 E-Mutabakat

Ödeme sistemleri gerçek zamanlı işlem ve dağıtık ağ teknolojilerince simüle edilen oldukça hızlı ve temel değişikliklere doğru ilerlemektedir. İnternet ve elektronik ticaret ödeme sistemlerinin geleceğinde önemli bir etkiye sahip olacaktır. Kullanıcı talepleri ve rekabet gelişmeleri tetikleyecektir. Ödeme sistemleri kağıt tabanlı yapıdan ağ tabanlı çözümlere doğru kayacaktır (Leinonen vd., 2002:3).

Ödeme sistemleri birinci adım olan kağıt ortamından elektronik ortama geçişi gerçekleştirmiştir. Şimdi sırada etkinliği, sunulan servislerin kalitesini arttırmak için ödeme sistemlerinin yeniden mühendislik aşamasını katetmesi bulunmaktadır. Bu süreç için kilometre taşları

- ✓ Modern ağ-tabanlı gerçek zamanlı süreçlerin olanakları
- ✓ Açık ve uluslararası hesap numarasına dönüşümün sağlanması
- ✓ Dağıtık bankalararası mutabakat sistemlerinin yararları

olarak sıralanabilir (Leinonen, 2002:29).

Yeni telekomünikasyon teknolojileri - TCP/IP tabanlı ağlar, PKI gibi güvenlik araçları, donanım güvenlik modülleri, gerçek zamanlı işlemler, düşük maliyet, etkin sunucu donanımları, yeniden mühendislik süreçlerinin zeminini oluşturacaktır. Bilgi teknolojileri de yeniden mühendislik çalışmalarında oldukça önemli yer tutacaktır.

Yeniden mühendislik çalışmaları kapsamında yeni bir kavram olan E-mutabakat ortaya atılmıştır.

Elektronik mutabakat (E-mutabakat) mevcut mutabakat yapılarıyla karşılaştırıldığında oldukça değişik ve yeni bir konudur (Leinonen vd., 2002:3). Finlandiya Merkez Bankası tarafından tanıtılan Elektronik Mutabakat bankalararası mutabakat sistemini geliştirmek için sunulmuş bir çözümdür. (Proje 2001 kasım ayında başlamış, gereksinimler 2002 şubat ayında prototip ise 2002 mayıs ayında sunulmuştur. 2002 yazı boyunca prototip üzerinde entegrasyon ve test çalışmaları tamamlanmış ve ön gösterim ağustos 2002 de hazır hale getirilmiştir (Leinonen vd., 2002:5). Bankaların ödeme sistemleri ile tümüyle entegre olmuş dağıtık bir yapı üzerine temellendirilmiştir. Ana düşünce merkez bankası parasının ve mutabakat bilgisinin bankalararası ödeme mesajının şifrelenmiş sayısal damga “stamp” olarak iletilmesidir. Bu modelde gelecek nesil ödeme sistemlerinin internet/e-posta yaklaşımı ile ödeme mesajlarının gönderen bankadan alıcı bankanın hesap/ödeme sunucusuna merkezi yapıya uğramadan gönderilmesi söz konusudur. Bu yaklaşımla doğrudan erişim sözkonusu olduğu için ödeme sistemleri daha etkin ve hızlı olacaktır.¹⁴

¹⁴ Bilgiler Bank of Finland web sitesinden derlenmiştir.

Günümüzde herkes ağılar aracılığıyla birbiri ile bağlantılı durumda bulunmaktadır. İnternet ve e-posta ile değişik türlerde mesajlar gerçek zamanlı olarak gönderilebilmektedir. Fakat ödeme sistemleri bu olanaktan yoksundur İnternetin dağıtık ağ anlayışının ödemelere yansıtıldığı , SWIFTnet gibi TCP/IP tabanlı güvenli ağların kullanıldığı, uçtan uca otomatize süreçlerle mesajların mutabakat merkezlerine uğramadığı bir yapı ile ödeme sistemleri de bu yapıya kavuşturulabilir. Bu yapıda ağ, mesajları e-postaların yönlendirildiği biçimde alıcılarına iletecektir. Modern ağ tabanlı ya da geleneksel sistemlerde mesajları etkin bir biçimde yönlendirebilmek için sistemdeki herhangi bir hesabın adresini açıkça belirleyecek uluslararası hesap tanımlama standardına gereksinim duyulmaktadır. Bu yaklaşım e-posta adreslerine ya da kısa mesajların yönlendirilmesi sisteminde kullanılan GSM-telefon numaraları ile kıyaslanabilir. IBAN (international Bank Account Number) uluslararası hesap numarası standardını oluşturmaktadır. Eğer tüm bankalar IBAN standardında hesap numaralarına dönüşümü sağlarsa ödeme kolaylıkla alıcıya yönlendirilebilecektir (Leinonen, 2002:29-30).

Ağ yapısı dağıtık olmakla beraber bağımsız birimlerin arasında telekomünikasyon ile köprüler kurulmaktadır. Bu köprüler aracılığı ile mesaj transferleri ve bankalar arası mutabakat iletilmektedir. Ve bu da diğer ödeme sistemleri yaklaşımlarından farkı oluşturmaktadır. Dağıtık ağ yapısında etkinliğin sağlanması için mutabakat sistemi de dağıtık olmalıdır. E-mutabakat sistemi bankalar arası mutabakatlarda yeni otomatize ve elektronik olanakları da beraberinde getirmektedir.

E-mutabakat çözümü yöntemi gelecek nesil ödeme altyapısının bir parçası olarak görülmelidir.

- İnternet üzerinde e-ticaret
- Gerçek zamanlı güvenlik ve para piyasası işlemleri ve transferleri
- Mobil ödemeler (GSM tabanlı yakın zamanda UMTS-tabanlı)
- Uluslararası işlem hacmi

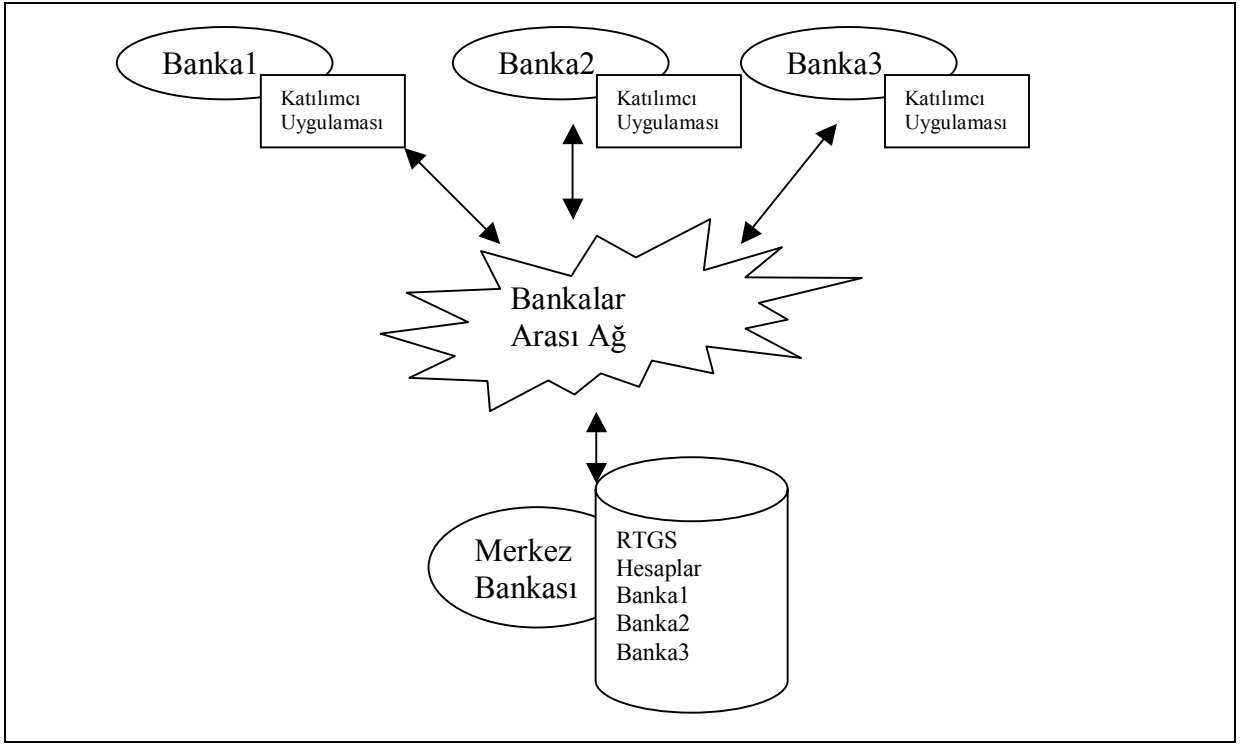
E-mutabakat günümüz sistemlerine entegre edilebilecek bir çözüm sunmaktadır. E-mutabakat damgası “stamp” her bir ödeme mesajına eklenmektedir. Bu damga merkez bankası parasını gönderenin bankasının hesabından alıcının bankasının hesabına aktarmaktadır. Damgalar güçlü ve modern kriptolama teknolojileri ile (örn. PKI) korunmaktadır. Ödeme sistemlerince yaratılıp şifrelenmektedirler. E-mutabakat sistemleri katılımcılara merkez bankaları tarafından sağlanmaktadır. Geleneksel RTGS sistemlerde bankaların mutabakat hesapları merkezi RTGS sisteminde tutulurken, e-mutabakat sistemlerinde bankaların kendi bünyelerinde merkez bankası kontrolündeki e-mutabakat modüllerinde bulundurulacaktır. Merkez bankası parasının elektronik formatta bankaların ödeme platformlarına taşınması e-mutabakat sisteminin önemli özelliklerindendir(Leinonen, 2002:30-31).

Mutabakat işlemleri için bankaların likiditeye ihtiyacı bulunmaktadır. Likidite e-mutabakat modülleriyle günbaşında merkez bankasından bankalara gönderilir. Gün içinde bu değer yeni gönderimlerle ya da banka ödemeleri ile arttırılabilir.

Günsonunda likidite merkez bankasına geri gönderilmektedir (Leinonen, 2002:30-31) .

Pratikte tüm RTGS sistemleri likidite yönetiminin, ödeme süreçlerinin ve veri saklamanın merkez bankalarının bünyesinde gerçekleştirildiği merkezileşmiş sistemleri kullanmaktadır.. Katılımcı bankalar RTGS sistem içindeki uygulamaları kullanarak merkezi sistem ile iletişim kurar. RTGS sistemin yapısına göre katılımcı uygulamaları RTGS sağlayıcı tarafından takdim edilebileceği gibi kendileri tarafından da geliştirilebilir. Güvenlik kontrolü (yazılım ve donanım bazlı) sadece yetkili kullanıcıların güvenli iletişim yapılarını kullanarak erişimini sağlar. Merkezileşmiş bir RTGS mutabakatında her bankanın merkezi RTGS hesabındaki likiditeyi kullanarak yapılmaktadır. Şekil-8’de bu yapı şematik olarak gösterilmektedir (Leinonen vd.,2002:18).

Şekil 8 - Merkezileşmiş RTGS sistemi

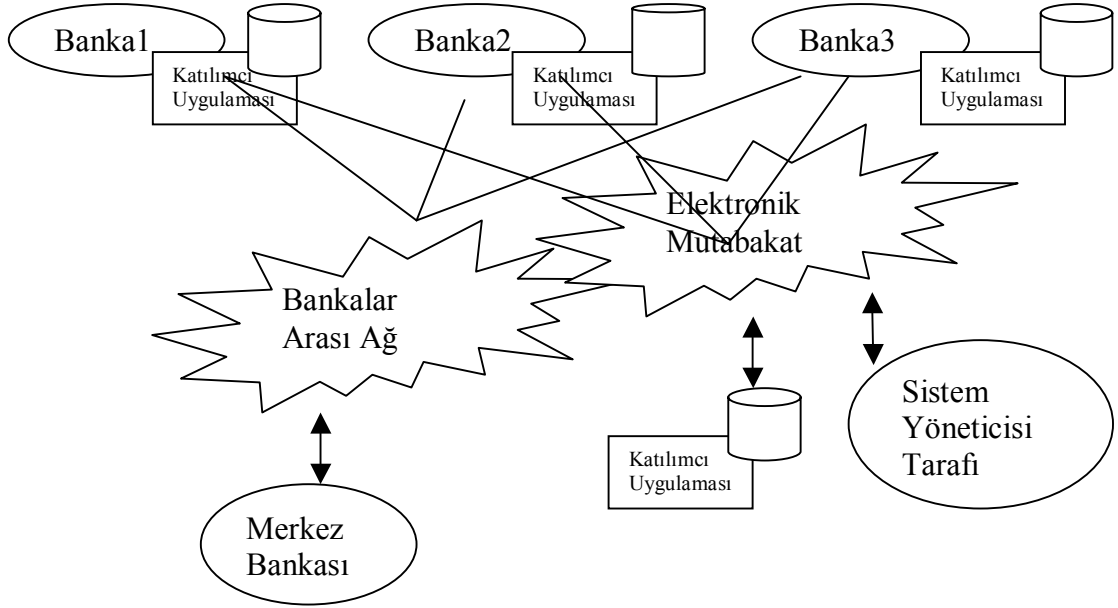


Kaynak: (Leinonen vd.,2002:18)

Dağıtık RTGS sistemi merkezi birim tarafından yönetilmekte ve kontrol edilmektedir fakat gün içi likidite yönetimi, ödeme süreçleri ve veri saklama işlevleri dağıtılmıştır. Bunu yapmanın bir yolu merkezi veritabanını her bankanın kendi bünyesinde kendi hesabıyla “küçük RTGS veritabanı” sahibi olmasıdır. Likidite bankaların hesabına gönderildiğinde, bankaların uygulamaları kendi aralarında mutabakatı doğrudan ve kesin bir biçimde gerçek zamanlı olarak gerçekleştirebilirler. E-mutabakat dağıtık RTGS sistemlerinde kullanılabilecek bir yapıdır. E-mutabakatın temel amacı standartlaşmış ve güvenli e-mutabakat modülleri ile süreçlerin dağıtılmasıdır. Modüller şifrelenmiş e-mutabakat damgaları “stamps” ile birbirleri ile doğrudan, merkezi birime ihtiyaç duymadan, mutabakat

gerçekleştirmektedir (Leinonen vd.,2002:18). Bahsi geçen yapının şekilsel gösterimi şekil-9’da sunulmaktadır.

Şekil 9 - E-mutabakat Sistemi



Kaynak : (Leinonen vd.,2002:18)

7.2.1 E-Mutabakatın Kazandırdıkları

7.2.1.1 Genel Kazanımlar

E-mutabakatın kazandırdıkları şu biçimde listelenebilir : (Leinonen vd., 2002:118)

- Mutabakat ödeme sürecinin bir parçası olarak gerçekleştirilir, mutabakat bilgisi ödemenin bir parçası olarak karşı tarafa iletilmesi.

- Mutabakat daha etkin bir biçimde gerçekleştirilmesi
- Ödeme sistemlerinin yeni ağ olanaklarını kullanacak biçimde yeniden yapılandırılması
- Sistemik riskin mutabakatın hemen yapılması ve likiditenin doğrudan kullanılması ile engellenmesi
- Likidite yönetimi ve ödeme likiditesinin tamamen banka tarafından yönetilen bir hesapta birleştirilmesi ile kolaylaşması
- Ödeme sürecinin doğrudan iki banka arasında gerçekleşmesi
- E-mutabakatın genel, tarafsız, otomatize ve standartlaşmış bankalararası mutabakat sistemi sunması
- E-mutabakatın otomatik mutabakat “reconciliation” ve hata yakalama çözümlerini barındırması
- E-mutabakatın ödeme sistemlerinde hızı arttırması, riski (mutabakat riski, kredi riski, operasyonel risk) düşürmesi
- Modern düşük maliyetli ve standartlaşmış teknolojiler kullanıldığı için değişik amaçlar için kullanım da söz konusu olması (örneğin bankalar arası dosya transferleri)
- Dağıtık yapı nedeniyle daha çok işlem hacmi gerçekleştirilebilmesi bunun da büyük maliyet düşüşlerini olanaklı kılması

7.2.1.2 Mevcut RTGS sistemlere göre kazanımları

Mevcut RTGS sistemlerle kıyaslandığında E-mutabakatın kazandırdıkları şu biçimde listelenebilir : (Leinonen vd., 2002:118)

- Merkezileşmiş hiçbir işlem ya da operasyonel maliyetin söz konusu olmaması
- Ödemelerin bankalar arasında doğrudan, merkez bankası hesaplarını kullanmadan, gerçekleştirilmesi
- E-mutabakatın ödeme sürecine yayılması (ödeme ve mutabakat mesajı ayırımına gerek kalmamıştır)
- Banka arayüzü için düşük maliyetli sunucuların yeterli olması
- Gelişmiş ve otomatize olmuş güvenlik sağlanması
- Daha az telekomünikasyon mesajı gönderilmesi ve alıcı banka arasında doğrudan ve uçtan uca kontrol sağlanması. E-mutabakat sistemleri mesajı göndermek için 2 mesajla yetinmektedir. (gönderilen ödeme ve confirmasyon mesajı) RTGS çözümleri ise bu işlem için iki ila dört arasında mesaja ihtiyaç duymaktadırlar (Biri ödeme mesajı diğerleri confirmasyon mesajları.)
- Daha etkin yedekleme ve olağanüstü durum çözümleri sunması

8 SONUÇ VE ÖNERİLER

Ödeme sistemleri, finansal işlemlerin globalleşmesi ve hacimlerinin artması ile birlikte daha da önem kazanmış ve yaygınlaşmıştır. Ödeme sistemlerinin öneminin artması ve yaygınlaşması ile birlikte, oluşacak risklerin etki alanı da artmış bulunmaktadır.

Ödeme sistemleri ekonomilerin vazgeçilmezi olmuşlardır. Her ekonomi için vazgeçilmez olan ödeme sistemleri uluslararası düzeyde, iletişim ağlarıyla bağlanarak daha büyük ödeme sistemlerini oluşturmaktadırlar. Bu vazgeçilmezlik ve bağlantılı durum, bir ödeme sisteminde oluşabilecek sorunun, ilgili ülkenin ekonomisine, sonrasında da bağlantılı olduğu bölgelerin ekonomilerine olumsuz etkilemesine yol açmaktadır. Bu nedenle ödeme sistemlerinde risklerin en aza indirilmesi ve mümkünse yok edilmesi konusunda önemli çalışmalar yapılmalıdır.

Ödeme sistemleri için kredi riski, likidite riski, sistemik risk, yasal risk ve operasyonel risk başlıkları altında risk irdelemesi yapılmaktadır. DNS sistemlerden RTGS sistemlere geçişle beraber kredi riski yerini likidite riskine bırakmıştır. Likidite riskinin ortadan kaldırılması için kuyruklama mekanizmaları, karma sistemler oluşturulması, sistem içinde kredi limitlerinin belirlenmesi gibi çözümler bulunmaktadır. Çözümlerin tamamı karmaşık bilgi işlem algoritmalarını ve yazılımlarını beraberinde getirmektedir. Dolayısıyla likidite tasarrufu yöntemleri de bilgi işlem riskini bünyesinde barındırmaktadır. Bu durumda DNS sistemlerden RTGS sistemlere geçişle birlikte kredi riskinin, likidite ve bilgi teknolojileri riskine (teknolojik değişiklik ve sunulan özellikler nedeniyle) kaydığı söylenebilir. Bu

nedenle, ödeme sistemlerinde bilgi teknolojileri risklerinin incelenmesine gerek duyulmuştur. Çalışmada, bu kapsamda öncelikle ödeme sistemleri tanımlanmış, sınıflandırılması yapılmış, önemi ve amaçları belirtilmiştir. Öneminin daha net ifade edilebilmesi için ödeme sistemlerinde işlem gören parasal büyüklüklere ilişkin değerler sunulmuştur. Sonrasında, ödeme sistemlerinin etkinliğinin gerekliliği, paranın dolaşım hızına etkileri, para politikalarına ve finansal istikrara katkıları incelenmiştir. Temel görevleri ile ödeme sistemlerinin yakından ilişkisi nedeniyle, ödeme sistemlerinin gözetimini üstlenen merkez bankalarının ödeme sistemlerindeki rolü değerlendirilmiştir. Çalışmada, ödeme sistemlerinin finansal dünyadaki ağırlığı vurgulanmaya çalışılarak, ödeme sistemlerinde oluşacak risklerin etkilerinin ne boyutta olabileceğinin belirtilmesi için bir alt yapı hazırlanmaya çalışılmıştır. Sonrasında ülkeler ve ödeme sistemleri örnekleri irdelenerek, ülkelerdeki farklı yapılardaki ödeme sistemleri tanıtılmıştır. Ödeme sistemlerine ve önemlerine ilişkin değerlendirme sonrasında ödeme sistemlerinde riskler değerlendirilmiş, bilgi teknolojileri riskleri detaylıca incelenmiştir. Ödeme sistemlerinin geleceği başlığı altında, beklenen ödeme sistemleri bütünleşmeleri, bütünleşmeler kapsamında ödeme sistemlerinin yenileneceği sonucuna varılmıştır. Açıklanan e-mutabakat kavramıyla, ödeme sistemleri için bilgi teknolojilerini daha da fazla içeren bir yaklaşım anlatılmıştır. Ödeme sistemlerinin geleceği başlığı altında, gelecekte bilgi teknolojilerinin ödeme sistemleri bünyesinde artarak kullanılmaya devam edeceği saptanmıştır.

Çalışma sonucunda şu sonuçlara ve önerilere ulaşılmıştır:

- Ödeme sistemleri, bilgi teknolojilerindeki kırılgan noktalar nedeniyle, kağıt tabanlı sistemlere oranla çok daha fazla riske açıktırlar.
- Ödeme sistemleri oldukça yaygın bir kullanıma ve güvenilirliğe ulaşmıştır. Ödeme sistemlerinde bilgi teknolojileri riskleri nedeniyle oluşacak bir sorun mevcut kullanılrlığı ve güveni azaltacak, ödeme sistemlerinin kullanımı yerine nakit kullanımının tercih edilmesine neden olacaktır.
- Bütün gelişmiş ülkelerde, merkez bankaları denetiminde kritik öneme sahip RTGS sistemler bulunmaktadır.
- RTGS sistemler bilgi teknolojileri risklerine daha açıktırlar.
- Bir katılımcıda oluşacak bilgi teknolojileri kaynaklı sorun, katılımcının işlemlerini gerçekleştirememesine, likidite sıkıntısı yaşamasına, katılımcıya güvenin aksamasına neden olabilecektir. Bu nedenle ödeme sistemi gözetimiyle görevli merkez bankaları, katılımcıların sistemlerini de denetlemelidir.
- Türkiye’de kullanılmakta olan sistem, RTGS ödeme sistemi türünün, erken örneklerindendir. Sistem, Türkiye Cumhuriyet Merkez Bankası öncülüğünde dünyadaki gelişmeleri takip etmekte, gelişmelere ayak uydurmakta ve ülke koşullarını değerlendirerek özel koşullara uygun çözümler sunmaktadır.
- Avrupa Birliği katılım sürecinde, Türkiye ödeme sistemi EFT’nin TARGET sistemine bağlantısı söz konusu olabilecektir. CLS’in yabancı para mutabakat riskini ortadan kaldırması ve sunduğu olanaklar göz önünde bulundurularak Türkiye’nin CLS sistemine üyeliğinin gündeme alınması gerekmektedir.

- Ödeme sistemleri kağıt ortamında yapılan işleri elektronik ortama aktararak birinci aşamasını tamamlamıştır. İkinci aşamada ise süreçlerin etkinliğini arttıracak yeniden mühendislik çalışmaları bulunmaktadır. Ülkemiz sistemi daha önce olduğu üzere yine erken örneklerden biri olacak şekilde bu süreci gerçekleştirmelidir.
- Uluslararası düzeyde SWIFT standartları yaygın olarak kullanılmaktadır. Türkiye ödeme sistemi bu standartları kullanmamaktadır. Ekonomimizin gelişmesi ve dış bağlantıların da artışı göz önünde bulundurularak, SWIFT standartlarının kullanımı ve uluslararası ödeme sistemleri ile bağlantı sağlanmasının faydalı olacağı düşünülmektedir.
- Türünün iyi örneklerinden sayılan TARGET sistemi ve BOJ-Net sistemi yeni nesil sistemler için çalışmalarını sürdürmektedir. Ödeme sistemleri, sürekli gelişerek değişecektir. Bu gelişmeler yeni bilgi teknolojileri ile sağlanan yeni çözümleri de bünyesinde barındıracaktır.
- Bütün önemli ödeme sistemleri, diğer temel ilkelere ilişkin gereksinimleri yerine getirirken, VII. maddeye ilişkin sıkıntılar bulunmaktadır. Bilgi teknolojileri riskleri üzerinde ulusal ve uluslararası düzeyde daha fazla çalışma yapılması gerekmektedir.
- Bilgi ve birikimlerin paylaşıldığı çeşitli forumlarda, bilgi alış verişinin sağlanması ve ödeme sistemleri etkinliklerine ağırlık verilmesi, merkez bankalarınca desteklenmelidir.
- Kurumlar prestijlerini yitirmemek için yaşanan sorunları dile getirmemeyi tercih etmektedirler. Sorunların dile getirilmesini sağlayacak yaptırımlar geliştirilmeli ve dünya genelinde bir sorun veritabanı oluşturulmalıdır.

- Bilgi teknolojilerinden kaynaklanabilecek pek çok risk bulunmaktadır. Ödeme sistemleri için bu riskleri ortadan kaldıracak güvenlik politikaları oluşturulmalı ve uygulandığı merkez bankalarınca denetlenmelidir.
- Ödeme sistemlerinin elektronik ortama tamamiyle geçmesi nedeniyle, işlemlerin elle gerçekleştirilmesinin imkanı neredeyse kalmamıştır. Bu nedenle, yedek sistemlerin ve olağandışı durum çalışmalarının yapılması bir zorunluluk olmuştur. Sistemler belirli zaman aralıklarıyla yedek merkezlerden çalıştırılmalı ve olağandışı durum senaryoları işletilmelidir.
- Bilgi teknolojileri risklerini ortadan kaldırmak oldukça maliyetli çalışmaları içermektedir. Hayata geçirilmesi planlanan çözümler için maliyet ve yarar analizleri iyi yapılmalı, gereksiz maliyetlerle sistem katılım ve işletim ücretleri arttırılmamalıdır.
- Sistemlerin iç ve dış denetimlerden düzenli olarak geçmesi sağlanmalıdır.
- Ödeme sistemlerinde bilgi teknolojileri risklerinin ortadan kaldırılması amacı ile ödeme sistemleri arasında kıyaslama (benchmarking) yapılmalıdır. Bu kıyaslamalar sırasında her sistemin ihtiyaçlarının ve özelliklerinin farklı olduğu gerçeği göz ardı edilmemelidir.
- Ödeme sistemleri konusunda uzmanlaşmış bilgi teknolojileri personeli yetiştirmek , sistemlerdeki risklerin azaltılmasında önemli bir etkiye sahiptir.
- Bilgi teknolojileri riski yaratma olasılığı olan ve bilgi teknolojilerindeki aksaklık nedeniyle sistemde sıkıntıya neden olan katılımcılara merkez bankalarının yaptırım gücü olmalıdır.

9 KAYNAKÇA

Akan, P. (2004).*Ödeme sistemlerinde risk yönetimi ve gözetim: Türkiye Cumhuriyet Merkez Bankası tarafından işletilen elektronik fon transfer sisteminin analizi*. Yayınlanmamış Uzmanlık Tezi, Türkiye Cumhuriyet Merkez Bankası.

Angelini, P. (1998). An analysis of competitive externalities in gross settlement systems. *Journal of banking and finance*, 22 (1), 1-18.

Bank for International Settlements (1997). *Real time gross settlement systems*. 9 Ekim 2005, <http://www.bis.org/publ/cpss22.pdf>.

Bank for International Settlements (2001).*Core principles for systemically important systems*. 8 Ekim 2005, <http://www.bis.org/publ/cpss43.htm>.

Bank for International Settlements (2003). *Payment and settlement systems in selected countries*. 10 Ekim 2005, <http://www.bis.org/publ/cpss53.pdf>.

Bank for International Settlements (2006). *Statistics on payment and settlement systems in selected countries – Figures 2004*. 30 Haziran 2006, <http://www.bis.org/dcms/fl.jsp?aid=6&pmdid=3&smdid=16&tmdid=30&fmdid=0&dtid=1&y=01012005&l=en>

Bank of England (2000). *Payment systems oversight*. 12 Şubat 2005, <http://www.bankofengland.co.uk/publications/psor/ops.pdf>

Bank of England (10.10.2005). *Bank of England*. 10 Ekim 2005, <http://www.bankofengland.co.uk>.

Bank of England (2005). *Payment systems oversight*. 10 Kasım 2005, <http://www.bankofengland.co.uk/publications/psor/psor2004.pdf>

Bank of Finland (2005). *Suomen Pankki – Finlands Bank – Bank of Finland*. 1 Kasım 2005, www.bof.fi.

Bank of Japan (10.10.2006). *Bank of Japan*, 10 Temmuz 2006, www.boj.or.jp/en.

- Barvell, K.(2002). *Risks and developments in payment systems*. 12 Şubat 2006, <http://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/barvell.pdf>.
- Centre for Latin American Monetary Securities (2000). *Payment and securities clearance and settlement systems in Argentina*. 20 Nisan 2006, http://www.forodepagos.org/pdf/report_argentina.pdf.
- Deutsche Bundesbank (1997). *Monetary policy and payment systems*. 12 Şubat 2006, http://www.bundesbank.de/download/volkswirtschaft/mba/1997/199703_mba_art02_monopay.pdf
- Ergin, O. (2001). *A.B.D.'deki büyük ölçekli ödeme sistemlerinin (FEDWIRE ve CHIPS) yapısı ve işleyişi ile merkez bankasının sistemdeki rolü*. Yayınlanmamış Rapor, Türkiye Cumhuriyet Merkez Bankası.
- European Central Bank (2002). *TARGET annual report*. 10 Temmuz 2006, <http://www.ecb.int/pub/pdf/other/targetar2002en.pdf>.
- European Central Bank (2003). *TARGET annual report*. 10 Temmuz 2006, <http://www.ecb.int/pub/pdf/other/targetar2003en.pdf>.
- European Central Bank (2004). *Assessment of euro large-value payment systems against the core principles*. 8 Temmuz 2006, <http://www.ecb.int/pub/pdf/other/assessmenteurolargevaluepayments2004en.pdf>.
- European Central Bank (2004a). *TARGET annual report*. 10 Temmuz 2006, <http://www.ecb.int/pub/pdf/other/targetar2004en.pdf>.
- European Central Bank (2005). *Overview of TARGET*. 30 Mart 2006, <http://www.ecb.int/paym/pdf/target/current/targetoverview.pdf>.
- European Central Bank (2006). *Payment and securities settlement systems in the european union and in the acceding countries*. 7 Temmuz 2006, http://www.bde.es/sispago/Addendum_BlueBook-ES.pdf.
- Federal Office for Information Security (BSI) (2005). *The IT-Security situation in Germany in 2005*. 26 Mart 2005, www.bsi.de/english/publications/securitysituation/lagebericht2005_englisch.pdf.

- Federal Reserve Newyork (2004). *Practices to assure telecommunications continuity for financial institutions and payment & settlements utilities*. 1 Temmuz 2006, <http://www.newyorkfed.org/prc/telecom.pdf>.
- Harri, L. (2001). *Payment and financial innovation, reserve demand and implementation of monetary policy*. 9 Mart 2006, <http://www.bof.fi/eng/>.
- Heinrich, G. (2000). *The Contribution of Payment Systems to Financial Stability*. 20 Nisan 2006, <http://www.bis.org/publ/cpss41.pdf>.
- Iivarinen, T. (2004). *Large value payment systems – principles and recent and future developments*. 20 Nisan 2004, www.bof.fi/eng/6_julkaisut/6.1_SPn_julkaisut/6.1.5_Keskustelualoitteita/0413.pdf
- Institute for security technology studies at Dartmouth College (2003). *Survey and analysis of security issues in the U.S. banking and finance sector*. 10 Temmuz 2006, <http://www.ists.dartmouth.edu/analysis/secfin0903.pdf>.
- International Monetary Fund (IMF) (2001) *Finland: Financial System Stability Assessment, including reports on the observance of standards and codes on the following topics: Financial policy transparency, banking supervision, insurance supervision, securities regulation, and payment systems*. 10 Temmuz 2006, <http://www.imf.org/external/pubs/ft/scr/2001/cr01214.pdf>.
- International Monetary Fund (IMF) (2002). *Switzerland: Financial System Stability Assessment, including reports on the observance of standards and codes on the following topics: Banking supervision, securities regulation, insurance regulation, payment systems, and monetary and financial policy transparency*. 10 Temmuz 2006, <http://www.imf.org/external/pubs/ft/scr/2002/cr02108.pdf>.
- International Monetary Fund (IMF) (2003a). *Germany: Financial System Stability Assessment, including reports on the observance of standards and codes on the following topics: banking supervision, securities regulation, insurance regulation, monetary and financial policy transparency, payment systems, and securities settlement*. 9 Temmuz 2006, <http://www.imf.org/external/pubs/ft/scr/2003/cr03343.pdf>.
- International Monetary Fund (IMF) (2003b). *Japan: Financial System Stability Assessment and supplementary information*. 10 Temmuz 2006, <http://www.imf.org/external/pubs/ft/scr/2003/cr03287.pdf>.

International Monetary Fund (IMF) (2003c). *United Kingdom: Financial System Stability Assessment including reports on the observance of standards and codes on the following topics: Banking supervision, insurance supervision, securities regulation, payment systems, monetary and financial transparency, securities settlement systems, and anti-money laundering and countering terrorist financing*. 10 Temmuz 2006 ,
<http://www.imf.org/external/pubs/ft/scr/2003/cr0346.pdf> .

International Monetary Fund (IMF) (2004). *Italy: Detailed assessment of compliance with the committee for payment and settlement systems (CPSS) core principles for systemically important payment systems, IMF country report no. 04/132*. 22 Mart 2006, <http://www.imf.org/external/pubs/ft/scr/2004/cr04132.pdf>

International Monetary Fund (IMF) (2005) . *France: Financial Sector Assessment Program— detailed assessments of observance of standards and codes including banking supervision, insurance regulation, securities legislation, monetary and financial policy transparency, payments systems, securities settlement, and anti-money laundering and combating the financing of terrorism*. 10 Temmuz 2006 ,
<http://www.imf.org/external/pubs/ft/scr/2005/cr05186.pdf> .

International Monetary Fund (IMF) (2006) . *Spain: Financial Sector Assessment Program – detailed assessment of the cpss core principles for systemically important payment systems*. 10 Temmuz 2006,
<http://www.imf.org/external/pubs/ft/scr/2006/cr06221.pdf> .

Johnson, E., Abrams, R., Destresse, J., Lybek, T., Roberts, N. & Swinburne, M. (1998). *Payment systems, monetary policy, and the role of the central bank*. Washington: International Monetary Fund.

Khiaonarong, T. (2003). *Payment systems efficiency, policy approaches, and the role of the central bank*. 22 Şubat 2006,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=444480.

Kirdaban, İ. (2005). *Ödeme sistemlerindeki gelişmeler ve ödeme sistemlerinin finansal sistem istikrarı üzerine etkileri*. Yayınlanmamış Uzmanlık Tezi, Türkiye Cumhuriyet Merkez Bankası.

Kuzu, Y. (2003). *Türkiye Cumhuriyet Merkez Bankası'nda uluslararası elektronik finansal iletişim ve yurt dışı ödeme sistemleri ile ilişkiler*. Yayınlanmamış Uzmanlık Tezi, Türkiye Cumhuriyet Merkez Bankası.

Leinonen, H., Lumiala, M. ve Sarlin R., (2002). *Settlement in modern network-based payment infrastructures*. 22 Şubat 2006,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=342361

Leinonen, H. (2000). *Re-engineering payment systems for the e-world*, Bank of Finland. 22 Şubat 2006,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=315000

Leinonen H. (2002). *Network-based payments and e-settlement- a long term perspective*. 19 Mart 2006 ,
http://www.bof.fi/eng/6_julkaisut/6.1_SPn_julkaisut/6.1.2_BOOf_bulletin/02b4.pdf

Lindley, R.(2002). Payment system risks. *E-money and payment systems review* içinde (77-109). London:Centralbanking.

Listfield, R.ve Negret, F. (1994). *Modernizing payment systems in emerging economies*. 2 Şubat 2006,
<http://ideas.repec.org/p/wbk/wbrwps/1336.html>

Manning, M. ve Willison M. (2006). *Modelling the cross-border use of collateral in payment systems*. 11 Şubat 2006,
<http://www.bankofengland.co.uk/publications/workingpapers/wp286.pdf> .

Mark, D. (2005). *IT investment: will the glory days ever return?* 25 Mart 2006,
<http://www.frbsf.org/publications/economics/letter/2005/el2005-13.pdf>.

Masha, I. (2002). Payment systems efficiency, monetary policy transmission and financial sector stability. *E-money and payment systems review* içinde (67-75). London:Centralbanking.

McAndrews, J. ve Trundle, J. (2001). *New payment systems designs: causes and consequences*. 10 Ocak 2006,
<http://www.bankofengland.co.uk/publications/fsr/2001/fsr11art3.pdf> .

Morten, L. ve Soramäki, K. (2001). *Gridlock resolution in interbank payment systems*. 10 Mayıs 2006,
http://www.bof.fi/eng/6_julkaisut/6.1_SPn_julkaisut/6.1.5_keskustelualoitteita/010

9mb.pdf

Okay, C. (2001). *Ödeme sistemlerinde ülkemizdeki durum ve dünyadaki gelişmeler*. 1 Mart 2006, <http://www.tbb.org.tr/turkce/gruplar/swift/CanBey-Turkce.pdf>

Okay, C. (2002). *Ödeme sistemleri*. 15 Mart 2006, <http://www.tcmb.gov.tr/yeni/evds/yayin/kitaplar/eurokitap/osim.doc>.

Okay C. (2004). *The Drivers of The Recent Payment Systems Reforms Globally*. 6 Temmuz 2006, <http://www.tcmb.gov.tr/research/cbreview/july04-3.pdf>.

Omonundee, G. ve Balino J. (1998). *Payment system reports and monetary policy , IMF*. 7 Şubat 2006, <http://www.imf.org/external/pubs/ft/fandd/1996/03/pdf/balino.pdf>.

Preneel, B. (1998). *Cryptographic primitives for information authentication*. 7 Nisan 2006, <http://www.cosic.esat.kuleuven.ac.be/publications/article-346.pdf>.

Pringlee, R. Ve Robinson, M. (2002). Introduction. *E-money and payment systems review* içinde (3-27). London:Centralbanking.

Sheppard, D. (1996). *Handbook* . 1 Ocak 2006, <http://www.bankofengland.co.uk/education/CCBS/handbooks/pdf/ccbshb08.pdf>.

SIA (01.07.2006). *SIA*, 1 Temmuz 2006, www.sia.ch.

Summers, B. (1994). *The payment system: design, management and supervision*. Washington, D.C. :International Monetary Fund.

SWIFT (01.03.2006) . *SWIFT* , 1 Mart 2006, www.swift.com .

The Central Bank of The Bahamas (2006). *Guidelines for electronic banking, supervisory and regulatory guidelines: pu23-0506*, 3 Temmuz 2006, <http://www.centralbankbahamas.com/public/E-Banking.pdf>.

The Eurosystem (2005). *The current target system*. 30 Haziran 2005, <http://www.ecb.int/pub/pdf/other/target2005en.pdf>

Türkiye Bankalar Birliği (04.04.2006). *Türkiye Bankalar Birliği*, 4 Nisan 2006, www.tbb.org.tr.

Türkiye Bankalar Birliği (1998). *Elektronik bankacılık ve elektronik para faaliyetleri için risk*. 30 Mart 2006, www.tbb.org.tr/turkce/basle/Electronic.doc

Türkiye Cumhuriyet Merkez Bankası (07.01.2006). *Türkiye Cumhuriyet Merkez Bankası*. 7 Ocak 2006, <http://www.tcmb.gov.tr/>.

Türkiye Cumhuriyet Merkez Bankası (2002). *Elektronik fon transfer sistemi ve elektronik menkul kıymet transfer sistemi*. 10 Ocak 2006, <http://www.tcmb.gov.tr/>.

Türkiye Cumhuriyet Merkez Bankası (2003). *Continuous link settlement (CLS) sistemi gerçekleştirilen çalışmalar*. Yayınlanmamış Rapor, Türkiye Cumhuriyet Merkez Bankası.

Türkiye İş Bankası (04.04.2006). *Türkiye İş Bankası*, 4 Nisan 2006, www.isbank.com.tr.

United States. Congress. Office of Technology Assessment. (1982). *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity*. 1 Temmuz 2006, http://govinfo.library.unt.edu/ota/Ota_4/DATA/1982/8223.PDF

United States General Accounting Office GAO (2004). *Knowledge of software suppliers needed to manage risks*. 30 Mart 2006, <http://www.gao.gov/new.items/d04678.pdf>.

Uzdil, P. (1997). Avrupa para birliđi sürecinde “TARGET ” projesi. *Bankacılar Dergisi*, 20.

Üstünel, B.,(1983). *Makro Ekonomi*. İstanbul : Mısırlı Matbaacılık.

Valerdi, R. Ve Kohl, R.(2004). *An approach to technology risk management*. 1 Temmuz 2006, <http://esd.mit.edu/symposium/pdfs/papers/valerdi.pdf>.

Vlatko, Č. (2000). *Internet economy and electronic commerce*. 25 Mart 2006, http://oliver.efzg.hr/~vlceric/publications/internet_economy_electronic_commerce.Pdf.

ÖZET

Ekonomik birimler arasında mal ve hizmetlerin değişimini kolaylaştıran araçları, kurumsal ve örgütsel çatıyı, işletim süreçlerini ve haberleşme ağını kapsayan ödeme sistemleri, finansal sistemin ve ekonominin etkin işleyişi için önem arz etmektedirler.

Küreselleşen dünyamızda finansal işlemlerin sayısı ve hacmi hızla artmakta, yapılan işlemler de küreselleşmektedir. Bu durum ödeme sistemlerinin daha yoğun ilgi görmesine ve merkez bankalarının önemli gündem maddelerinden biri haline gelmesine neden olmaktadır.

Ödeme sistemleri ekonominin can damarlarından biri haline gelirken, oluşabilecek risklerin yaratabileceği etkilerin boyutları da büyümektedir. Kredi riski, likidite riski, operasyonel risk, yasal risk, sistemik risk başlıkları altında incelenen risk gruplarının oluşmasını engellemek için merkez bankalarının bankası olarak bilinen Bank for International Settlement (BIS) bünyesinde çalışmalar yürütülmektedir. Bu kapsamda sistemik açıdan önemli ödeme sistemleri için temel ilkeler (Core Principles of Systemically Important Payment Systems:CPSIPS) Ocak 2001’de yayınlanmıştır. Ülkeler sistemik açıdan önemli ödeme sistemlerinin bu raporda belirtilen prensiplere uygunluğunu inceleyip, aksayan yönlerini gidererek risk oluşumlarını en aza indirmeye çalışmaktadırlar.

Gelişen bilgi teknolojileri ödeme sistemlerinin gelişmesinde önemli altyapıyı hazırlarken ödeme sistemleri için riskler de oluşturmaktadır. Operasyonel risk başlığı altında, CPSIPS raporunda VII. ilkede irdelenen bilişim risklerinin, en aza indirilmesi yönünde ilgili otoritelerce çalışmalar sürdürülmektedir.

Çalışma ödeme sistemlerinin önemini vurgulamak, ödeme sistemlerinin barındırdığı bilgi teknolojileri risklerini belirlemek ve bu risklerin ortadan kaldırılmasına yönelik öneriler sunmak amacı ile hazırlanmıştır. Bu kapsamda çalışmada ödeme sistemlerinin tanımı yapılmış, etkinliği değerlendirilmiş, çeşitli ödeme sistemlerinin yapıları irdelenmiş, ödeme sistemlerinin barındırdıkları bilgi teknolojileri riskleri genel olarak ve tanıtılan ödeme sistemleri bünyesinde incelenmiş, risklerin ortadan kaldırılması için önerilerde bulunulmuştur.

Anahtar Kelimeler: Ödeme sistemleri, CPSIPS, Bilgi teknolojileri Riskleri, EFT, E-mutabakat

Rumelili, Özlem Menekşe, Information Technology Risks in Payment Systems, Master's Thesis, Advisor: Assoc.Prof. Yalçın Karatepe, 148 p.

ABSTRACT

Payment systems containing tools that facilitates exchange of goods and services, institutional and organizational framework, telecommunication and communication network are important for efficient functioning of financial system and economy.

In our globalizing world, number and volume of financial transactions are enhancing and transactions are becoming global. As a result of this change, payment systems take more interest and place in central banks' agendas.

While payment systems are becoming vital points of the economy, the effects of possible risks are growing as well. For preventing risks studies are made in the Bank for International Settlement known as the bank of the central banks. Within this context, Core Principles of Systemically Important Payment Systems: CPSIPS is published at 2001.

After the CPSIPS report and the increased importance of the payment systems, central banks take an active role on the oversight. Payment systems are the main actors for the financial stability and monetary policies.

Developing information techonologies prepares an important infrastructure for development of the payment systems, at the same time they make the payment systems more vulnerable.

The aim of this study is to stress the importance of the payment systems, to determine the information technology risks arising from these systems and to propose solutions for alleviating these risks. In this context payment systems are described, efficieny of payment systems are evaluated, same payment system examples are given, information technology

risks exposed in payment systems are analyzed within introduced payment system in general, recommendations have been made to alleviate the risks.

Key Words : Payment systems, CPSIPS, IT Risks, EFT, E-settlement