



YILDIZ TEKNİK ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ

radio frekansı ile kimlik tanıma..:

Yüksek Lisans Tezi

burcu tuğaç



**YILDIZ TEKNİK ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ**

**RADYO FREKANSI İLE KİMLİK TANIMA**

207

**Elektronik ve Haberleşme Mühendisi Burcu TUĞAÇ**

**FBE Elektronik ve Haberleşme Mühendisliği Anabilim Dalı Haberleşme Programında  
Hazırlanan**

**YÜKSEK LİSANS TEZİ**

**Tez Danışmanı : Yrd. Doç. Dr. Aktül KAVAS**

**İSTANBUL, 2007**



YILDIZ TEKNİK ÜNİVERSİTESİ  
KÜTÜPHANE VE DOKÜMANTASYON  
DAİRE BAŞKANLIĞI

Yer No (DDC) : R-373-134

Kayıt No : 3576

Geldiği Yer : Fen Bil. Enst.

Tarih : 05.12.2007

Fiyat : 6,75

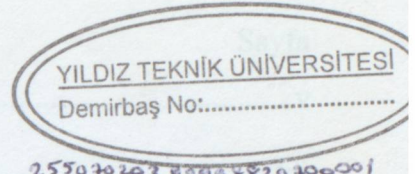
Fatura No : .....

Ayniyat No : 23

Ek : .....



YILDIZ TEKNİK ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ



XII-135

RADYO FREKANSI İLE KİMLİK TANIMA

Elektronik ve Haberleşme Mühendisi Burcu TUĞAÇ

FBE Elektronik ve Haberleşme Mühendisliği Anabilim Dalı Haberleşme Programında  
Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Yrd. Doç. Dr. Aktül KAVAS

*Kavas*

Yrd. Doç. Dr. ÜNAL KÜSÜK

Doç. Dr. Nurettin Umutkaya

İSTANBUL, 2007



# İÇİNDEKİLER

	Sayfa
KISALTIMA LİSTESİ .....	v
ŞEKİL LİSTESİ.....	vii
ÇİZELGE LİSTESİ .....	ix
ÖNSÖZ .....	x
ÖZET .....	xi
ABSTRACT.....	xii
1 GİRİŞ .....	1
2 OTOMATİK KİMLİK TANIMA SİSTEMLERİ.....	5
2.1 Optik Karakter Tanıma Sistemleri, Özellikleri, Avantajları, Uygulama Alanları .....	7
2.2 Biyometrik Kimlik Tanıma Sistemleri, Özellikleri .....	8
2.2.1 Biyometrik Kimlik Tanıma Sistemlerinin Avantajları .....	9
2.2.2 Biyometrik Kimlik Tanıma Sistemlerinin Uygulama Alanları.....	10
2.2.3 Biyometrik Tanıma Sistemi Çeşitleri .....	10
2.2.3.1 Yüz Tanıma Sistemi.....	11
2.2.3.2 Parmak İzi Tanıma .....	11
2.2.3.3 İris Tanıma .....	14
2.2.3.4 El Geometrisi Tanıma .....	15
2.2.3.5 Ses Tanıma.....	15
2.2.3.6 Retina Tanıma.....	15
2.3 Akıllı Kart Sistemleri Özellikleri.....	15
2.3.1 Akıllı kart Tipleri .....	17
2.3.1.1 Bellekli Kartlar, Özellikleri, Uygulama Alanları.....	17
2.3.1.2 Mikroişlemcili Kartlar, Özellikleri, Uygulama Alanları .....	18
2.3.2 Akıllı Kart Sisteminin Avantajları .....	21
2.3.3 Akıllı Kart Sisteminin Uygulama Alanları .....	21
2.4 Barkod Sistemleri, Özellikleri, Avantajları & Dezavantajları, Uygulama Alanları .....	22
2.5 RFID Sistemleri, Özellikleri, Avantajları & Dezavantajları, Uygulama Alanları .....	25
3 RFID SİSTEMLERİ .....	27
3.1 Tarihçesi.....	27
3.2 RFID Etiketler.....	28
3.2.1 Fonksiyonlarına göre RFID Etiketleri .....	29
3.2.2 Frekanslara Göre RFID Etiketleri.....	30
3.2.3 Bellek Tipine Göre RFID Etiketleri.....	31



3.2.4	Çipsiz RFID Etiketi .....	32
3.3	RFID Sisteminin Uygulama Alanları .....	32
3.4	RFID Sisteminin Güncel Uygulamaları.....	35
3.4.1	Pasaportlarda RFID Teknolojisi .....	35
3.4.2	Kopya DVD'ye Karşı RFID .....	36
3.5	RFID Sisteminin Gelecekteki Uygulamaları .....	37
3.6	RFID Sistem Seçimi İçin Kriterler .....	38
3.6.1	Doğru Frekansın Seçilmesi.....	39
3.6.2	Doğru Etiketin Seçilmesi.....	39
3.6.3	Doğru Okuyucunun Seçilmesi.....	40
4	RFID FREKANS BANDLARI .....	42
5	RFID SİSTEMLERİNİN YAPISI .....	46
5.1	RFID Sisteminin Haberleşme Yapısı.....	46
5.1.1	Okuyucunun İşlevi.....	47
5.1.2	Okuyucunun Tasarım ve Performansı .....	48
5.1.3	Etiket İşlevi.....	49
5.1.4	Endüktif Kuplaj -Pasif etiketlere güç kaynağı .....	51
5.1.4.1	Kuplaj Katsayısı k.....	51
5.1.4.2	Endüktans L .....	52
5.1.4.3	Karşılıklı Endüktans (M) .....	53
5.2	RFID Sisteminin Çalışma Prensibi .....	55
5.2.1	Alçak Frekansta Anten Parametrelerinin Hesaplanması .....	55
5.2.2	RFID Sistemlerinde Kullanılan Modülasyon Yöntemleri .....	61
5.2.2.1	ASK Modülasyonu : Genlik Kaydırmalı Anahtarlama (ASK).....	61
5.2.2.2	FSK Modülasyonu : Frekans Kaydırmalı Anahtarlama (FSK) .....	63
5.2.2.3	BPSK Modülasyonu : İkili Faz Kaydırmalı Anahtarlama (BPSK) .....	65
5.2.2.4	QPSK Modülasyonu : Çeyrek Faz Kaydırmalı Anahtarlama (QPSK) .....	66
5.2.3	RFID Sistemlerine Telekomünikasyon Kurumunca Getirilen Standartlar	67
6	RFID SİSTEMLERİNDE ÇÖZÜLMESİ GEREKEN SORUNLAR.....	71
6.1	RFID Sisteminde Standardizasyon .....	71
6.2	RFID Sistemlerinde Güvenlik .....	73
6.2.1	RFID Teknolojisinde Güvenlik ve Gizlilik için Önerilen Çözümler.....	74
6.3	RFID Sistemlerinde Çarpışma ve Çarpışma Önleyici Algoritmalar .....	76
6.3.1	Okuyucu Çarpışması.....	76
6.3.2	Etiket Çarpışması.....	77
6.3.3	Çarpışma Önleyici Algoritmalar.....	77
7	TEZ UYGULAMASINDA KULLANILAN DEMO KİT .....	79
7.1	Mifare Blok Tanımlaması.....	80
7.1.1	Fabrika Ayarı Bloğu .....	80
7.1.2	Veri Bloğu.....	80
7.1.3	Değer Blokları.....	83



7.2	Smrfid Mifare Yazılımı .....	83
7.3	Mifare Etiket Komutları ve İşlemleri.....	84
7.3.1	Etiket Seçme İşlemi .....	84
7.3.2	İşlemi Durdurma .....	85
7.3.3	Onaylama İşlemi .....	85
7.3.4	Okuma / Yazma İşlemi .....	86
7.3.5	Değer Okuma ve Değer Yazma İşlemi .....	87
7.3.6	Değer Arttırma ve Değer Azaltma İşlemi.....	88
7.3.7	Şifreleme .....	88
8	TEZ UYGULAMASI .....	90
8.1	Uygulama için geliştirilen yazılım.....	90
8.2	Kartlara Bilgilerin Girilmesi .....	112
8.2.1	Ondalık sayıyı Onaltılık Sisteme Çevirme: .....	112
8.2.2	Uygulama için Seçilen Rakamların Onaltılık Sistemdeki Karşılıkları ....	113
8.3	Ürün etiketlerine Veri yükleme .....	113
8.3.1	Birinci ürün kartına bilgi girilmesi .....	113
8.3.2	İkinci ürün kartına bilgi girilmesi .....	114
8.3.3	Üçüncü ürün kartına bilgi girilmesi .....	114
8.4	Kredi Kartlarına Veri Yükleme .....	115
8.4.1	Birinci kredi kartına bilgi girilmesi .....	115
8.4.2	İkinci kredi kartına bilgi girilmesi .....	117
9	YAZILIMIN ÇALIŞTIRILMASI VE YAPILAN RFID UYGULAMASI	120
9.1	Örnek Uygulama 1 .....	120
9.1.1	Birinci Ürünün Okuyucuya Okutulması .....	120
9.1.2	İkinci Ürünün Okuyucuya Okutulması .....	121
9.1.3	Kredi Kartından Harcamanın Düşülmesi.....	122
9.2	Örnek Uygulama 2 .....	123
9.2.1	Ürünün okuyucuya okutulması:.....	123
9.2.2	Kredi Kartından Harcamanın Düşülmesi.....	124
10	SONUÇ .....	127
	KAYNAKLAR .....	130
	EKLER.....	132
EK 1	ISO RFID Standartları (03.02.2005).....	132
EK 2	ISO RFID Standart Taslakları (03.02.2005) .....	134
	ÖZGEÇMİŞ .....	135



## KISALTMA LİSTESİ

ABD	Amerika Birleşik Devletleri
AES	Auger Elektron Spektroskopisi
API	Application Program Interface (Uygulama Program Ara yüzü)
ASK	Amplitude Shift Keying
ATM	Automatic Teller Machine
BAC	Basic Access Control
BMP	Bitmap
BPSK	Binary Phase Shift Keying
C#	Csharp
CCD	Charge Couple Device
CD	Compact Disc
CPU	Central Processing Unit (İşlemci)
DOC	Document
DoS	Denial of Service
DV	Decrement Value
DVD	Digital Versatile Disc
EEPROM	Electrical Erasable Programmable Read Only Memory (Elektriksel Silinebilir Programlanabilir ROM)
EPC	Electronic Product Code (Elektronik Ürün Kodu)
ETSI	European Telecommunications Standard Institute
FC	Faraday Cage
FSK	Frequency Shift Keying
GIF	Graphics Interchange Format
GSM	Global System for Mobile Communications (Mobil İletişim için Küresel Sistem )
HD-DVD	High Density Digital Versatile Disc
HF	High Frequency
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standards Organization
IV	Increment Value
LF	Low Frequency
LSB	Least-Significant Bit
MRAM	Magnetic RAM
MW	MicroWave
OCR	Optic Character Recongition (Optik Karakter Tanıma)
ONS	Object Name Service
OT/VT	Otomatik Tanıma / Veri Toplama
OTP	Output
PIN	Personal Identification Number
PML	Physical Markup Language
POS	Point Of Sale
PRF	Pseudo-Random Function
PSK	Phase Shift Keying
QPSK	Quadrature Phase Shift Keying



RAM	Random Access Memory	17
RF	Read Firmware	17
RF	Radyo Frekansı	17
RFID	Radio Frequency Identification (Radyo Frekanslı Tanımlama)	17
RV / WV	Read Value /Write Value	17
SIM	Subscriber Identity Module	17
SMRFID	Son Micro RFID (Yazılım programının adı)	17
TIF	Tagged Image File Format	17
TXT	Text File Format	17
UHF	Ultra High Frequency	17
WORM	Write Once Read Many	17
Sayı		
Sayı 1.1	RFID Sistemleri	19
Sayı 1.2	RFID Sistemleri	23
Sayı 1.1	RFID Sistemleri	23
Sayı 1.2	RFID Sistemleri	28
Sayı 1.3	RFID Sistemleri	28
Sayı 1.3	RFID Sistemleri	29
Sayı 1.4	Frekans Aralığı Mesafeler	30
Sayı 1.5	Yeterince okunabilir RF etiketleri	31
Sayı 1.6	Okunabilir yazılabilir RF etiketleri	31
Sayı 1.7	Etiket İçerik Dizaynı	32
Sayı 1.8	Radyo frekanslı kimlik tanıma sistemleri: Dilekçeleri	46
Sayı 1.9	RFID Okuyucu devre yapıları	49
Sayı 1.10	Okuyucu tarafından üretilen manyetik alan ile etiketler arasındaki ilişki	51
Sayı 1.11	1. Manyetik alanın oluştuğu alan	51
Sayı 1.12	İki bobinin oluşturduğu karşılıklı manyetik alan	54
Sayı 1.13	Manyetik alan şiddetinin mesafeye göre değişimi	57
Sayı 1.14	Manyetik alan şiddetinin alanın yarıçapına göre değişimi	57
Sayı 1.15	Çanak endüktansın mesafeye göre değişimi	58
Sayı 1.16	Kuplar kapasitansın mesafeye göre değişimi	58
Sayı 1.17	Manyetik alan şiddetinin frekansa göre değişimi	59
Sayı 1.18	Etiket ve Okuyucu Etkileşimi	60
Sayı 1.19	RFID Haberleşme Yapısı	60
Sayı 1.20	Sinusoidal sinyal modülasyonu (taşıyıcı ve yan bantlar)	61
Sayı 1.21	Mesaj (Bilgi) İsmareti ve ASK İsmareti	61
Sayı 1.22	ASK modülasyonunda ikili kod sinyali ile iki durumda mesajın gönderilmesi	62
Sayı 1.23	ASK modülasyonunun frekansları	63
Sayı 1.24	FSK İsmareti	63
Sayı 1.25	FSK modülasyonu	64
Sayı 1.26	2-PSK modülasyonunun frekansları	64
Sayı 1.27	BPSK İsmareti ve Üretimi	65
Sayı 1.28	QPSK İsmareti	65
Sayı 1.29	QAM modülasyonu (QPSK modülasyonu)	66
Sayı 1.30	9-125 kHz aralığında 10 mesajda üretilen manyetik alan sınır değerleri	70



## ŞEKİL LİSTESİ

	Sayfa
Şekil 2.1	Otomatik Kimlik Tanıma Sistemleri Auto- ID ..... 5
Şekil 2.2	Optik Karakter Tanıma Sistemi ..... 7
Şekil 2.3	Yüz Tanıma Biyometrik Sistemi ..... 11
Şekil 2.4	Parmak izi Tanıma Biyometrik Sistemi ..... 11
Şekil 2.5	Parmak izi Görüntüsü ..... 12
Şekil 2.6	Parmak izi tanımda görüntünün alınması..... 13
Şekil 2.7	Parmak izi tanımda görüntünün işlenmesi ..... 13
Şekil 2.8	Parmak izi tanımda görüntünün doğrulanması ..... 14
Şekil 2.9	Tipik Bellekli Kart Yapısı..... 17
Şekil 2.10	Tipik Mikroişlemcili Kart Yapısı..... 19
Şekil 2.11	Tipik Barkod Örneği ..... 23
Şekil 2.12	RFID Sistemi ..... 25
Şekil 3.1	RFID Etiketi..... 28
Şekil 3.2	RFID Çipi..... 28
Şekil 3.3	RFID Etiket yapısı ..... 29
Şekil 3.4	Frekans Aralığı Mesafeler..... 30
Şekil 3.5	Yalnız okunabilir RF etiket..... 31
Şekil 3.6	Okunabilir yazılabilir RF etiketler ..... 31
Şekil 3.7	Etiket İç Dizayn ..... 32
Şekil 5.1	Radyo frekans kimlik tanıma Sistem Bileşenleri..... 46
Şekil 5.2	RFID Okuyucu devre yapısı ..... 49
Şekil 5.3	Okuyucu tarafından üretilen manyetik alan ile endüktif kuplajlanan etiket..... 51
Şekil 5.4	"L" endüktansının tanımı ..... 53
Şekil 5.5	İki bobinin oluşturduğu karşılıklı endüktans ..... 54
Şekil 5.6	Manyetik alan şiddetinin mesafeye göre değişimi..... 57
Şekil 5.7	Manyetik alan şiddetinin anten yarıçapına göre değişimi..... 57
Şekil 5.8	Ortak endüktansın mesafeye göre değişimi ..... 58
Şekil 5.9	Kuplaj katsayısının mesafeye göre değişimi..... 58
Şekil 5.10	Manyetik alan şiddetinin frekansa göre değişimi ..... 59
Şekil 5.11	Etiket ve Okuyucu Etkileşimi ..... 60
Şekil 5.12	RFID Haberleşme Yapısı ..... 60
Şekil 5.13	Sinüzoidal sinyal modülasyonu (taşıyıcı ve yan bantlar) ..... 61
Şekil 5.14	Mesaj (Bilgi) işareti ve ASK işareti..... 61
Şekil 5.15	ASK modülasyonunda ikili kod sinyali ile iki durumda anahtarlanan taşıyıcının genliği..... 62
Şekil 5.16	ASK modülasyonunun üretilmesi ..... 63
Şekil 5.17	FSK üretimi..... 63
Şekil 5.18	FSK modülasyonu..... 64
Şekil 5.19	2 FSK modülasyonunun üretimi ..... 64
Şekil 5.20	BPSK işaretinin üretilmesi..... 65
Şekil 5.21	BPSK işareti..... 65
Şekil 5.22	QAM modülatörü (QPSK modülatörü) ..... 66
Şekil 5.23	9-135 kHz aralığında 10 metrede ölçülen manyetik alan sınır değerleri .. 70



Şekil 5.24	6.78 MHz ve 13.56 MHz bandlarında 10 metrede ölçülen manyetik alan sınır değerleri .....	70
Şekil 6.1	EPC genel yapısı .....	71
Şekil 6.2	RFID Okuyucu Çarpışması Protokolü.....	77
Şekil 7.1	SM 1013 Uygulama Geliştirme Kitinin Üstten Görünümü .....	79
Şekil 7.2	SMRFID Mifare Yazılımı Ekran Görüntüsü .....	83
Şekil 7.3	Etiket seçme ve işlemleri durdurma butonları / Select - Halt .....	85
Şekil 7.4	Onay İşlem Butonu .....	85
Şekil 7.5	Mifare 1K /4K kartlarda okuma işlemi ("R" çift tıklanır.) .....	86
Şekil 7.6	Mifare 1K/4K kartlarda yazma işlemi ("W" çift tıklanır.).....	86
Şekil 7.7	Okuma İşlemi Butonu .....	87
Şekil 7.8	Değer Oku "Read Value- RV" Butonu.....	87
Şekil 7.9	Değer Yaz "Write Value –WV" Butonu.....	87
Şekil 7.10	Değer Arttırma "Increment Value – IV" Butonu.....	88
Şekil 7.11	Değer Azaltma "Decrement Value – DV" Butonu.....	88
Şekil 7.12	Şifreleme Butonu .....	88
Şekil 7.13	Erişim Koşulları Penceresi.....	89
Şekil 8.1	Yazılımın çalıştırıldığında bilgilerin sergileneceği ekranın görüntüsü.....	90
Şekil 9.1	Ürün okutulduğunda yazılım ekranının görüntüsü .....	120
Şekil 9.2	Ürün okutulduğunda yazılım ekranının görüntüsü .....	121
Şekil 9.3	Kredi kartı yanlış şifre girişinde yazılım ekranının görüntüsü .....	122
Şekil 9.4	Kredi kartının geçerli şifresi girildiğindeki yazılım ekranının görüntüsü ....	123
Şekil 9.5	Ürün etiketinin okunması anındaki yazılım ekranının görüntüsü.....	124
Şekil 9.6	Kredi kartının bilgilerinin okutulduğu andaki yazılım ekran görüntüsü	125
Şekil 9.7	Kredi kartına bakiye için geçerli şifre girişindeki yazılım ekranının görüntüsü .....	126



## ÇİZELGE LİSTESİ

	Sayfa
Tablo 2.1	Sistemlerin Karşılaştırılması..... 6
Tablo 2.2	Barkod ve RFID karşılaştırması..... 24
Tablo 3.1	RFID Uygulama Alanları..... 34
Tablo 3.2	Özelliklerine Göre Aktif ve Pasif Etiketlerin Karşılaştırması ..... 40
Tablo 3.3	Pasif ve Aktif RFID Etiketleri ..... 41
Tablo 4.1	RFID Frekans Bandları ..... 42
Tablo 4.2	RFID ETSI Frekansları ..... 42
Tablo 4.3	Ülkelerde kullanılan RFID çalışma frekansları ..... 43
Tablo 4.4	Frekans Bandları ve Uygulamalar ..... 44
Tablo 4.5	Frekans Bandları ve Özellikleri ..... 44
Tablo 5.1	Radyo Frekanslı Tanımlama Sistemleri Teknik Kriterleri..... 67
Tablo 5.2	RF Algılayıcı (Dedektör) ve İkaz Cihazları Teknik Kriterleri..... 68
Tablo 5.3	Endüktif Sistemler Teknik Kriterleri ..... 69
Tablo 6.1	EPC Global 'Sınıfları'..... 72
Tablo 7.1	Mifare 1K kartların Hafıza Dizaynı ..... 81
Tablo 7.2	Mifare 4K kartların Hafıza Dizaynı ..... 82
Tablo 7.3	Mifare etiketleri üzerinde en çok kullanılan işlemler ..... 84
Tablo 8.1	"1128" in onaltılık sistemdeki karşılığının hesaplanması ..... 112
Tablo 8.2	Uygulamada kullanılan ondalık değerlerin onaltılık sistemdeki karşılıkları... .....113



## ÖNSÖZ

Yüksek Lisans Bitirme tezimi hazırlama sürecinde bana olan güvenini hissettirerek azimle, verimli bir çalışma yapmamı sağlayan, bilgi ve tecrübeleri ile araştırma safhasından, kontrol safhasına kadar yardımlarını esirgemeyen çok kıymetli hocam Sn. Yrd. Doç. Dr. Aktül Kavas'a, tez demo kitinin temininde Son Micro firmasına, tez sürecinde bana destek olan çalıştığım firmam RETURN Group'taki ve özel yaşamımdaki tüm arkadaşlarıma, çok sevdiğim arkadaşım Gülan Pehlivan'a ve aileme, özellikle de gece yaralarına, hatta sabahlara kadar çalışırken hep yanımda olan (bu yüzden uyku düzeni mahvolan) ve onu ihmal etmek durumunda kaldığımda bile; "Sen çalış annecim..." diyerek bana anlayış gösteren 4 yaşındaki biricik kızım Hatice'ye teşekkürü bir borç bilirim.

Burcu TUĞAÇ



## ÖZET

Bu tez çalışması temelde iki bölümden oluşur; RFID sisteminin ve teknolojisinin anlatıldığı teorik bölüm ve yapılan uygulamanın, uygulamada kullanılan demo kitin tanıtıldığı ve geliştirilen yazılımın sunulduğu, uygulama bölümü. Uygulama bölümüne bir hazırlık olmak üzere, uygulamanın tipine göre, sistem seçilirken dikkat edilmesi gereken kriterler ve sistemi etkileyen faktörler teorik bölümde sunulmuştur.

Bu tez çalışmasında “elektronik para” uygulaması yapılmıştır. Çalışmada 13,56 MHz, yüksek frekansta çalışan pasif mifare kartlar ve SMRFID 1013 demo kiti kullanılmıştır. Visual Studio 2005. NET platformunda C# dilinde RFID teknolojisi kullanılarak kredi kartı ile ürün satın alımı yapılabilen bir yazılım geliştirilmiştir. Ancak yazılımda kredi kartları, banka ile veri haberleşmesi yapmamaktadır.

Geliştirilen yazılıma göre, RFID sistemi, okuyucuya gösterilen ürünlerin fiyatlarını okur ve toplam harcamayı hesapladıktan sonra ekranda gösterir. Satın alım gerçekleştiğinde ise, kredi kartı şifresi girildikten sonra, toplam harcama, kredi kartındaki meblağdan düşürülür. Kart bilgilerinin erişimine veya kart üzerinde bir işlem yapılmasına ancak doğru onaylama şifresi girildiği takdirde izin verilmektedir.

Yazılımın bu gizlilik özelliği ve SMRFID programının çarpışma önleyici bir yapıda tasarlanmış olması ile tezde yapılan uygulama ayrıca RFID'nin iki temel problemi olan güvenlik (gizlilik) ve çarpışma sorunlarını çözerek başarı ile gerçekleştirilmiştir.

RFID Teknolojisi, günümüzde sağlık sektöründen lojistik'e, envanter yönetiminden askeri uygulamalara kadar hemen her sektörde kullanılmaya başlamasıyla, tez konusu olarak tercih edilmiştir. Ve görünen o ki gelişen yapısıyla geleceğin teknolojisi de RFID olacaktır.

**Anahtar Kelimeler:** RFID, kimlik tanıma, radyo frekansı, otomatik kimlik tanıma sistemleri, etiket, okuyucu, anten



## ABSTRACT

This study consists of two main parts; a theoretical part which tells about the RFID systems, technology and an application part where the application and the demo kit used is explained in detail and the software developed is performed. As a kind of preparation for the application, the criteria to be considered choosing the system and the factors that affect the system according to the application types are also given in the theoretical part.

In this study an “e-money” application is preferred. At 13.56 MHz (HF) operating frequency passive mifare tags and SMRFID 1013 demo kit are used. A software is developed using C# at Visual Studio 2005. NET platform for this application in which a purchase of a product can be done with credit cards by using RFID technology. But in this thesis the credit cards do not communicate with bank servers during the operation.

According to the software developed, the prices of the products that are displayed to the reader are read and the total cost is displayed on the screen after calculated. When the purchasing exists, after the credit card key entrance is done, the total cost can be reduced from the amount money in the credit card. Any “access” or an “operation” on a credit card is only allowed, in case that the correct authentication key is entered.

So by this privacy advantage of the software and the SMRFID program being designed with anticollision requirements, this application has been successfully performed by also removing the two main problems of RFID systems; collision and non-security.

RFID technology has been preferred as the thesis subject since it has become useful in almost every sector. By its developing structure, RFID seems to be also the future technology.

**Key words:** RFID, identification, radio frequency, automatic identification systems, tag, transponder, reader, antenna



## 1 GİRİŞ

1970'lerden beri var olan, teknolojisini kanıtlamış RFID (Radyo Frekansı ile Kimlik Tanıma) sistemi, bugün büyük alışveriş merkezlerinden, hayvan takip sistemlerinden, lojistik-kargo şirketlerine kadar geniş bir uygulama alanında hayat bulmaktadır. Teknolojik alandaki, endüstriyel standartlardaki gelişmeler ve bu alana yapılan yatırımlar geleceğin teknolojisi olarak gösterilen RFID Sistemlerinin tez konusu olarak seçilmesinde etken olmuştur.

RFID Teknolojisi, etiket kullanarak, radyo frekansları ile veriyi uzaktan alıp depolamaya dayalı bir otomatik kimlik tanıma metodudur. RFID sistemleri dışında pek çok otomatik kimlik tanıma sistemi mevcuttur. Bunlardan OCR; optik karakter tanıma sistemleri, yüz tanıma, parmak izi tanıma gibi biyometrik kimlik tanıma sistemleri, bankalardaki kart sistemleri ile günlük hayatımıza çok hızlı giren akıllı kartlar ve marketlerde, eczanelerde ürünlerin üzerinde yer alan barkodlar ile ürün takibinde zirveye oturan barkod sistemleri en temel olanlarıdır. RFID teknolojisini daha iyi tanıtabilmek için bu otomatik kimlik tanıma sistemlerinin, teknolojilerine, özelliklerine, avantajlarına ve kullanım alanlarına tezin ikinci bölümünde yer verilecektir. Özellikle de daha hızlı, daha uzun okuma menzili ve daha güvenilir bir sistem olması ile barkod sistemlerinin yerini alacağı iddia edilen RFID sisteminin, barkod sistemlerine olan üstünlükleri avantajları ve dezavantajları detaylı bir şekilde ele alınacaktır.

Üçüncü bölümde RFID' nin tarihçesine kısaca değinilerek, RFID sisteminin en önemli parçası olan ve birçok araştırma kaynağında "transponder/tag" olarak geçen RFID etiketleri detaylı bir şekilde incelenecektir. RFID etiketi, bir ürün, hayvan veya insana iliştilmiş, silikon çipler ve antenleri olan küçük nesnelere dir. RFID etiketlerini iki temel çeşidi olan pasif ve aktif etiketlerine, güç kaynağı, okuma mesafesi, bellek kapasitelerine göre kıyaslamalarına yer verilecektir. Bu bölümde RFID etiketlerinin frekans bandına ve bellek tiplerine göre sınıflandırması da açıklanmaktadır.



Daha sonra RFID teknolojisinin mevcut uygulama alanları, güncel uygulamaları ve gelecekteki uygulamaları hakkında bilgi verilecektir. RFID hakkında geçtiğimiz dönemde çok tartışılan uygulamalardan biri olan pasaportlarda RFID teknolojisi kullanımı ve bir türlü önüne geçilemeyen CD ve DVD kopyalamaları için getirilen RFID tabanlı çözüm önerilerine, RFID' nin güncel uygulamaları bölümünde kısaca değinilmektedir. Günümüze kadar etiketlerin maliyeti sebebiyle pek yaygınlaşamayan RFID teknolojisi, geliştirilen nano teknolojisi ile etiket fiyatlarının düşmesine paralel olarak, hücresel telefonlardan sonra en hızlı gelişecek kablosuz teknoloji olarak görülmektedir. Gelecek uygulamalar bölümünde, maliyeti düşürmek üzere geliştirilen nano teknolojisi ve mikroçiplerin kapasite artırımı konularındaki çalışmalara da değinilmektedir.

RFID konusunda bir uygulamanın yapılabilmesi için, öncelikle o sistem için gerekli olan doğru frekansın, doğru etiket tipinin, doğru okuyucunun ve kullanılacak yazılım programının belirlenmesi gerekmektedir. Tüm bunlar belirlenirken dikkat edilmesi gereken noktalar ve etken faktörler, üçüncü bölümün sonlarında (Bölüm 3.6'da) detaylı verilmektedir.

RFID sisteminde en önemli konulardan biri de frekans bantlarıdır. RFID' de genellikle 125 KHz (LF), 13.56 MHz (HF), 800–900 MHz (UHF) ve 2.45GHz frekansları kullanılmaktadır. Alçak frekans, yüksek frekans, çok yüksek frekans ve mikrodalga olarak adlandırılan bu frekans aralıkları ve özellikleri dördüncü bölümde karşılaştırmalı olarak incelenecektir.

Beşinci bölümde RFID sisteminin yapısı ele alınmaktadır. RFID sistemi, etiketler, etiket okuyucular, anten ve uygulama yazılımı bileşenlerinden oluşur. Sistemin amacı, verinin mobil bir cihazdan gönderilmesini ve belirli bir uygulamanın ihtiyaçlarına uygun olarak işlenmesini sağlamaktır. Etiket tarafından gönderilen veri, kimlik veya konum bilgisini ya da belirli bir ürün için fiyat, renk, alım tarihi gibi bilgileri içerir. Okuyucu, alıcı anteni yoluyla etiketin göndermiş olduğu bilgiyi alır, haberleşme için geliştirilmiş yazılımı kullanarak bilgiyi işlenmek ve depolanmak üzere gerekli veri tabanına iletir.



Okuyucu ve etiket arasındaki bu sinyalleşme anında, bazen çarpışmalar gerçekleşebilmektedir. RFID sisteminde çarpışma ve kullanılan çarpışma önleyici algoritmalar RFID de çözülmesi gereken sorunlar başlığı altında, altıncı bölüm sonunda irdelenmektedir.

RFID' nin bu çarpışma probleminden başka gizlilik, güvenlik ve standartlar sorunu da çözülmesi gereken sorunlar arasında olup altıncı bölümde, ele alınan konular arasındadır. Etiket ile okuyucu arasındaki mesajların izinsiz dinlenmesi vb. kaynaklı gizlilik ihlali sorunları için geliştirilmiş çözümlere de kısaca değinilecektir.

RFID ile bir uygulama yapılacaksa öncelikle, uygulama yapılacak ülkede izin verilen frekans opsiyonları belirlenir. Bu tez uygulaması için Türkiye'de izin verilen yüksek frekans aralığından 13,56 MHz frekansında bir çalışma yapılmasında karar kılınmıştır. Frekans belirlendikten sonra ne kadarlık bir okuma mesafesine ihtiyaç duyulduğu öncelikli kriterdir. Buna göre etiketin aktif mi pasif mi olacağı belirlenecektir. Her ne kadar aktif etiketlerin okuma mesafesi uzun olsa da, pasif etiketlere nazaran daha pahalı ve daha büyük boyuttadırlar. Bu yüzden yapılacak uygulamada ebadı küçük ve maliyet öncelikli ise pasif etiket seçilmelidir ki bu amaçla, tezde yapılan uygulamada pasif etiket kullanılacaktır. Tezde yapılacak olan uygulama (kredi bilgilerinin bulunduğu banka ile veri haberleşmesi olmayacak şekilde dizayn edilen) bir çeşit elektronik para uygulaması olarak belirlendiğinden, kısa mesafeden okuma yeterli olmaktadır.

Uygulamada kullanılacak demo kit bu özellikler göz önünde bulundurularak, piyasa araştırmalarının sonucunda Son Micro'nun SM1013 demo kiti olarak tercih edilmiştir. Kitin özellikleri, komutları, etiket okuma yazma, şifreleme vb. işlemlerin nasıl olacağı konusu yedinci bölümde detaylı olarak anlatılmaktadır.

Bu kite ilave olarak M.S. Visual Studio 2005. NET platformunda C# dilinde geliştirilen temelde, ürün etiketi okutuldukça ürünlerin fiyatlarını toplayan ve kredi kartı bakiyesinden doğru şifre girildiği takdirde işlem yaparak hesaptan düşen ve kalan bakiyeyi karta işleyen yazılım sekizinci bölümde kodları ile sunulmaktadır.

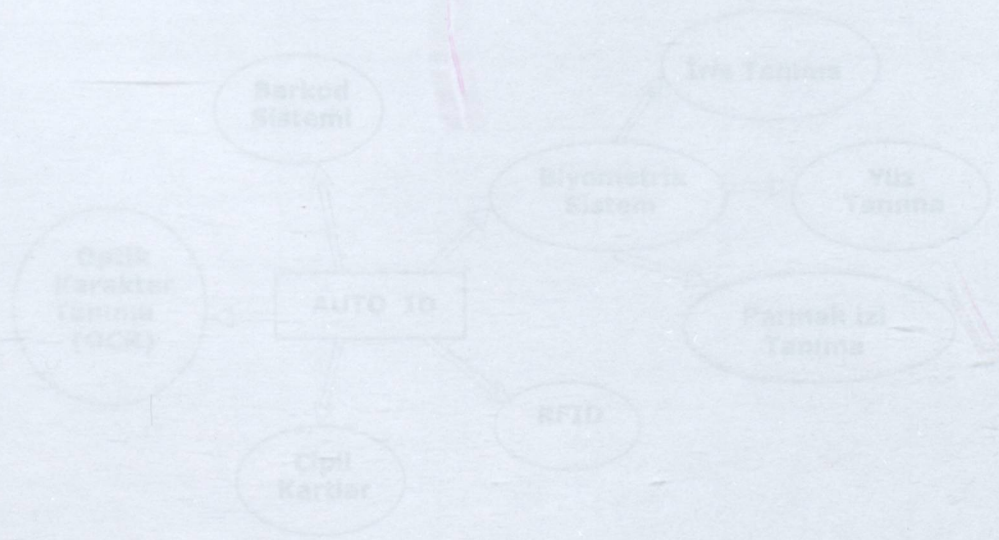


Uygulamada kullanılacak etiketlere, bilgilerin hexadecimal olarak (16'lı sayı sisteminde) demo kit üzerinden işlenmesi ve gerekli hesaplamalara da yine bu bölümde yer verilmektedir.

Yazılım çalıştırıldığında örnek olarak iki ayrı şahsa düzenlenmiş kredi kartından, ürün okutularak hesaptan düşülmesi ve bakiye işlemlerinin yapılması ile elde edilen ekran görüntüleri dokuzuncu bölümde gösterilerek, 13,56 MHZ de gerçekleştirilen örnek bir RFID uygulaması başarı ile tamamlanmaktadır.

Geliştirilen otomatik tanıma sistemleri aşağıdaki şekilde uygulanabilir:

1. OCR: optik karakter tanıma sistemleri
2. Biyometrik kimlik tanıma sistemleri (yüz tanıma, parmak izi tanıma... vb.)
3. Akıllı Kart Sistemi
4. Barkod Sistemleri
5. RFID; Radyo Frekansı ile kimlik tanıma



Şekil 2.1 Otomatik Kimlik Tanıma Sistemleri Aşağı ID

Kaynak: RFID Handbook: Fundamentals and Applications in Commerce, Smart Cards and Identification

Yayıncı: Wiley - Klaus Finkenzeller

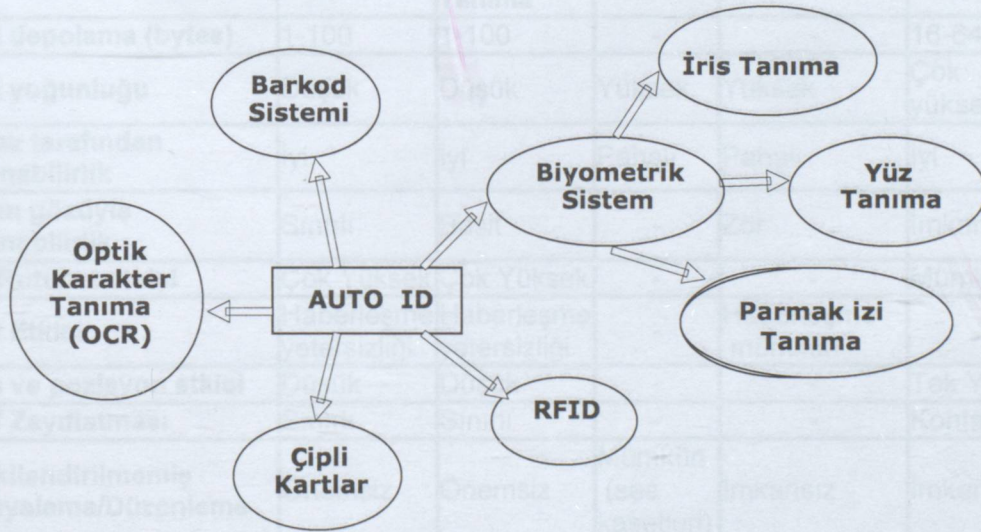


## 2 OTOMATİK KİMLİK TANIMA SİSTEMLERİ

Gelişen teknoloji insanların hayatlarını kolaylaştırıcı sistemleri de beraberinde geliştirdi. Kimlik tanıma işlemlerinin otomatik olarak gerçekleşmesi hayatı kolaylaştırıcı adımların başında gelir ve bunun için günümüze kadar pek çok sistem tasarlanmıştır. Bu sistemler çeşitli sektörlerde birçok uygulamada hayat bulmuştur. Otomatik kimlik tanıma sistemlerini (Auto-ID) incelediğimizde kendi içinde farklı teknolojileri içermekte olduklarını görürüz.

Geliştirilen otomatik tanıma sistemlerini temel olarak 5 grupta toplayabiliriz:

1. OCR; optik karakter tanıma sistemleri
2. Biyometrik kimlik tanıma sistemleri (yüz tanıma, parmak izi tanıma... vb.)
3. Akıllı Kart Sistemi
4. Barkod Sistemleri
5. RFID; Radyo Frekansı ile kimlik tanıma



**Şekil 2.1** Otomatik Kimlik Tanıma Sistemleri Auto- ID

*Kaynak: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, İkinci Baskı - Klaus Finkenzeller*



Optik karakter tanıma sistemi, bir yazının bilgisayar ortamında düzenlenebilir bir formata aktarılmasında kullanılır. Biyometrik sistemler, insan kimlik bilgisinin yüz, ses veya göz gibi biyolojik özellikler ile ortaya çıkarılmasında kullanılmaktadır. Barkod sistemleri ise ürün veya malzeme tanıma amaçlı olarak günümüzde en fazla kullanılan otomatik tanıma sistemidir. Bu sistemler ucuz olmakla birlikte, veri depolama kapasitesi yetersiz ve programlanabilir değildir. Çipli kartlarda bu yetersizlikler biraz olsun ortadan kalkmakla beraber, mikroçip ve okuyucu arasında mekanik temasın gerekliliği bazı dezavantajlar taşımaktadır. Zaman içindeki aşınma ve kirlenme okuyucunun kartı tanımasında sorun çıkarabilir. RFID sistemleri otomatik tanıma sistemleri arasında en fazla çipli kartlar ile benzerlik göstermektedir.

Bu sistemlerin karşılaştırılması da aşağıdaki tabloda gösterilmiştir.

**Tablo 2.1 Sistemlerin Karşılaştırılması**

Sistem Parametreleri	Barkod	Optik Karakter Tanıma	Ses Tanıma	Biometrik Uygulamalar	Akıllı Kart	RFID Sistemleri
Veri depolama (bytes)	1-100	1-100	-	-	16-64k	16-64k
Veri yoğunluğu	Düşük	Düşük	Yüksek	Yüksek	Çok yüksek	Çok yüksek
Cihaz tarafından okunabilirlik	İyi	İyi	Pahalı	Pahalı	İyi	İyi
İnsan gözüyle okunabilirlik	Sınırlı	Basit	-	Zor	İmkansız	İmkansız
Kir/Rutubet etkisi	Çok Yüksek	Çok Yüksek	-	-	Mümkün	Etkisiz
Kılıf Etkisi	Haberleşme yetersizliği	Haberleşme yetersizliği	-	Haberleşme mümkün	-	Etkisiz
Yön ve pozisyon etkisi	Düşük	Düşük	-	-	Tek Yönlü	Etkisiz
Kılıf Zayıflatması	Sınırlı	Sınırlı	-	-	Kontaklar	Etkisiz
Yetkilendirilmemiş Kopyalama/Düzenleme	Önemsiz	Önemsiz	Mümkün (ses kasetleri)	İmkansız	İmkansız	İmkansız
Okuma Hızı	Düşük	Düşük	Çok Düşük	Çok Düşük	Düşük	Çok Hızlı
	~4s	~3s	>5s	>5-10s	~4s	~0.5s
Alıcı verici arasındaki maksimum uzaklık	0-50cm	< 1cm tarayıcı	0-50cm	Doğrudan temas	Doğrudan temas	0-5m mikrodalga



## 2.1 Optik Karakter Tanıma Sistemleri, Özellikleri, Avantajları, Uygulama Alanları

Optik Karakter Tanıma (Optical Character Recognition), bilgisayar ortamında bulunmayan yazılı dokümanların özel tarayıcılar aracılığıyla veya normal olarak taranmış resimlerin FineReader, OmniPage gibi bazı özel programlar yardımıyla bilgisayar ortamına, düzenlenebilecek sayısal halde ("word", "txt") aktarılmasıdır.

Kısaca, resim formatındaki herhangi bir dosya içindeki yazıyı, tanıyarak sonradan tekrar düzenlenebilecek metin biçimine dönüştürebilen sistem olarak da tanımlayabiliriz.



ABCDEFGHIJKLMNPO  
 QRSTUVWXYZ ,AÉİÖÜ  
 abcdefghijklmnop  
 qrstuvwxyzââéîöø&  
 1234567890(\$£.,!?)

**Şekil 2.2** Optik Karakter Tanıma Sistemi

Eğer elinizde, içinde yazı bulunan bir JPG, GIF, TIF ya da BMP dosyası varsa OCR teknolojisi bunu içinden çıkartıp TXT ya da DOC olarak kaydedebilir. Bu resim dosyasını elde etmek için bir de tarayıcı gerekmektedir. Bu şekilde önce herhangi bir kitap, dergi ya da kağıt üzerine yazılmış yazı tarayıcı kullanarak bilgisayara bir resim dosyası olarak aktarıldıktan sonra kullanılan OCR yazılımı diğer tüm işlemleri yapabilmektedir. Normal şartlarda bir A4 sayfasının bilgisayara aktarılması; taranması için ortalama 40, 45 sn. ve karakterlerin tanımlanması için de 1 dakika olacak şekilde toplam 2 ve hataların düzeltilmesini de eklersek ortalama 2,5 dakika içinde bitebilmektedir. 10 parmak klavye kullanan profesyonellerin bile zor eriştiği bu süre için optik karakter tanımla sistemi büyük kolaylık sağlamıştır.



Örneğin bankalarda çeklerin okunup sisteme kayıt edilmesinde, farklı yazı tiplerinin makineler tarafından okunup anlaşılmasını gerektiren birçok uygulama alanında OCR teknolojisi kullanılmaktadır. Ancak sistemin pahalı olması nedeniyle, kullanım alanı dar bir çerçevede kalmaktadır.

## 2.2 Biyometrik Kimlik Tanıma Sistemleri, Özellikleri

Biyometrik, bireyin ölçülebilir fiziksel ve davranışsal karakteristiklerini tanıyarak kimlik saptamak üzere geliştirilmiş otomatik sistemler için kullanılan bir terimdir.

İnsan bedeninin bir parçasının ölçülmesi ile veri elde edilen Fiziksel Biyometriler şunlardır:

- Yüz Tanıma
- İris Tanıma
- Parmak İzi Tanıma
- Retina Tanıma
- El İzi & Damar Tanıma

Bir davranışın ölçülmesi ile veri elde edilen Davranışsal Biyometriler;

- Ses Tanıma
- İmza Tanıma

Biyometrik kimlik tanıma sistemleri bireyin belli biyolojik karakteristiklerini sadece o kişiye özel tek ve benzersiz bir koda dönüştürür. Bu kod elektronik ortama kaydedilir ve aktif kimlik saptanmasında kayıtlar ile ilgili kişi anında karşılaştırılır ve sonuca varılır. Biyometrik sistemler kişilerin kontrollü geçişini/erişimini sağlamayı amaçlar yani yetkili kişilerin geçişine/erişimine izin verilir, yetkisiz kişilere geçiş/erişim hakkı verilmez.

Kartlı ya da şifre kullanılan Sistemlerin aksine, biyometrik sistemlerde bireyin özelliklerinin kopyalanması ya da taklit edilmesi neredeyse imkânsızdır. Ayrıca, kimlik saptama, kişinin fiziksel veya davranışsal özelliği ile yapıldığı için kişi özelliğini başkasına devredemez, unutamaz veya kaybedemez. Dolayısı ile kartlı



veya şifreli sistemlerde yaşanan kaybedilme, unutulma veya çalınma gibi problemler de yaşanmaz.

Bilgisayarındaki bilgilerin güvenliğini sağlamak isteyen kullanıcılar için de son derece güvenilir ve kullanışlıdır. Bilgisayar kullanımında kullanıcı aktif kimlik saptaması yapmak istediğinde diğer erişim sistemlerindeki, örneğin şifre, PIN kodu, kişisel bilgi sorma ya da kart vb. göre daha güvenli bir metottur.

Genel Biyometrik Tanıma İşlem Prosedürü;

Görüntü Yakalama > Özellik Çıkarma > ID Kod Oluşturma > Karşılaştırma şeklinde ilerlemektedir.

### 2.2.1 Biyometrik Kimlik Tanıma Sistemlerinin Avantajları

Biyometrik kimlik tanıma sistemlerinin genel olarak avantajlarını aşağıdaki gibi sıralayabiliriz:

- Şifre, kart, pin numarası kaybetme yoktur, sadece kişinin olması yeterlidir.
- En yüksek güvenlik seviyesini sağlar.
- Kullanım için bir uzmanlık gerektirmez.
- Biyometrik bilgiler başka kişiye transfer edilemez ve kopyalanamaz.
- Tamamen temassızdır; kullanıcının herhangi bir fiziksel etkileşimine gerek duyulmaz.
- Güvenilirdir; çok sayıda kullanıcının kaydedilmesine ve kimlik saptama işlemine izin verir.



## 2.2.2 Biyometrik Kimlik Tanıma Sistemlerinin Uygulama Alanları

Aşağıdaki alanlarda biyometrik kimlik tanıma uygulamaları mevcuttur.

- İnternet bankacılığında kullanıcı tanımlama
- Bilgisayar ve veri güvenliği
- ATM'lerde kullanıcı tanımlama
- Çağrı merkezlerinde kimlik tespiti
- Personel takibi
- Hastanelerde hasta takibi
- Sigorta şirketlerinde kimlik tespiti
- Havaalanlarındaki giriş ve çıkış işlemleri
- Kredi kartı uygulamaları
- Kriminal Amaçlı teşhis ve tespit uygulamaları
- Ağ ve veri güvenliği
- Sosyal güvenlik, vergi süreçleri gibi kamu hizmetleri
- Evlere, ofislere ve binalara fiziksel erişimin kontrolü
- E-ticaret işlemleri
- Elektronik imza uygulamaları

## 2.2.3 Biyometrik Tanıma Sistemi Çeşitleri

Biyometrik tanıma sistemleri, iris tanıma, el geometrisi tanıma, ses tanıma, retina tanıma, yüz tanıma ve parmak izi tanıma çeşitlerine göre aşağıda açıklanmıştır. Yüz tanıma ve parmak izi tanıma teknolojileri yaygın oldukları için biraz daha detaylı yer verilecektir.

Şekil 2.4 Parmak izi Tanıma Biyometrik Sistemi



### 2.2.3.1 Yüz Tanıma Sistemi



**Şekil 2.3** Yüz Tanıma Biyometrik Sistemi

Yüz tanıma biyometrik sistemi, bazı yüz karakteristiklerin analizi, bunların veritabanına kaydedilmesi, kimlik saptamasında, canlı yüz ile kaydın karşılaştırılması ve uyumluysa kullanıcının erişimine izin verilmesi işlemini içerir.

Yüzdeki yaklaşık 50 noktayı inceleyerek ve bu verilerden kalıp oluşturularak sonuca varan bu sistem yine bilgisayar programları kullanılarak uygulanmaktadır. Yüz tanıma sistemlerinin pratik uygulamalardaki başarı grafiği yüksek olmamakla birlikte bu alandaki gelişmeler devam etmektedir.

### 2.2.3.2 Parmak İzi Tanıma

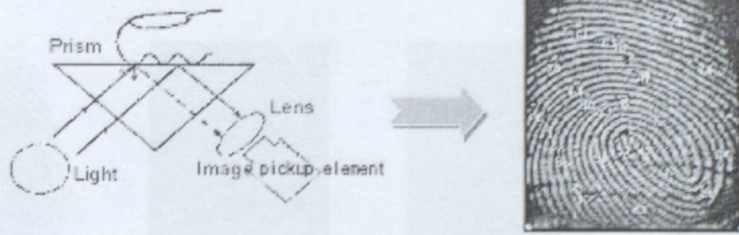
Biyometrik tanıma da kullanılan parmak izi her bir kişide farklı desen ve çizgilere sahiptir. Parmak izi tanımda işlem optik algılayıcılardan alınan görüntü ile başlar.



**Şekil 2.4** Parmak izi Tanıma Biyometrik Sistemi



Parmak izi tanıma algoritması alınan görüntü üzerinden her bir parmak izi için farklı ve tek olan parmak izi özelliğini çıkartır ve kişiye özel bir ID kod oluşturarak veri tabanına kaydeder. Veri tabanında bulunan her bir parmak izi kodu her kişi için farklıdır.



**Şekil 2.5** Parmak izi Görüntüsü

Parmak izi tanımda kullanılan optik okuyucular parmak izi temasından kaynaklanabilecek sorunlara karşı farklı olarak tercih edilebilmektedir. Buradaki amaç farklı çalışma ortamlarında en iyi parmak izi görüntüsünü almaktır.

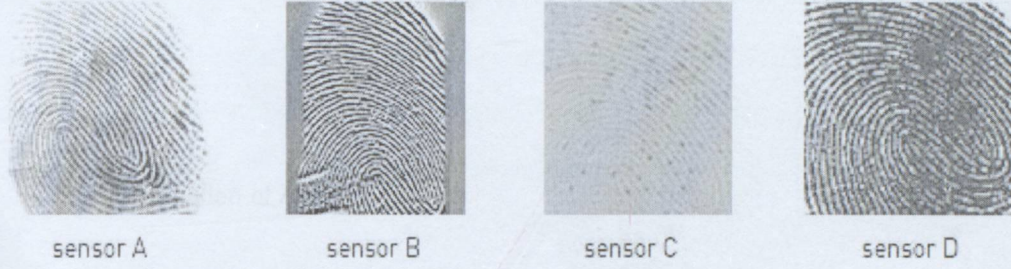
Biyometrik teknolojiler arasında en düşük maliyetle kurulabilen parmak izi okuyucular özellikle ofis çalışma ortamları için idealdir. Sanayi tipi uygulamalar için tercih edilmemektedir.

Parmak izi tanıma teknolojisinde farklı yaklaşımlar bulunmaktadır. Bunlardan bazıları polisin kullandığı geleneksel karşılaştırma yöntemini oluşturmakta, bazıları ise kendine özgü yaklaşımlar sergilemektedir. Bu cihazların diğer biyometrik cihazlardan çok daha fazla çeşidi mevcuttur. Ancak bilinenin aksine parmak uçlarındaki deri ayrıntılarıyla yapılan kimliklendirmeler yerlerini çok daha detaycı ve hassas sistemlere bırakmaktadır. Örneğin "termal görüntüleme" sisteminde parmağın ıslısından faydalanılır. Parmak bir çip üzerinden geçirilir ve parmak ıslısının izleri okunur. Parmak izi sisteminin kullanıcılara yeterli açıklamanın ve eğitiminin verildiği ve sistemin kontrollü bir ortam dahilinde gerçekleştiği ev içi uygulamalarda kullanılmasının iyi bir seçenek olduğu öngörülmektedir.



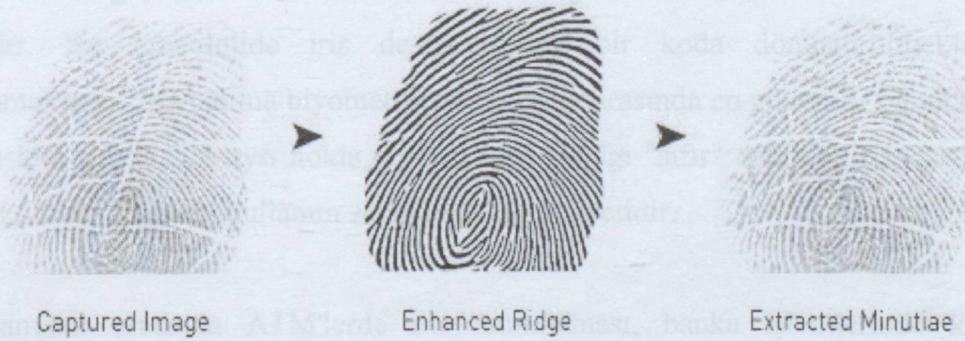
Parmak izinin tanıma adımları aşağıdaki gibidir:

- **Görüntünün Alınması:** Parmak izi görüntüsünün alınması ile başlar. Aşağıda görüldüğü gibi farklı sensör tiplerinden alınan görüntü kalitesi ve görünümü birbirlerinden farklıdır.



**Şekil 2.6** Parmak izi tanıma adımlarında görüntünün alınması

- **Görüntünün İşlenmesi:** Optik sensörlerden alınan görüntü üzerinde parmak izi çizgi sırtları belirginleştirilerek farklı noktalardan alınan noktalar özellik çıkarma algoritmasından geçirilerek değişme imkanı en az olan en belirgin noktalardan resim olmayan kişiye özel bir ID kod oluşturulur.

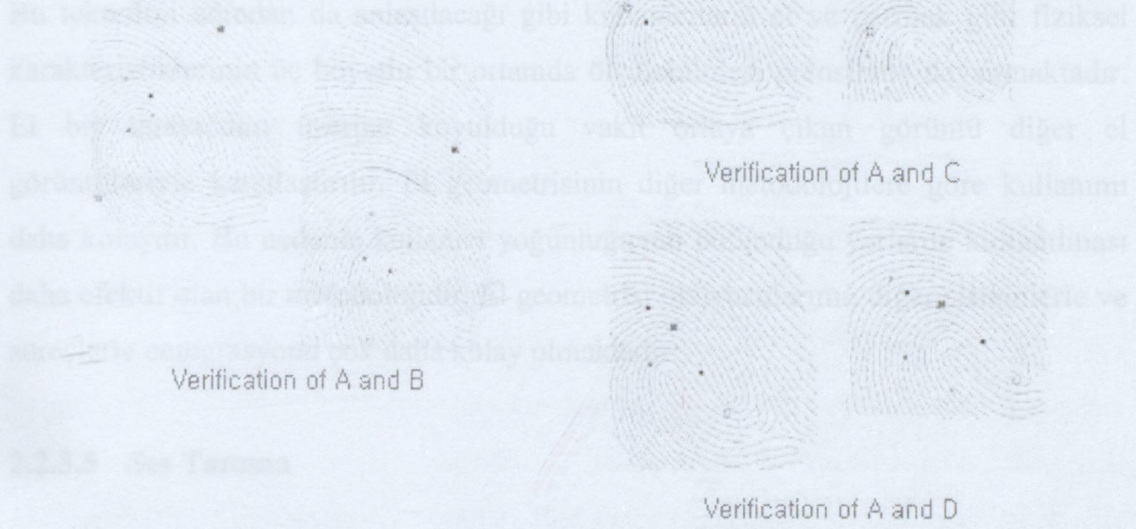


**Şekil 2.7** Parmak izi tanıma adımlarında görüntünün işlenmesi

- **Doğrulama İşlemi:** Aşağıda görüleceği gibi doğrulama işlemi için kullanılan anahtar noktalar her parmak izinde diğerlerinden farklıdır.



### 2.2.3.4 El Geometrisi Tanıma



**Şekil 2.8** Parmak izi tanımda görüntünün doğrulanması

### 2.2.3.3 İris Tanıma

İris tanıma kullanıcı ile okuyucu arasında yakın temas gerektirmeyen ve kullanışlı olan bir biyometri teknolojisidir. İris özellikleri üç adım öndeki bir kameradan tanımlanabilmektedir. İris tabakası gözün renkli olan kısmında bulunur ve her insana göre farklılık gösterir. Hatta bir insanın her iki gözünün de iris deseni birbirinden farklıdır. Bu teknolojiye iris deseni dijital bir koda dönüştürülmekte ve saklanmaktadır. İris tanıma biyometrik teknolojiler arasında en güvenilir olanıdır. Bu durum için gözde 276 ayrı nokta taranır, yani yanlış "sıfır" denilebilir. Ancak çok yaygın olmama nedeni kullanım zorluğu değil maliyetidir.

Uygulamalar arasında ATM'lerde iris tanımlaması, banka işlemlerinde kimlik doğrulama ve online alışverişlerde kimlik tanımlaması sayılabilir. Bir bilgisayarın sadece sahibi tarafından açılmasını güvence altına almak veya bina güvenliği sağlamak gibi nispeten alışılmış uygulamalara artık araba ve cep telefonu uygulamaları da eklenmiştir. Bu sistem çok büyük ve çok yüksek güvenlik gerektiren yerlerde kurulur, hatta ABD'de bu tip yerlerin çoğunda ikili dediğimiz aynı anda hem göz hem parmak izi tanımlaması yapılır.



#### 2.2.3.4 El Geometrisi Tanıma

Bu teknoloji adından da anlaşılacağı gibi kullanıcıların el ve parmak gibi fiziksel karakteristiklerinin üç boyutlu bir ortamda ölçülebilmesi prensibine dayanmaktadır. El bir tarayıcının üzerine koyulduğu vakit ortaya çıkan görüntü diğer el görüntüleriyle karşılaştırılır. El geometrisinin diğer metodolojilere göre kullanımı daha kolaydır. Bu nedenle kullanıcı yoğunluğunun bulunduğu yerlerde kullanılması daha efektif olan bir metodolojidir. El geometrisi okuyucularının diğer sistemlerle ve süreçlerle entegrasyonu çok daha kolay olmaktadır.

#### 2.2.3.5 Ses Tanıma

Günlük iş süreçlerinde sesin ne kadar kullanıldığı düşünüldüğünde ilginç bir teknik olarak ortaya çıkan ses tanıma teknolojileri pek de güvenilir bir metot değildir. Buna rağmen insan sesi davranışsal birimlerden oluşur ve bu bile tek başına belirleyici bir unsur olmaktadır. Bu teknikte ses frekansları üç boyutlu görüntüleri oluşturmakta ve sesin en küçük birimleri özel bir takım biçimlerde karakterize edilmektedir. Bu alanda bazı ürünler piyasaya sunulmuş olsa da birçoğunun kullanımı yerel akustiğin değişebilir yapısı itibariyle zorlaşmıştır.

#### 2.2.3.6 Retina Tanıma

Retinanın kendine özgü yapısının optik sistemler tarafından taranması prensibine dayanan bu teknolojinin güvenilirliği yüksektir ancak kullanıcının belirli bir noktaya bakması gerektiğinden kullanımı zordur. Teknolojisinin yeterli olmasına rağmen bu nedenden dolayı fazla kabul görmemiştir.

### 2.3 Akıllı Kart Sistemleri Özellikleri

Akıllı kartlar, içine küçük bilgisayar niteliği taşıyan bir mikroişlemci yerleştirilmiş olan plastik kartlardır. Bu işlemci, farklı şekildeki bilgileri saklayıp işleyebilmekte ve bu nedenle farklı sektörlerde farklı çözümler ile kullanılabilir.



Akıllı kartlar dış dünya ile iki şekilde veri alışverişinde bulunurlar. Birinci olarak altın kaplı temas noktaları ile iletişim; bu kartlar endüstri genelinde “Temaslı Kartlar” olarak tabir edilir. İkinci olarak da Plastik üretimi esnasında kart içerisine yerleştirilmiş yonga ve bağlı bulunduğu anten üzerinden radyo frekansı ile iletişim; bu kartlara ise “Temassız Kartlar” adı verilir.

Bilgi alışverişinde bulunabilmek için temaslı kartlar uyumlu bir okuyucuya yerleştirilirler veya temassız kartlar radyo frekansı destekli temassız okuyucuların yarattığı manyetik alana dahil edilerek işlem görürler. Akıllı kartlarda pil veya benzeri enerji kaynağı bulunmamaktadır. Her iki tip için de gerekli enerji dışarıdan, yani okuyuculardan sağlanmaktadır. İşlemci (CPU) zamanlaması da yine okuyuculardan gelmektedir. Hafıza türü EEPROM’ dur (Electrical Erasable Programmable Read Only Memory – Elektriksel Silinebilir Programlanabilir ROM) ve herhangi bir gerilim uygulanmadığında bile içeriğini bozulmadan korumaktadır.

Bazı kartlarda ise sadece hafıza modülü bulunmaktadır ve uygulamalar ile karttaki sayaç değerleri artırılabilir veya azaltılabilir. Bu kartlar ise sektör genelinde Bellekli kart olarak isimlendirilmektedirler. Sadece belli türlerde yonga zekası (mikroişlemci-çip) içeren kartlara mikroişlemcili akıllı kartlar adı verilmektedir. Akıllı kartların iki temel özelliği güvenlik ve hareketlilik/dolaşımdır (mobility). Akıllı kart kullanılmak üzere tasarlanmış tüm uygulamalardaki ana esas kart üzerinde koruma altında bulunan verilere erişimin ve kartın taklit edilmesinin neredeyse imkansız olmasıdır. Herhangi bir sebepten ötürü kart güvenliği tehlikeye girse bile kullanımının doğrulanması neredeyse imkansızdır.

Bellekli kartlar, ağırlıklı olarak bilgi saklama amacıyla kullanılan kartlardır. İşlemci tabanlı kartlar, içerisindeki mikroişlemci sayesinde kendisine dışarıdan gönderilen komutlara belirlenen kurallar doğrultusunda cevap verebilen kartlardır.

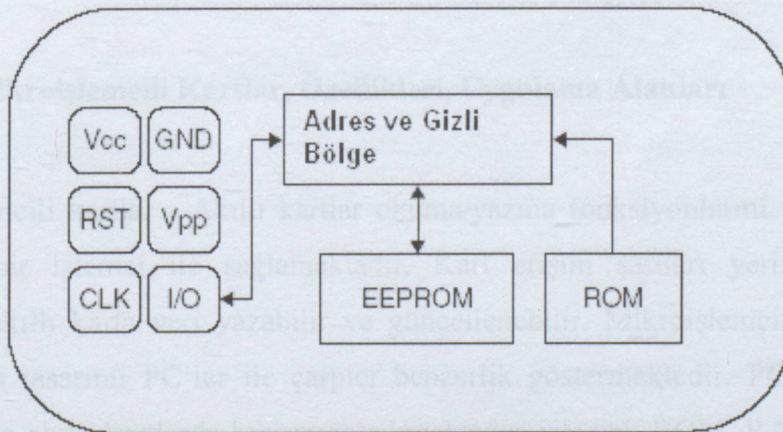


### 2.3.1 Akıllı kart Tipleri

Akıllı kartlar iki ana çeşitte mevcuttur ve aralarındaki esas belirleyici fark kartın mikroişlemci içerip içermediğinden kaynaklanır. CPU'suz kartlara Bellekli kart adı verilirken, CPU içeren kartlar akıllı kartlar olarak adlandırılır. Maliyete bağlı özellikleri, uygulama basitliği veya fonksiyonel üstünlükleri ile her kart türü pazarın değişik bölümlerine özgü uygulamalar içerir.

#### 2.3.1.1 Bellekli Kartlar, Özellikleri, Uygulama Alanları

Bellekli kartlar tek fonksiyonlu uygulamalar için tercih edilirler ve düşük maliyetlidirler. Yaygın olarak telefon kartı gibi ön ödemeli uygulamalarda kullanılmaktadırlar. Veri erişimi, çip içerisinde yazılan veya silinen değerleri koruyan bir güvenlik modülü ile yönetilmektedir. Ödeme kartlarında kontör değişiklikleri (veya kartın içerdiği değer değişimi) çip tarafında gerçekleşir ve geri dönüştürülemez. Bu özellikleri sağlayan hafıza modülleri kart birim fiyatını manyetik bantlı kartlara göre artırırsa da yine de bellekli kartların maliyetleri akıllı kartlara oranla çok daha düşüktür. Dahası bu basit teknoloji ilgili okuyucu/yazıcı cihaz ve ekipmanın daha ucuza üretilmesine olanak sağlamaktadır.



**Şekil 2.9** Tipik Bellekli Kart Yapısı

*Kaynak: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, İkinci baskı - Klaus Finkenzeller*



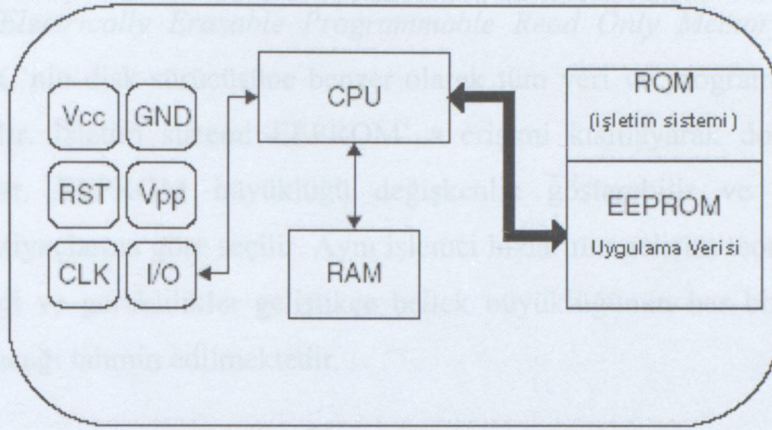
Bellekli kartlar akıllı kart teknolojisine geçiş yapılması düşünülen uygulamalarda kullanılmak üzere ilk bakışta yeterli birer alternatif olarak gözükebilirler. Fakat terminal altyapılarında oluşacak uyumsuzlukların giderilmesi için veya API' lerin (Application Program Interface – Uygulama Program Arayüzü) programlanma metodlarındaki farklılıklardan ötürü ek yatırım ihtiyaçları doğabilir. Bellekli kart yapısından mikroişlemcili kart teknolojilerine geçiş uzun vadede önemli ek maliyetler getirebilir. Buna en büyük etken olarak bellekli kartların standart dışı yapılanma doğası bulunduğu, ISO' nun bellekli kartların standartlaştırılmasına yönelik kısıtlı girişimi bulunması ve tüm yoğunluğunu akıllı kartlara odaklamış olduğu söylenebilir. Bellekli kartların kendini bir sisteme doğrularak (örneğin bir terminal üzerinden gelen rasgele numara sorgusuna doğru cevap dönebilen) fazladan güvenlik sağlayan daha akıllı türleri de mevcuttur. Bu tür kartlar ayrıca PIN doğrulama yapma özelliğine de sahiptirler fakat uygulama esnekliği söz konusu olduğunda çok kısıtlıdırlar.

Bellekli kartların uygulama alanları Telekomünikasyon, ön-ödemeli hazır kartlar, sağlık sigorta numaraları, otomatik satış makineleri (içecek/yiyecek otomatları), otoparklar, toplu taşımacılık, hava yolu mil kartları uygulamaları vs. olarak sıralanabilir. En yaygın örneklerini ön ödemeli telefon kartları, üniversite kampüs kartları, özel kulüp kartları olarak görmekteyiz.

### **2.3.1.2 Mikroişlemcili Kartlar, Özellikleri, Uygulama Alanları**

Mikro işlemcili kartlar - Akıllı kartlar okuma/yazma fonksiyonlarını ve bütünleşik güvenliği bir işlemci ile sağlamaktadır. Kart erişim şartları yerine getirildiği müddetçe akıllı karta veri yazabilir ve güncellenebilir. Mikroişlemcili kartların iç mimarisinin tasarımı PC'ler ile çarpıcı benzerlik göstermektedir. PC'lerdeki yapı taşları bu tip akıllı kartlarda karşımıza çıkmaktadır; işlemci, ROM, RAM, I/O portu ve bu durumda depolama için disk yerine EEPROM.





**Şekil 2.10** Tipik Mikroişlemcili Kart Yapısı

*Kaynak: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, İkinci Baskı - Klaus Finkenzeller*

**İşlemci (CPU-Central Processing Unit)** : İşlemci genelde 16-bit adres bus' a sahip 8-bitlik bir mikroişlemcidir. Bu işlemci benzer işlemci kartlarında 128KB'a kadar kapasite sağlar.

**RAM (Read Access Memory)** : RAM veri saklayabilmek için enerji kaynağına ihtiyaç duyan değişken bellektir. İşlemciye çalışma alanı sağlar. Genelde RAM büyüklüğü yaklaşık 256 bittir. Bu küçüklükte bir alan olmasının nedeni RAM belleğin bit başına EEPROM' dan veya ROM'dan daha fazla yer tutması ve akıllı kart yongalarının özelliklerini sağlayabilmek için özellikle küçük tutulmasıdır.

**ROM (Read Only Memory)** : ROM akıllı kart işletim sistemini içermektedir ve çip üretimi esnasında yüklenmektedir. Yüklenen yazılıma ROM-mask adı verilir. ROM boyutu işletim sistemi fonksiyonlarına göre değişkenlik gösterir. İşletim sistemi ROM içinde bulunduğundan kart kişiselleştirildikten sonra yeni bir versiyonla ROM'un güncellenmesi mümkün değildir. Fakat kart EEPROM' a yazılan bir kodu çalıştırabilir ve geniş bir ifadeyle işletim sistemi güncellemesi olarak kullanılabilir ama bu türde bir işlem gerçekte çok nadir olarak uygulanır. Uygulama kodu yazılması için özel koruma altında bulunan işlemci hakkında çok üstün bilgiye ihtiyaç olup bu tür bir işlem uzmanlık ve özel yetkinlik gerektirecektir.



*EEPROM (Electrically Erasable Programmable Read Only Memory)* : Bu sabit bellek bir PC'nin disk sürücüsüne benzer olarak tüm veri ve programları saklamak için kullanılır. İşletim sistemi EEPROM' a erişimi kısıtlayarak dosya koruması sağlamaktadır. EEPROM büyüklüğü değişkenlik gösterebilir ve bu büyüklük uygulama ihtiyaçlarına göre seçilir. Aynı işlemci hızlarının gelişim teorisinde olduğu gibi teknoloji ve gereklilikler geliştikçe bellek büyüklüğünün her birkaç yılda bir ikiye katlanacağı tahmin edilmektedir.

*I/O Port' u:* I/O Port' u veriyi seri şekilde bit bit iletmek için kullanılır. Varsayılan hız (baud rate) saniyede 9600 bit olup bazı kartlar daha yüksek süratleri desteklemektedir.

*Co-İşlemci:* Ek işlemciler dijital imza gibi uygulamalarda kullanılan daha ileri düzeydeki kartlarda şifreleme işlemleri için rakamlar üzerinde modüler işlemleri gerçekleştirmek üzere sağlanmaktadır. Mikroişlemcili kartlar çok işlevli olup kendilerine geniş bir uygulama alanı portföyü bulmuşlardır.

Mikroişlemcili –akıllı kartların uygulama alanları genellikle kredi kartları, SIM kartlar (GSM), akıllı kimlik kartları, geçiş kontrol, yetki kartları, elektronik para, havayolu biletleri, güvenli mesajlaşma ve dijital imza şeklinde sıralanabilir. En yaygın kullanım örneklerine bankalar ve GSM operatörlerinde rastlanmaktadır.

### 2.3.1 Akıllı Kart Sisteminin Uygulanmış Alanları

Akıllı kartlar sadece ATM ve POS uygulamalarında değil aynı zamanda internet, telefon, TV dekoderleri, cep telefonları, akıllı telefonlar gibi birçok uygulamada kullanılmaktadır.

Akıllı kartların kullanım alanları aşağıdaki gibi gruplanabilir.

- \* Çıkarılmış kart uygulamaları (örneğin; işsizlik, alımlarına vs.)
- \* Akıllı kartların kullanım alanları



### 2.3.2 Akıllı Kart Sisteminin Avantajları

Akıllı kartlar online işlemler için gereken saniyelerce zamanla karşılaştırıldıklarında saniyenin altında güvenli işlem sürati gerçekleştirmektedirler. Elektronik cüzdan gibi uygulamalar için bu özellik kullanıcılar tarafında zaman alan ve risk taşıyan diğer tür kartlara ve nakit paraya karşı önemli avantaj sağlar. Bu doğrultuda kart sağlayıcılar temassız teknoloji barındıran akıllı kartlar geliştirmişlerdir. Böylece daha hızlı güvenli işlemler maliyet düşüşleri ve hizmet verimliliğinin artması ile sonuçlanmıştır.

Akıllı kartlar manyetik bantlı kartlara nazaran çok daha fazla veri taşırlar. Çok uygulamalı kartların geliştirilmesi birçok değişik uygulamanın tek kart üzerinde toplanabildiğini göstermektedir (kredi kartı/ATM kartı, e-cüzdan, seyahat biletleri, puan sistemi, güvenlik ve kimlik kartı gibi...)

Güvenlik yönünden de manyetik kartların çok ötesindedir. İçerdiği yazılımın çok daha gelişmiş olması, güvenlik düzeyini de arttırmaktadır. Dışarıdan gelebilecek tehditlere yönelik olarak, bilgi kopyalamayı engelleyen, şifreleme algoritmalarını koruyan yazılımlar sayesinde, akıllı kartların 3. şahısların eline geçmesi durumunda kart içeriğinin ele geçirilmesi tehlikesini minimuma indirmektedir.

Akıllı kart sisteminde tek bir yazılımla onlarca işlevi görülebilmektedir. Bu sebeple birçok değişik sektörde kullanılmaktadır.

### 2.3.3 Akıllı Kart Sisteminin Uygulama Alanları

Akıllı kartlar sadece ATM ve POS uygulamalarında değil aynı zamanda Internet, telefon, TV dekodeerleri, cep telefonları, akıllı telefonlar gibi birçok uygulamada kullanılmaktadır.

Akıllı kartların uygulama alanlarını aşağıdaki gibi gruplayabiliriz.

- \* Otomatik ücret toplama sistemlerinde (toplu taşımacılık, ulaştırma vs.)
- \* Alışveriş, bankacılık ve finans işlemlerinden



- \* Elektronik cüzdan uygulamalarında
- \* Biyometrik tanımlamada (retina, parmak izi, dijital görüntü taraması vs.)
- \* Geçiş kontrol sistemlerinde
- \* Telekomünikasyon sektöründe (GSM, telefon vs.)
- \* Depo ve envanter kontrolünde

Kamu, finans, ulaştırma, telekomünikasyon, sağlık, eğitim, perakende ve daha birçok sektör daha güvenli ve iyileştirilmiş hizmet sunmak için akıllı kart kullanmaktadır.

## **2.4 Barkod Sistemleri, Özellikleri, Avantajları & Dezavantajları, Uygulama Alanları**

Barkod bilginin makineler tarafından okunabilir şekilde görsel olarak bir yüzey üzerinde sunulmasıdır. Orijinal olarak barkod, veriyi paralel çizgilerin genişlikleri ve boşlukları arasında saklamakta idi, ama günümüzde noktasal şekiller, iç içe daireler ve görüntü içinde gizli şekiller gibi farklı türleri de görülebilmektedir.

Barkod, barkod okuyucu olarak da adlandırılan optik okuyucular ile okunabilir veya özel yazılımlarla görüntü içinden taranabilir yapıdadır. Barkod bilgisayara veri girişinin doğruluğunu ve hızını artıran Otomatik Tanıma Veri Toplama (OT/VT) uygulamalarında geniş bir kullanım alanı bulmaktadır.

Geleneksel olarak barkod kodlaması sadece rakamları sembolize ederken, yeni sembolojiler tüm ASCII karakter setine büyük harf ve daha fazlasını eklemiştir. Basit barkodların ihtiyaç duyduğu alana daha fazla bilgi sığdırma gereksinimi çizgiler yerine kare hücreleri içeren (bir tür İki boyutlu barkod) matrix kodların geliştirilmesine sebebiyet vermiştir. İç içe kodlar iki boyutlu ve tek boyutlu kodların karışımıdır ve geleneksel tek boyutlu sembolojiyi birden fazla satır içerecek şekilde bir çerçeve içinde yeniden boyutlandırma işlemidir.





**Şekil 2.11** Tipik Barkod Örneği

Tek boyutlu barkod ikili bir koddur (1'ler ve 0'lar). Çizgi ve boşluklar değişen kalınlıklarda olurlar ve farklı kombinasyonlarda basılırlar. Okunabilme için, iyi bir baskı ve çizgi ve boşluklar arasında yeterli kontrast olmalıdır. Tarayıcılar kodları okumak için farklı teknolojiler kullanır. En genel iki teknoloji lazer ve kameradır. Tarayıcılar, birçok süpermarket kasasında olduğu gibi sabit veya envanter takibinde kullanıldığı şekilde el-tipi cihazlar olabilir.

Barkod birçok ve farklı uygulamada fark edilir bir başarı kazanmıştır. İlk başarılı barkodlardan olan ve Dr. David Allais tarafından geliştirilen Code 39, lojistik ve savunma sanayi uygulamalarında geniş bir uygulama alanı bulmuştur. Code 39 daha yeni barkodlara göre daha az karmaşık olmasına rağmen bugün hala kullanımdadır.

Sadece dünyada değil, ülkemizde de çok yoğun bir şekilde kullanılan barkod teknolojisini, yakın gelecekte rakip çıkan bu tezin asıl konusu olan RFID (Radyo frekansı ile kimlik tanıma) teknolojisi ile karşılaştırdığımızda her ikisinin de avantajları ve dezavantajları daha belirgin ortaya çıkmaktadır.

RFID; sürat, daha uzun okuma menzili ve daha güvenilir bir sistem olması ile barkod teknolojisinin önüne çıkmaktadır. Ayrıca RFID etiketleri uygulamalarda barkod etiketlerine kıyasla üstün özelliklere sahiptir. Nesne hareket halinde iken veya etiket ile okuyucu arasında (metal olmadığı sürece) engelleyici bir katman olsa bile okuma gerçekleşmektedir. Bu sebeple kutulanmış ve paketlenmiş ürünler dahi okunabilmektedir.



Barkodların başka dezavantajları da vardır; eğer barkod etiketi kazara çizilir, darbe alır ya da yırtılırsa bir daha onu okumak imkansız hale gelir. Ayrıca standart barkodlar sadece üreticiyi ve ürünü tanımlar. Nesnenin kendisini tanımlamazlar. Yani taranan ürün hakkında detaylı bilgi vermezler. RFID etiketleri tüm bu isteklere cevap verebilir.

**Tablo 2.2 Barkod ve RFID karşılaştırması**

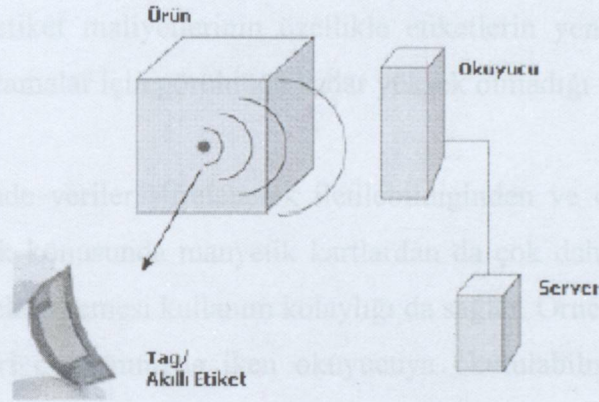
BARKOD	RFID
<ul style="list-style-type: none"> <li>•Sadece veri okuma</li> </ul>	<ul style="list-style-type: none"> <li>• Etiket verisini hem okuma hem de etiket üzerine yeni veri yazma</li> </ul>
<ul style="list-style-type: none"> <li>•Kısıtlı alan ve okuma oranı</li> </ul>	<ul style="list-style-type: none"> <li>• Uzun mesafe ve her okumada birden çok kalem mal okuması</li> </ul>
<ul style="list-style-type: none"> <li>•Etiket başına maliyet düşük</li> </ul>	<ul style="list-style-type: none"> <li>• Dayanıklılık</li> <li>• İnsan/Operatör müdahalesine gerek yok</li> <li>• Daha fazla veri (256K+)           <p>Bu sayede sadece ürünün kodu değil, gerekiyorsa geldiği depo, son kullanma tarihi ya da istenen başka bilgiler etiketlere yüklenebilir.</p> </li> </ul>

Barkod etiketleri el ile birer birer okutulurken, RFID okuyucular etiketlerin çarpışma önleme özelliği sayesinde aynı anda birden fazla etiketi okuyabilmektedir. Ayrıca barkod etiketleri sadece bir defa yazılabilirken, okuma-yazma özelliğine sahip olan RFID etiketlerin üzerine bilgi defalarca yazılıp okunabilir ve tüm bu işlemler etiket hareket halinde iken bile yapılabilir.



## 2.5 RFID Sistemleri, Özellikleri, Avantajları & Dezavantajları, Uygulama Alanları

RFID, bugüne kadar bildiğimiz otomatik veri toplama teknolojileri olan barkod çubukları ve optik sinyaller (lazer ya da CCD) kullanan formlardan farklı olarak entegre devreler, taşıyıcı etiketler ve okuyucular arasında radyo dalgaları kullanılarak iletişim kurulan kimlik tanıma metodudur.



Şekil 2.12 RFID Sistemi

RFID, üzerinde mikroişlemci ile donanmış etiket taşıyan bir nesnenin, bu etikette taşıdığı kimlik yapısı ile hareketlerinin izlenebilmesine imkan veren radyo frekansları ile çalışan bir teknolojidir.

RFID ve barkod uygulamaları bazen benzerlik gösterse de temelde iki farklı teknolojidir. En büyük fark da yukarıda dile getirdiğimiz barkodların doğrudan görüş teknolojisini kullanmasıdır. Bu barkodu okumak zorunda olan bir tarayıcı gerekliliği kılar. Bu yüzden kullanıcılar tarayıcıyı barkoda tutup okutmak zorundadır. RFID etiketleri ise RFID okuyucunun menziline olduğu sürece okunabilir. Barkodun aksine etiket ile okuyucu arasında görsel temas olmasa dahi okuma süratli ve kesin bir şekilde sağlanabilmektedir.

Zor çevre koşullarında kullanılabilen RFID etiketler; kar, sis, buz, boya, yağ gibi çevresel faktörlerden de etkilenmezler. RFID teknolojisinin barkoda olan tüm bu üstünlüklerine rağmen, en büyük dezavantajı pahalı olması olarak görülmektedir.



Aslında RFID etiketlerin fiyatlarının doğrudan olarak barkod etiket fiyatları ile birebir kıyaslanması doğru bir yaklaşım değildir. RFID etiketlerin fiyatları barkod etiketlerinden daha yüksek olsa da, okunabilir-yazılabilir bir RFID etiketin üzerine bilginin defalarca yazılabildiği göz önüne alındığında RFID etiketlerinin, barkod etiketinden uzun vadede daha kârlı geldiğini söyleyebiliriz.

Ayrıca RFID etiketlerin her türlü hava şartlarında, açık alanda kullanılabilirdiği, uzun yıllar (yaklaşık on yıl) ömrünün olduğu, uygulamalara esneklik kazandırıcı faktörleri de eklendiğinde etiket maliyetlerinin özellikle etiketlerin yeniden kullanılabilirdiği kapalı devre uygulamalar için görüldüğü kadar yüksek olmadığı ortaya çıkmaktadır.

RFID teknolojisinde veriler şifrelenerek iletilebildiğinden ve diğer birçok özelliği sayesinde güvenlik konusunda manyetik kartlardan da çok daha güvenlidir. Ayrıca fiziksel temas gerektirmemesi kullanım kolaylığı da sağlar. Örneğin RFID teknolojisi ile kimlik bilgileri cüzdanınızda iken okuyucuya okutulabilmektedir. RFID' nin uygulama alanları 3. bölümde detaylandırılacaktır.



### 3 RFID SİSTEMLERİ

RFID; İngilizce açılımı ile Radio Frequency Identification kelimelerinin kısaltmasıdır. Türkçe ifadesi ile "Radyo Frekanslı Tanımla"; canlıları ya da nesnelere radyo dalgaları ile tanımlamak için kullanılan teknolojilere verilen genel isimdir. Bu bölümde RFID Teknolojisinin tarihçesi, en temel bileşeni olan RFID etiket tipleri, özellikleri, RFID Teknolojisinin uygulama alanları, güncel uygulamaları ve bir RFID sistemi seçimindeki etken kriterlerin neler olduğu anlatılacaktır.

#### 3.1 Tarihçesi

Oldukça eski bir teknoloji olan RFID' nin kullanımı, İkinci Dünya Savaşı yıllarına kadar uzanmaktadır. İlk olarak 1940'lı yılların başlarında İngiltere'de dost ve düşman uçaklarının tanımlanmasında kullanılmıştır. Bunu 1970'li yıllarda nükleer malzeme izleme uygulamaları takip etmiş, ticari uygulamaları 1990'lı yıllarda başlamıştır. Geçtiğimiz 20 yıl boyunca bu teknoloji ABD, İtalya, Fransa, Portekiz ve Norveç'te otoban ve köprülerde geçişlerin ücretlendirilmesinde, çiftlik hayvanlarının izlenmesinde, nükleer madde stoklarının kontrolü ve izlenmesinde, otomobil üretiminde araçların montaj hattı üzerinde izlenmesinde kullanılmıştır. Ancak etiketlerin maliyetlerinin yüksekliği ve kullanım zorluğu, RFID teknolojisinin uzunca bir süre kitlesel ticari faaliyetlerde kullanılmamasına neden olmuştur.

Bu sistem günümüze kadar pahalı olduğundan kurumsal uygulamalarda çok kısıtlı olarak kullanılmaktaydı. Son yıllarda RFID teknolojisi sağladığı kullanım kolaylıkları, ürün takip kesinliği, üretim ve stoklama bantlarında sağladığı kesinlik ve performans sebebiyle diğer kimlik tanıma sistemlerine nazaran daha çok ön plana çıkmıştır.

Radyo Frekansı ile kimlik tanımda radyo dalgaları metal-olmayan birçok yüzeyin içinden geçerek yayılabilirler. Bu sebeple bir paketin içindeki RFID etiketi, ya da kötü hava şartlarından zarar görmemesi için korunmuş, paketlenmiş ürünlerin içinde yer alan etiketler de rahatlıkla okunabilmektedir. Etiketlerdeki mikroçip içerisinde



saklanan seri numarasının tek olması (yani o numaranın dünyada başka bir eşi olmaması) da RFID' nin ürün takip ve kontrol sistemlerindeki yerini kaçınılmaz hale getirmektedir.

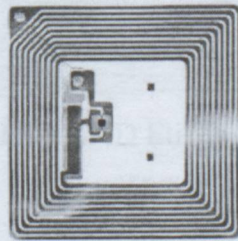
### 3.2 RFID Etiketler

RFID etiketi, sınırlı kapasitede belleğe sahip, taşınabilen bir modüldür. Bu modül bir kibrit çöpü boyutunda, kredi kartı ebatlarında veya 20 x 200 mm silindirik olabilir. Bazı yerlerde etiket yerine tag veya transponder ifadesi de kullanılmaktadır. RFID etiketleri her tür ürüne gömülebilir yada yapıştırılabilir.



**Şekil 3.1** RFID Etiketi

Son derece küçük olan bu etiketler içinde bilgi barındıran (ürün numarası üretici kodu, üretim tarihi, doz, ilaç adı... vb) birer mikro yonga ve yine minik birer antenden oluşurlar.



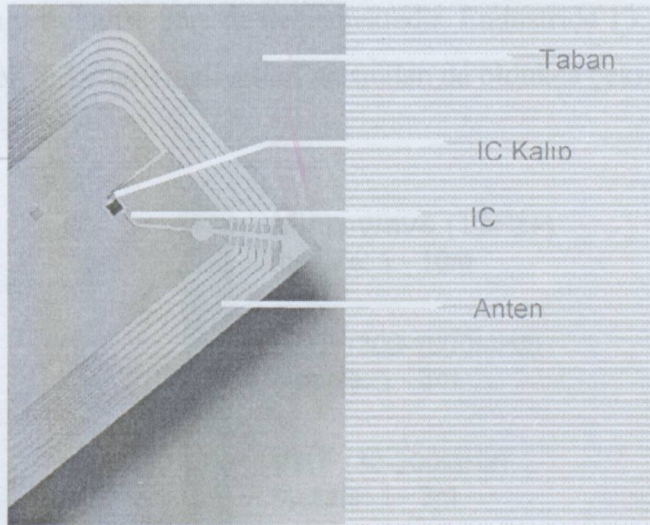
**Şekil 3.2** RFID Çipi



### 3.2.1 Fonksiyonlarına Göre RFID Etiketleri

RFID etiketlerin bazı modelleri içindeki bilgiyi koruyabilmek için pil kullanır. Bu tip etiketlere aktif etiket denir. **Aktif etiketler** okuma menzili bakımından pasif etiketlere (içinde pil bulunmayanlara) göre daha verimli olmasına rağmen pil bitme riski ve fiyat yüksekliği bakımından fazla tercih edilmezler. **Pasif etiketler** okuyucudan yayınlanan radyo frekansı ile kendisini enerjiler, okuyucudan gelen komutu değerlendirir ve cevabını gönderir.

Aktif RFID etiketleri bir verici ve bir güç kaynağına sahiptir. Pasif etiketlerse güç kaynağına sahip değildir. Yalnızca bir RFID okuyucu tarafından uyarıldıklarında sinyal yayar ve bilgi gönderirler. RFID okuyucular 1-3 metrede etkili bir elektromanyetik alan oluştururlar.



Şekil 3.3 RFID Etiket yapısı

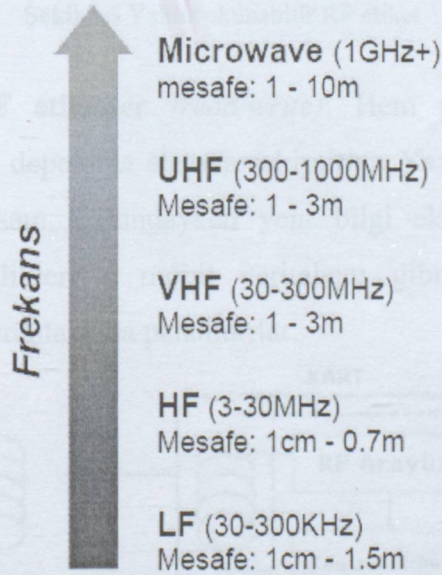
Pasif RFID etiketleri bu etki alanına girdiklerinde elektromanyetik alanın etkisi ile etkinleşir ve sinyal üretirler. Okuyucu bu sinyali alır ve bağlı olduğu bilgisayar sistemine iletir. Örneğin, hastane eczanesinde bulunan bir okuyucu kapıdan çıkan her serum şişesini satın alma ve depo programlarına bildirebilir. **Yarı aktif etiketler** ise çipin devrelerini harekete geçirmek için güç kaynağı kullanırken, iletişim kurmak için okuyucudan uyarı alırlar. Okuma işlemi yine okuyucunun yaydığı elektromanyetik alan yoluyla gerçekleşir.



Aktif ve yarı aktif etiketler uzun aralıklarla takip edilmesi gereken tren vagonları gibi yüksek değerli varlıklar için kullanılırlar, ancak pasif etiketlerden daha pahalı olduklarından düşük değerli varlıklarda kullanılamazlar. Bugün aktif etiketleri daha ucuza mal etmek için çalışmalar yapan firmalar bulunmaktadır. Son kullanıcılar 1 milyon ve daha fazla etiket için maliyeti 40 cent' ten daha düşük olan pasif etiketleri tercih etmektedir.

### 3.2.2 Frekanslara Göre RFID Etiketleri

RFID etiketlerinin ayırt edici bir diğer özelliği de çalıştıkları frekans aralıklarıdır. RFID etiketlerinin çalışma frekanslarını aşağıdaki tabloda görebilirsiniz. Günümüzde yaygın olarak kullanılan etiketlerin frekansları daha çok HF (High Frequency) - yüksek frekans aralığındadır. Bir etiketin maliyeti sadece aktif ya da pasif olmasına göre değil, çalıştığı frekansa göre de değişmektedir. Endüstride 13.56 MHz' lik etiket kullanılan projeler, şirketlere maliyetleri açısından da oldukça çekici gelmektedir.



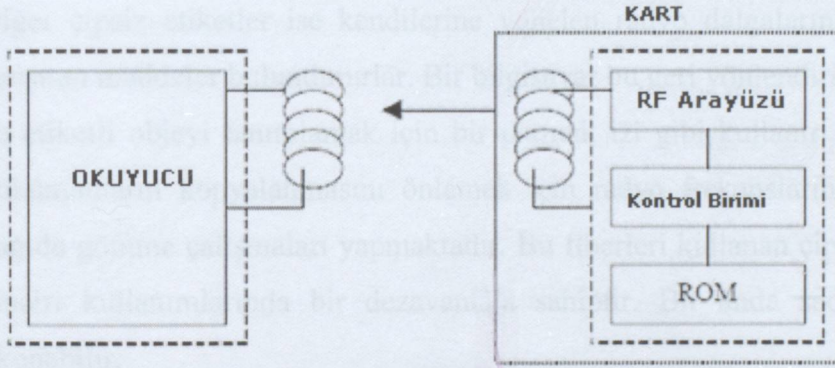
Şekil 3.4 Frekans Aralığı Mesafeler



### 3.2.3 Bellek Tipine Göre RFID Etiketleri

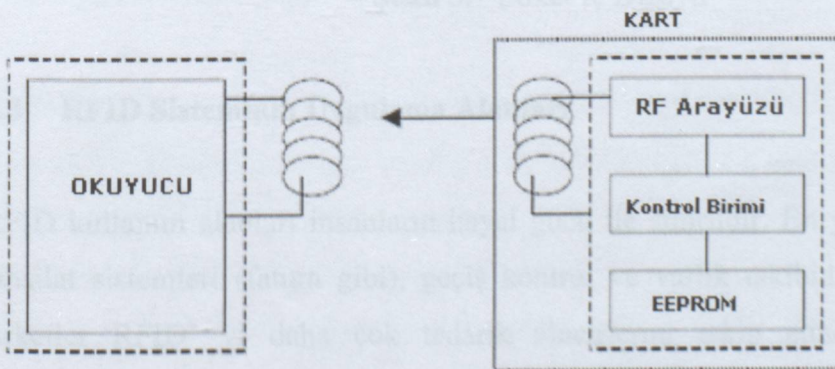
RFID etiketlerindeki mikroçipler 3 çeşittir: Sadece okunabilen, hem okunup hem yazılabilen, bir kez yazılıp birçok kez okunabilen (WORM-Write Once Read Many).

**Yalnız okunabilir RF etiketler (read-only):** Genellikle pasif RF etiketlerdir. Daha düşük bilgi depolama alanına sahiptirler. Üretim sırasında üzerlerine depolanan bilgiyi saklarlar. Bu bilgi değiştirilemez. Bu nedenle genellikle yalnız tanıtıcı etiket olarak kullanılırlar. Bu tip etiketlerin kullanıldığı sistemlerde merkezi bilgisayar sistemi ve veritabanı nesnelere ilgili tüm işlemlerin kontrolünü gerçekleştirir.



Şekil 3.5 Yalnız okunabilir RF etiket

**Okunup yazılabilir RF etiketler (read/write):** Hem pasif hem de aktif RF etiketlerdir. Yüksek bilgi depolama alanına sahiptirler. Yazılabilme özelliği olan bu etiketlere, okuyucu kapsam alanındayken yeni bilgi eklenebilir ya da bilgileri değiştirilebilir. Bu özellikleriyle mobil veritabanı gibi davranabilirler. Yalnız okunabilir RF etiketlere oranla daha pahalıdırlar.



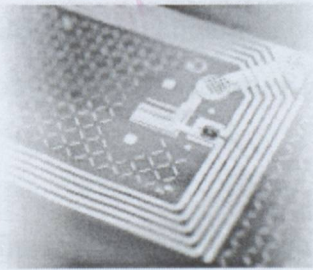
Şekil 3.6 Okunabilir yazılabilir RF etiketler



**Bir defa yazılıp sürekli okunabilen** (*write-once read-many WORM*) : Üretim sırasında üzerlerine sadece bir defa bilgi depolanabilen RF etiketlerdir. Kapasitesine bağlı olarak talep edilen bilgi üretici tarafından etikete yüklenir ve bir daha değiştirilemez.

### 3.2.4 Çipsiz RFID Etiketi

Çipsiz RFID etiketi, data aktarımı için radyo frekanslarını kullanan fakat silikon bir mikroçipte seri numarası bulundurmeyen sistemlere verilen isimdir. Bazı çipsiz etiketler silikon mikroçipler yerine plastik ya da iletken polimerler bulundurlar. Diğer çipsiz etiketler ise kendilerine yönelen radyo dalgalarının bir kısmını geri yansıtan maddeler bulundurlar. Bir bilgisayar bu geri yönlendirilen dalgaları algılar ve etiketli objeyi tanımlamak için bir parmak izi gibi kullanır. Şirketler bazı gizli dokümanların kopyalanmasını önlemek için radyo frekanslarını yansıtan fiberleri kağıda gömme çalışmaları yapmaktadır. Bu fiberleri kullanan çipsiz etiketler tedarik zinciri kullanımlarında bir dezavantaja sahiptir. Bir anda sadece tek bir etiket okunabilir.



**Şekil 3.7** Etiket İç Dizayn

### 3.3 RFID Sisteminin Uygulama Alanları

RFID kullanım alanları insanların hayal gücü ile sınırlıdır. En yaygın uygulamalar tahsilat sistemleri (fatura gibi), geçiş kontrol ve varlık takibidir. Son zamanlarda şirketler RFID' yi daha çok tedarik zincirlerini takip etmek gibi süreçlerde kullanmaktadır. Bu zamana kadar RFID' nin bu alanda yaygınlaşmasını engelleyen başlıca faktörler ise standartlar ve maliyettir.



RFID okuyuculardan yüksek maliyetli olanlarını kullanan bazı şirketler, tüm fabrikalarını, depolarını, dağıtım merkezlerini, bayilerini kapsamak için binlerce okuyucu kullanmak durumunda kalırlar. Eğer bir şirket kendi bölgesi içerisinde ürün takibi yapıyorsa RFID etiketlerini defalarca kullanabilir. Fakat tedarik zincirinin açık olduğu bir sistemde etiketlerin ucuz olması gerekir çünkü paketin üzerine konan etiket bir daha kullanılmayacaktır. 20 cent ya da daha fazla tutan RFID etiketler tedarik zincirinin açık olduğu sistemler için kullanılabilir olmanın dışında kalmaktadır.

Birçok firma avantajlarından faydalanmak için RFID' ye yatırım yapmıştır. Bu yatırımlar genellikle kapalı devre sistemlerden oluşmaktadır (ürün ya da varlık şirket içinden çıkmadığı sistemler). Çünkü firmalar aynı üretici tarafından üretilmiş RFID cihazlarını ve sistemini kullanmadığında A şirketi bir ürününe bir RFID etiketi yaptırdı ise, bu etiket B şirketi tarafından okunamamaktadır.

Ayrıca düşük ve yüksek frekanslı RFID sistemleri için geliştirilen standartlar bulunmaktadır. Birçok şirket kendi tedarik zinciri sisteminde UHF kullanmak ister. UHF teknolojisi yeni sayılabilecek bir teknolojidir ve bu sebeple standartlar henüz yeni yeni oturmaktadır. Teknoloji standartlaştıkça, RFID tedarik zinciri yönetiminde daha çok kullanılacaktır.

RFID teknolojisi süreç takibinden depo yerleşimine kadar pek çok alanda yararlı olabilir. Amaç idari hataların, barkod tarama sırasındaki işçilik kayıplarının, şirket içi hırsızlığın, sevkiyat hatalarının ve stok düzeylerinin azaltılmasıdır.

Bugün dünyada iç verimliliğini artırmak için RFID kullanan binlerce firma vardır. Bu yüzden RFID için sadece tek bir alan ya da sektörde kullanılır denemez. Bugün büyük alışveriş merkezlerinde, zincir marketlerde, hayvan takiplerinde, havayolları-kargo şirketlerinde kullanılan örnekleri vardır. Bu teknoloji ile şirketlerin avantajları, zamanla azalan insan gücü maliyeti, otomatikleştirilmiş stok kontrolü, ürün takibi ve anında ulaşılabilen envanter bilgisidir. Ayrıca RFID sayesinde şirketlerin iş süreçleri hızlanarak, ihtiyaç duyulan gelişmiş raporları hızlı ve doğruluğu yüksek bir şekilde



almak mümkün olabilmektedir. RFID' nin günümüz sektörlerindeki uygulama alanları tablo 3.1 de belirtilmiştir.

**Tablo 3.1 RFID Uygulama Alanları**

### Lojistik



RFID sistemler ile lojistik alanında katma değeri oldukça yüksek uygulamalar geliştirilebilmektedir. Depo yönetimi, liman yönetimi, üretim, taşımacılık ilk aklı gelen lojistik uygulamalarıdır.

### Fabrika Otomasyonu



Otomotiv ve beyaz eşya gibi çok fazla malzemenin bir araya getirilmesiyle yapılan üretimlerde RF teknolojilerinden yararlanılarak üretimin hızı ve kalite düzeyi artırılabilir.

### Otomotiv



Üretimden son satışa noktasına değin uzanan süreç içerisinde araçların takibi ve stok kontrolü için kullanılmaktadır.

### Oteller, Tatil Köyleri, Aquaparklar



Personel verimliliğini artırıcı projeler ayrıca ziyaretçiler için değer yaratacak uygulamalar gerçekleştirilmektedir.

### Sağlık Sektörü



Sağlık kuruluşları RFID' yi hastaların ilaçlarını zamanında verebilmek ve tıbbi cihazlardan yeterli verimi almak için kullanabileceklerini düşünmektedir.

### Askeri Uygulamalar



Hassas ve tehlikeli malzemenin takibi, personelin yönlendirilmesi ve kontrolü başlıca kullanım alanlarıdır.



### İnsanlar üzerinde Uygulama

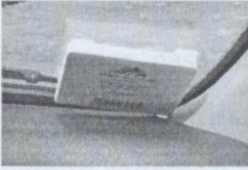
İnsan eline RFID çip yerleştirilmesi planı



RFID çip yerleştirilmiş İnsan eli:



### Araç Kimliklendirilmesi



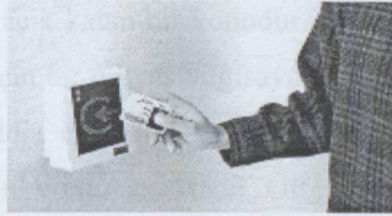
Otoyollar, Otoparklarda kullanılan OGS-OKS sistemleri vb.

### Perakende (Süpermarketler)



Perakende şirketleri, RFID teknolojisinin tedarik zincirini daha verimli hale getireceğine, hırsızlık ve malların kaybolması nedeniyle doğan sorunların önüne geçeceğine inanıyor.

### İnsan Kimliklendirilmesi



(Fabrikalar, Hastaneler, Okullar ...)

## 3.4 RFID Sisteminin Güncel Uygulamaları

RFID hakkında en son geliştirilen ve tartışılan uygulamalardan biri Pasaportlarda RFID teknolojisinin uygulanmasıdır. Bir diğeri de önüne geçilemeyen lisans hakkı ödenmeden kullanılan CD ve DVD kopyalamalarıdır. Bu iki konuda geliştirilen RFID uygulamalarının detayı aşağıda verilmektedir.

### 3.4.1 Pasaportlarda RFID Teknolojisi

ABD pasaportlarında kullanılması düşünülen RFID teknolojisi için ilk adım Infineon firması ile atılmıştır. Pasaport içerisine gömülecek olan RFID çipi, kişiler hakkında bilgileri içereceği gibi sayısal resimlerini de saklayacaktır.



Uygulamaya göre bu çipler üzerindeki veriler "50den fazla bireysel güvenlik mekanizması" ile korunacaktır. Örneğin, Temel Erişim Kontrolü (Basic Access Control (BAC)) teknolojisi ile okuyucunun çip üzerindeki veriye ulaşması için yetkilendirme yapılması sağlanmaktadır. Kullanılan çipler, 10 cm mesafeden veri transferi yapabilmektedir. Yetkisiz okumaların engellenmesi için BAC' in yanında, okuma voltajını değiştiren alıcılar, çip üzerindeki aktif koruyucu kalkanlar ve veriyi şifrelemede kullanılan karmaşık kodlama yöntemleri gibi güvenlik önlemleri de alınmıştır.

Ancak tüm bu güvenlik önlemlerine rağmen elektronik pasaportlar üzerinde ciddi tartışmalar olan bir konudur. Almanya, Norveç, İsveç'in de aralarında bulunduğu 20 ülke bu teknolojiyi kullanmaya ve sınamaya başlamış olsa da, bu pasaportların güvenliğinin gerçekten nasıl sağlanabileceği açık kalan bir konudur. Bu uygulamayı çıkaranlar, pasaport verisinin çözülebilmesi için bir milyar bilgisayarın bir milyar yıl çözüm için birlikte çalışması gerektiğini iddia etse de; bazı güvenlik uzmanları, verinin çalınması için çözülmesi gerekmediğini vurgulamaktadır. Ortamda elektronik bir pasaport olduğunu algılamanın bile bazı durumlarda yeterli bir tehdit oluşturacağı ifade edilmektedir.

### 3.4.2 Kopya DVD' ye Karşı RFID

Günümüzde üzerinde çalışılan bir RFID uygulaması da, sinema sektöründeki soruna çözüm aramaktadır. En bilinen film yapımcılarından Warner, Disney ve Fox için DVD ve CD üreten Tayvan firması, disklerin içerisine kopyalamayı önlemek amacıyla RFID çipleri yerleştirmiştir. Bu yöntemle, kopyalanmış disklerin, RFID okuyucular ile donatılan DVD/CD çalarlar tarafından okunmaması sağlanılmaya çalışılmıştır. DVD/CD çalarlar, diske gömülü çipi kontrol ederek "yanlış bir coğrafi alanda" izlenmeye çalışılan veya kopya olan diskleri okumayı reddedebilecek bir yapı kazanmaktadır. Blue-Ray ve HD-DVD disklerin de korunmasını sağlayacak bu yöntem ile film yapımcılarının diskleri fabrikalardan, raflara hatta evlere kadar uzaktan takip edebilecekleri bir sistem geliştirilmiş olmaktadır.



### 3.5 RFID Sisteminin Gelecekteki Uygulamaları

Radyo Frekansı ile kimlik tanıma (RFID) halen gelişmekte olan bir teknoloji olduğundan kullanım modelleri ve bütünleşik mimarisi sürekli değişmektedir. RFID hızlı bir şekilde geleceğe hazırlanmakta; teknolojik gelişmeler, endüstriyel standartlardaki gelişmeler ve bu alana yapılan yatırımlar da RFID' yi parlak bir geleceğin beklediğini işaret etmektedir.

Günümüzde oldukça düşen etiket fiyatları, özellikle 2007-2008 yıllarında dalga dalga RFID kullanımı tetikleyecek unsur olarak görülmektedir. Şu anda -özellikle ABD'de- çok büyük perakendeciler, market zincirleri ve ordu RFID teknolojisini etkin bir şekilde kullanmak için çalışmalar yapmaktadır.

RFID teknolojisi, hücresel telefonlardan sonra en hızlı gelişecek kablosuz teknoloji olarak görülmektedir ve 2009 yılına kadar %120'lik bir artış beklenmektedir. RFID çalışmaları yönünü, radyo vericilerinin daha iyi yayın yapmasını sağlayabilecek olan Nano teknoloji kullanmaya doğrultmuştur. Çünkü RFID kullanımının yaygınlaşması için anahtar gereklilik 0.3-0.5 Dolar civarında olan etiket fiyatlarının düşmesidir. Nano teknolojinin bu seviyeyi 0.05 Dolara kadar düşürmesi ve RFID' nin yaygın kullanımını sağlaması beklenmektedir.

RFID etiketlerin birçoğu bakır veya alüminyum antenler kullanmaktadır. Nano teknoloji üreticileri ise bu antenleri nano boyutlarda parçalardan oluşan mürekkep baskı kullanarak yapmayı başarmak için uğraşmaktadırlar. Kağıt üzerine antenler basmak daha hızlı ve ucuz üretim sağlayacaktır. RFID etiketlerinin maliyetinin yarısını, üzerlerindeki çipler oluşturmaktadır, bu nedenle araştırmacılar bu çip kullanım yönteminin nano boyutlarda çözülmesi üzerine çalışmaktadırlar.

RFID mikroçiplerin kapasite artırımı konusunda ise Micromem firması "manyetik RAM" veya MRAM üzerinde çalışmaktadır. MRAM, RFID teknolojisine büyük yenilikler ve fırsatlar getirecektir. Elektrik enerjisini saklamak mantığına dayalı var olan bilgisayar belleklerinin aksine, MRAM, nano boyutlardaki manyetik bit dizileri ile bilgiyi saklar. MRAM üzerine yazma işlemi, her bir bit'in manyetik kutuplarını



değiştirerek yapılır ve bu değer elektrik gereksinimi duymadan saklanabilir. Bunun yanında, “flash memory” olarak tabir edilen hafıza cihazlarının aksine MRAM’ ler radyasyona karşı da dirençlidirler. Bu özelliği ile MRAM’ lerin, havayolları ve askeri alanlar gibi yerlerde bulunabilen X- ışını uygulamalarında kullanılabilirlikleri daha yüksektir.

Gelecekteki nano teknoloji uygulamaları, mürekkep tabanlı RFID devrelerini mümkün kılarak silikon çip gereksinimini ortadan kaldıracaktır. Bunun en iyi örneği tamamen mürekkepten geliştirilen bir prototip olan “Organik ID” dir ve maliyeti 0.01 doların altındadır. Organik ID’ nin 5-10 yıl arasında yaygınlaşması beklenmektedir.

### 3.6 RFID Sistem Seçimi İçin Kriterler

Bir RFID uygulamasına başlarken öncelikle, yapılacak uygulama için;

- Doğru frekansın belirlenmesi
- Doğru etiket belirlenmesi
- Doğru okuyucunun belirlenmesi
- Kullanılacak yazılım programının belirlenmesi

ve bu malzemelerin tedariki gerekmektedir.

Gereklilik duyulan sisteme ve okuma mesafesine uygun etiket seçildikten sonra istenilen bilgiler etikete yazılır. Belirlenen okuma noktalarında sistem için seçilen uygun okuyucular tarafından etiket içindeki bilgiler bilgisayara aktarılır. Şimdi uygulama için sistemi oluşturan parçaların en uygun olanının seçimindeki etken faktörleri inceleyelim.

Bir uygulamada frekans ve etiket seçimine etkili olan faktörler, istenilen okuma mesafesi, etiketler arasındaki mesafe, istenilen bilgi okuma hızı ve performans maliyet oranıdır. Uygulama adımlarını tek tek incelenerek karar verirken nelere dikkat edilmesi gerektiği belirtilecektir.



### 3.6.1 Doğru Frekansın Seçilmesi

Öncelikle o bölgede / ülkede geçerli olan çalışma frekansları bilinmelidir. Dünyamızda en çok kullanılan alçak frekanslar 134 KHz ve yüksek frekanslar 13.56 MHz USA, Kanada, Japonya, Avrupa da altyapı olarak desteklenmektedir. Bölgede izin verilen frekans opsiyonları bilindikten sonra en uygun frekansın belirlenmesine geçilir.

Frekansın seçiminde ne kadarlık bir okuma mesafesine ihtiyaç duyulduğu öncelikli kriterdir. Okuma mesafesi birçok etkene bağlıdır; okumanın sıklığı, okuyucunun gücü, diğer RF araçlarıyla çakışma...vs. Genelde düşük frekanslı etiketler 0.33 m ve daha az uzaklıktan okunabilir. Yüksek frekanslı etiketler 1 m' den, UHF etiketler ise 3-7 metreden okunabilir. Daha büyük uzaklıklar gerektiğinde, aktif etiketler güç kaynağı kullanarak 100 m ve daha fazlasını destekleyebilir.

Doğru frekansın belirlenmesi aslında o projenin düşünülen ortamda gerçekleştirilip gerçekleştirilemeyeceğini belirler. Çünkü Radyo dalgaları “çok yüksek frekanslar” da (UHF) metalden yansır, şeker ve su tarafından yutulur. Bu işlem metal veya yüksek su içeren ürünlerin takibinde problem yaratır, ancak iyi bir sistem tasarımı ve mühendislik çalışması bu problemi ortadan kaldıracaktır. Düşük ve yüksek frekanslardaki etiketler (LF-HF) su içeren ve metal olan ürünlerde daha iyi sonuç verirler. Bu yüzden metal otomotiv parçalarının takibi için düşük frekanslı (LF) RFID etiketleri kullanılır. Yapılacak uygulamaya göre frekans seçimi bu yüzden önem arz etmektedir.

### 3.6.2 Doğru Etiket Seçilmesi

Hangi etiketin kullanılacağına karar verirken, ihtiyaç duyulan okuma mesafesi belirlenmelidir. Buna göre etiketlerin aktif mi pasif mi olduğu belirlenecektir. Her ne kadar aktif etiketlerin okuma mesafesi uzun olsa da, pasif etiketlere nazaran daha pahalı ve daha büyük boyuttadırlar. Bu yüzden yapılacak uygulamada ebadı küçük ve az maliyet öncelikli ise pasif etiket seçilmelidir.



Aşağıdaki tablodaki bilgiler kullanılarak sinyal gücüne, okuma mesafesine, etiketin bataryalı olup olmamasına, çoklu etiket okuma ve veri depolama hacmi özelliklerine göre pasif mi aktif mi etikete ihtiyaç duyulduğuna karar verilebilir.

**Tablo 3.2 Özelliklerine Göre Aktif ve Pasif Etiketlerin Karşılaştırması**

	<b>Aktif RFID</b>	<b>Pasif RFID</b>
<b>Güç Kaynağı</b>	Etiketin içinde	Okuyucudan gelen Radyo dalgaları transferi ile
<b>Batarya</b>	Var	Yok
<b>Gerekli sinyal gücü</b>	Çok düşük	Çok yüksek
<b>Okuma Menzili</b>	100m'ye kadar	(Okuyucunun anten özelliklerine göre)3-5m'ye kadar, genellikle daha az
<b>Veri depolama</b>	Tekrar yazılabilir	Genellikle sadece okuma
<b>Maliyet</b>	Pahalı	Ucuz

Aktif etiket veya pasif etiketin hangisinin kullanılacağına karar verildikten sonra, bu seçime göre etiketin ihtiyaçlarının giderilmesi düşünülmelidir. Eğer aktif etikete karar verildiyse, bu durumda etiketin ömrünün ne kadar olması gerektiği belirlenmelidir. Çünkü birçok aktif etiket 1-2 yıl gibi kısa ömürlüdür ve süresi dolduğunda değiştirilmesi gerekmektedir. Gerçi dıştan güç kaynaklı olan ömrü uzatılabilir aktif etiketler de vardır. Eğer pasif etiket gerektiğine karar verildiyse, ne kadar sağlamlıkta bir etikete ihtiyaç duyulduğu belirlenmelidir. Bu etiketin boyutunu, materyalini ve fiyatını etkileyecektir. Genellikle uzun okuma menzili sağlanması, daha geniş ebatlı pasif etiket gerektirir.

### 3.6.3 Doğru Okuyucunun Seçilmesi

Etiketin okunmasında uygulama için en doğru okuyucu seçilmelidir. Tüm etkenlerin yanı sıra doğru okuyucunun seçilmesinde en önemli etken, ihtiyaç duyulan okuma mesafesidir.



Alçak frekanslarda 125 - 134 KHz kullanıldığında pasif etiketlerde, ne kadar iyi bir okuma mesafesine ihtiyaç duyuluyorsa, o kadar yüksek güçte okuyucuya ve o kadar geniş çaplı antene ihtiyaç duyulmaktadır. Aktif etiket kullanılması durumunda, anten seçimi daha kritik hale gelmektedir. Bu, okuyucunun hem boyutunu hem maliyetini etkilemektedir. Birçok uygulamada taşınabilir okuyucuya ihtiyaç duyulmaktadır. Bunlar pasif etiketlerin okunmasında kullanılan tipik antenlerdir.

**Tablo 3.3 Pasif ve Aktif RFID Etiketleri**

<b>Aktif Etiketler</b>		<b>Pasif Etiketler</b>	
<b>Avantajları</b>	<b>Dezavantajları</b>	<b>Avantajları</b>	<b>Dezavantajları</b>
Daha uzun okuma mesafesi	Daha geniş ebat	Daha küçük ebat	Kısa okuma mesafesi
Okuyucu menziline kendinden aktive olur	Sınırlı operasyon ömrü	Uzun operasyon ömrü	Daha yüksek güçte okuyuculara ihtiyaç duyar.
Hem okunur-hem yazılabilir	Daha pahalı	Daha ucuz	Çoğu sadece okunabilir



#### 4 RFID FREKANS BANDLARI

RFID sistemleri çok sayıda farklı frekans kullanmakla beraber, en yaygın olanları düşük frekans (125 KHz civarı), yüksek frekans (13.56 MHz) ve çok yüksek frekans ya da UHF (860-960 MHz)' dir. Ayrıca 2.45 GHz mikrodalgalar da bazı uygulamalarda kullanılmaktadır. Radyo dalgaları farklı frekanslarda farklı özellikte olduklarından, uygulama için uygun frekansın seçilmesi gereklidir.

**Tablo 4.1 RFID Frekans Bandları**

Band	Frekans Aralığı	Uygulama
Alçak Frekans (LF)	120-135 KHz	Kısa mesafe uygulamalar
Yüksek Frekans (HF)	13.56 MHz	Akıllı kartlar ve etiketler için kullanılan frekans
Ultra Yüksek Frekans (UHF)	433MHz	Aktif düşük güçlü etiketler
	860-960MHz	Tedarik Zinciri uygulamaları
Mikrodalga	2450MHz	Aktif etiketlerle daha büyük haberleşme mesafeleri ve daha yüksek hızlarda data iletimi

**Tablo 4.2 RFID ETSI Frekansları**

	ETSI 300-220	ETSI 302-208
<b>Frekans</b>	869.4 - 869.65 MHz	865 - 868 MHz
<b>Band Genişliği</b>	0.25 MHz	3 MHz
<b>Maksimum Güç</b>	0.5 Watt ERP	2 Watt ERP
<b>Kanal</b>	1	15



RFID teknolojisinin ülkelere göre çalışma frekansları aşağıdaki tabloda gösterilmektedir.

**Tablo 4.3 Ülkelerde kullanılan RFID çalışma frekansları**

Ülkelerde kullanılan RFID çalışma frekansları	
Frekans	Ülkeler/ Bölgeler
125 – 134 KHz	USA, Kanada, Japonya, Avrupa
13.56 MHz	USA, Kanada, Japonya, Avrupa
433.05 – 434.79 MHz	Avrupa'nın büyük bölümü, USA (bazı bölgelerde aktif etiket FCC ye kayıt edilmesi şartı ile), Japonya (henüz işlem aşamasında)
865 - 868 MHz	Avrupa
866 - 869 ve 923 - 925 MHz	Güney Kore
902 – 928 MHz	USA
952 – 954 MHz	Japonya
2400–2500 ve 5.725 – 5.875 GHz	USA, Kanada, Avrupa, Japonya

Frekanslar farklı karakteristiklere sahiptir. Örneğin düşük frekanslı etiketler daha az güç kullanırlar ve metal olmayan cisimleri algılamada daha iyidirler. Meyve gibi yüksek su içeren cisimlerde idealdirler, ancak okuma kapasiteleri düşüktür (0.33 metre). Yüksek frekanslı etiketler metal cisimlerde daha iyidirler ve su içeren cisimler için de kullanılabilirler. 1 metreden çok rahat okunabilirler.

UHF frekansı daha yüksek okuma kapasitesine sahiptir ve düşük ve yüksek frekanslara göre veri aktarımını daha hızlı yaparlar. Ancak çok fazla güç kullanırlar ve cisimle aralarında görüş engeli olmamalıdır. Bu yüzden etiket ile okuyucu arasında net bir iletişim yolu olmalıdır. UHF frekanslı etiketler bir deponun kapısından girişi yapılan kutuların taranması için daha iyidir. Uygulama için doğru frekansı seçilmesi çok önemlidir. Günümüzde en sık kullanılan ve pazar tarafından en çok talep edilen frekans 13.56MHz'dir.



**Tablo 4.4 Frekans Bandları ve Uygulamalar**

Frekans Bandı	Uygulamalar
433.5 - 434.5 MHz	Avrupa'da ISM bandı kullanılmaktadır. Japonya ve Kore'de uygulanmak üzere planlanmaktadır.
865 - 868 MHz	ETSI 302-208 düzenlemeleri sonucunda tanımlanan spektrum
869.4 - 869.65 MHz	Avrupa'da RFID ve diğer uygulamaları için lisans gerektirmeyen bandda ayrılmış 250 kHz' lik spektrumdur.
902 - 928 MHz	Kuzey Amerika'da yayılı spektrum haberleşmesi için ayrılmış lisans gerektirmeyen banddır.
918 - 926 MHz	ERP 1 Watta kadar müsaade edilen Avustralya standardıdır.
950 -956 MHz	Japonya'da RFID uygulamaları için ayrılmıştır.
2.4 GHz (mikrodalga)	Dünyanın birçok ülkesinde lisans gerektirmeden yayılı spektrum uygulamaları için tanımlanmış olan banddır. Bluetooth ve WLAN uygulamaları için de kullanılmaktadır. (IEEE 802.11b ve 802.11g)

Aşağıdaki tabloda, alçak frekans, yüksek frekans, çok yüksek frekans ve mikrodalga frekansları ve özellikleri görülmektedir.

**Tablo 4.5 Frekans Bandları ve Özellikleri**

<b>Alçak frekans - (Low Frequency -LF &lt;135 KHz)</b>
<ul style="list-style-type: none"> <li>• Tipik olarak pasif, sadece okunabilir veya okunur-yazılır etiketler kullanılır.</li> <li>• Etiketler ucuz ama anten açısından sistem uzun ve pahalı bir bakır antene ihtiyaç duyar.</li> <li>• Metal ve sıvıların performansı düşüren etkilerinden en az etkilenilen frekanstır.</li> <li>• LF kısa okuma mesafesine ve düşük okuma hızına sahiptir.</li> <li>• Diğer frekanslara nazaran daha geniş boyutlara sahip etiket kullanılır.</li> </ul>



**Yüksek Frekanslar – (High Frequency -HF - 13.56 MHz)**

- Tipik olarak pasif, sadece okunabilir, okunur-yazılır veya bir kere yazılıp çok kez okunabilen WORM etiketler kullanılır.
- Uzun okuma menziline ihtiyaç duyamayan çoklu etiket uygulamaları için iyi uyumlu.

**Çok yüksek Frekanslar – (Ultra-High Frequency UHF- 868 MHz- 915 MHz)**

- Aktif veya pasif sadece okunabilir, okunur-yazılır veya bir kere yazılıp çok kez okunabilen WORM etiketler kullanılır.
- HF –Yüksek frekanslara nazaran daha yüksek menzil kapasitesi, daha fazla veri transferi ve hızlı tanımlama imkanı sunar.
- Özellikle çoklu etiket okumada mesafe ve performans arasında iyi bir denge sağlar.

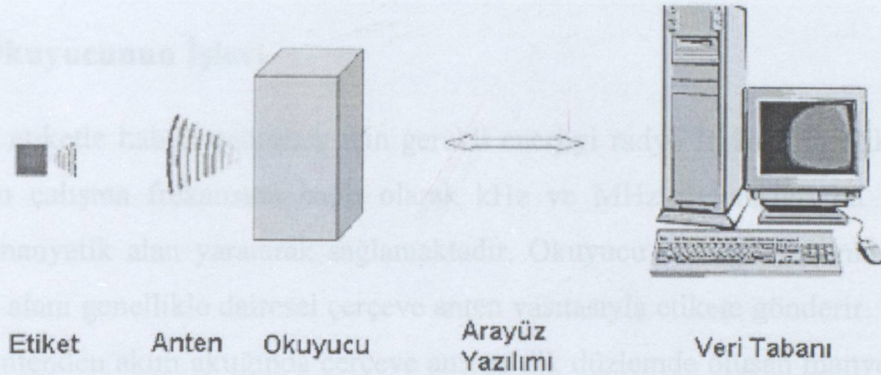
**Mikrodalga -Microwave (2.45 GHz, 5.8 GHz)**

- Aktif veya pasif sadece okunabilir, okunur-yazılır veya bir kere yazılıp çok kez okunabilen WORM etiketler kullanılır.
- UHF etiketlerine benzer karakter göstermekle beraber daha hızlı okuma oranına sahiptir.
- Maliyeti alçak frekanslarınkinin bazen iki katı olabilmektedir.



## 5 RFID SİSTEMLERİNİN YAPISI

Bu bölümde RFID sisteminin çalışma prensibi ve haberleşme yapısı açıklanacaktır. Radyo frekans tanımlama sistemleri, (şekil 5.1) radyo frekansı ile yapılan sorguları almaya ve cevaplamaya olanak tanıyan etiket (transponder), okuyucu (alıcı verici) ve alınan bilgilerin depolandığı veri tabanından oluşmaktadır.



**Şekil 5.1** Radyo frekans kimlik tanıma Sistem Bileşenleri

### 5.1 RFID Sisteminin Haberleşme Yapısı

Etiket, okuyucu tarafından gönderilen elektromanyetik alana girdiğinde aktif olur. Aktif olan etiket, sadece kendisine ait olan programlanmış kimlik bilgisini okuyucuya gönderir. Okuyucu, alıcı anteni yoluyla etiketin göndermiş olduğu bilgiyi alır, haberleşme için geliştirilmiş yazılımı kullanarak bilgiyi işlenmek ve depolanmak üzere gerekli veri tabanına iletir.

Radyo frekans kimlik tanıma sistemlerinde okuyucu antenleri küçük yarıçaplı olarak seçildiklerinde anten merkezinde büyük manyetik alan yaratırken, büyük mesafelerde  $x > R$  büyük yarıçapa sahip antenler büyük alan şiddeti yaratmaktadır. Bunun sonucu olarak RFID sistemlerinde verici/sorgulayıcı anten yarıçapları bu nedenle büyük seçilmelidir. RFID sistemlerinde okuma mesafesini maksimum yapmak için anten yarıçapını büyütme her zaman çözüm olmamaktadır. Maksimum okuma mesafesini



hesaplarken sorgulama alan şiddeti değeri de bilinmelidir. Aksi halde anten yarıçapının büyütülmesi alan şiddetinin  $x=0$  mesafesinde bile çok küçük olup sorgulama için gerekli enerjiyi sağlayamamasına sebep olur. Etiket okuyucu ile haberleşmesi için gerekli olan rezonans frekansından sapma gösterdiğinde haberleşme için büyük manyetik alan şiddetine ihtiyaç duyulur ki bu da haberleşme mesafesinin küçülmesine sebep olmaktadır.

### 5.1.1 Okuyucunun İşlevi

Okuyucu etiketle haberleşebilmek için gerekli enerjiyi radyo frekans kimlik tanıma sisteminin çalışma frekansına bağlı olarak kHz ve MHz frekanslarında zamanla değişen manyetik alan yaratarak sağlamaktadır. Okuyucu ürettiği zamanla değişen manyetik alanı genellikle dairesel çerçeve anten vasıtasıyla etikete gönderir. Dairesel çerçeve antenden akım aktığında çerçeve antene dik düzlemde oluşan manyetik alan şiddeti,

$$H = \frac{I.N.R^2}{2(R^2 + x^2)^{3/2}} \quad (5.1)$$

(1) olarak hesaplanmaktadır. Burada

$I$  = Çerçeve antenden akan akım

$N$  = Çerçeve anten sarım sayısı

$R$  = Anten yarıçapı

$x$  = Anten düzlemine dik doğrultudaki alıcı uzaklığını tanımlar.

Denklemden de görüleceği üzere manyetik alan şiddeti mesafenin küpü ile ters orantılıdır. Endüktif bağlaşım prensibine dayanan radyo frekans kimlik tanıma sistemlerinde alanın mesafenin küpüyle ters orantılı olarak zayıflaması ana sınırlayıcı faktördür. Okuyucu tarafından gönderilen radyo frekans enerjisi etiketin fonksiyonlarını yerine getirebilmesi için taşıyıcı sinyal içermektedir. İncelediğimiz durumda söz konusu taşıyıcı frekansı 13.56MHz'dir. Taşıyıcı sinyal etikete enerji



sağlamasının yanı sıra, etiketteki bilgilerin okuyucuya gönderilmesini ve haberleşmenin senkronizasyonunu sağlar. Etiket okuyucu tarafından gönderilen sinyali alır ve modüle ederek tekrar okuyucuya gönderir. Etiket tarafından gönderilen okuyucu antenine gelen sinyaller geri saçılım sinyalleri olarak adlandırılır. Okuyucu doğrultusunda geri saçılan sinyaller okuyucu tarafından şifresi çözülerek alınır.

### 5.1.2 Okuyucunun Tasarım ve Performansı

Pratikte kullanılan tipik bir yüksek frekans RFID okuyucu devre yapısı şekil 5.2 de verilmektedir. Okuyucu aynı zamanda alıcı-verici olduğundan alıcı ve verici kısımlarını içermektedir. Verici 13.56MHz frekansında sinyali osilatörde üretir, kuvvetlendirir, filtreler ve akord devresi yardımıyla antenden etiket doğrultusunda gönderir. Alıcı kısımda ise etiketin göndermiş olduğu bilgiler zarf dedektörü ile işlenir, filtrelenir ve kuvvetlendirilerek mikro kontrolöre veri tabanına gönderilmek üzere iletilir. (1) ifadesine göre anten yarıçapı artırıldığında manyetik alan şiddeti de artmaktadır. Diğer taraftan NI da artırıldığında H da artacaktır. Manyetik alan şiddetinin artırılması için her iki durumda da sınırlamalar mevcuttur. Anten yarıçapı büyütüldüğü zaman okuyucu portatif özelliğini kaybedecek ve maliyeti artacaktır. NI değeri artırıldığında okuyucu anten endüktansı artacak, yüksek endüktans yükü de büyük oranda geriye yansıyan güce sebep olacaktır. Sonuç olarak NI çarpanını mümkün olduğu kadar küçük tutup haberleşme için gerekli manyetik alan şiddeti seviyesini elde edecek sistem tasarlanmalıdır.

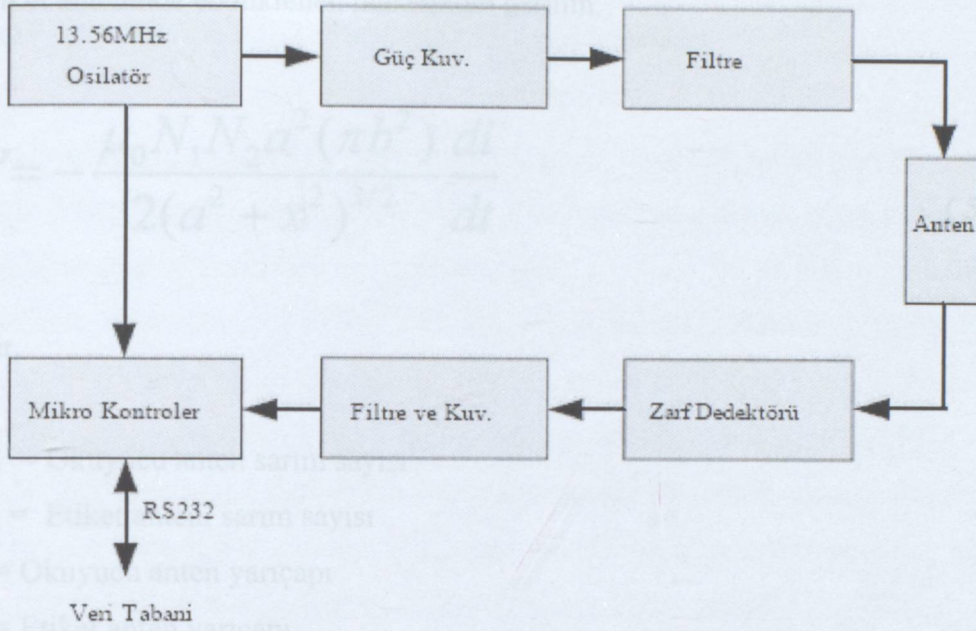
$$V = -N \frac{d\phi}{dt} \quad (5.2)$$

Ve manyetik akı

$$\phi = \int B \cdot dS \quad (5.3)$$

olarak hesaplanır. Manyetik alan şiddeti okuyucu anten ile etiket antenini paralel olarak durdurduğunda büyük edilir.





Şekil 5.2 RFID Okuyucu devre yapısı

### 5.1.3 Etiket'in İşlevi

Pasif radyo frekans kimlik tanıma etiketleri çalışması için gerekli gücü endüktif bağlaşımla antende endüklenen gerilimden alır.

Antende endüklenen gerilim [3],[4]

$$V = -N \frac{d\phi}{dt} \quad (5.2)$$

Ve manyetik akı

$$\phi = \int B \cdot dS \quad (5.3)$$

olarak hesaplanır. Maksimum manyetik akı okuyucu anteni ile etiket anteninin paralel olması durumlarında elde edilir.



Etiket anteninde endüklenen maksimum gerilim

$$V = - \frac{\mu_0 N_1 N_2 a^2 (\pi b^2)}{2(a^2 + x^2)^{3/2}} \frac{di}{dt} \quad (5.4)$$

dir.

$N_1$  = Okuyucu anten sarım sayısı

$N_2$  = Etiket anteni sarım sayısı

$a$  = Okuyucu anten yarıçapı

$b$  = Etiket anten yarıçapı

$x$  = Okuyucu ile etiket arasındaki uzaklık



Şekil 5.3 Okuyucu tarafından üretilen manyetik alan ile endüklendi kupaillanmış etiket

#### 5.1.4.1 Kuplaj Katsayısı k

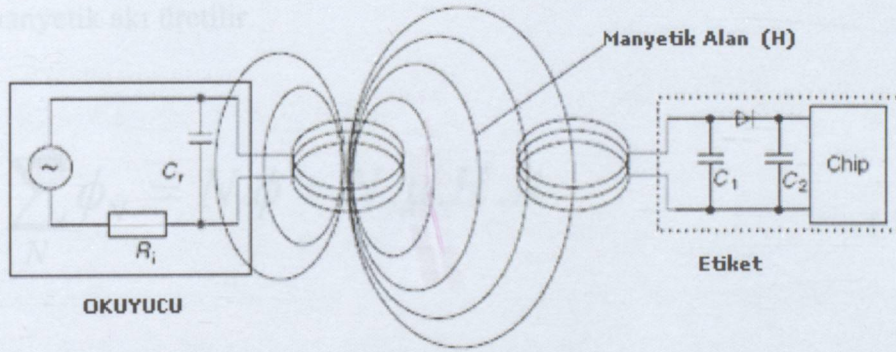
İki tane döngüselinin geometrik yapılarına bağlı kuplajı hakkında nitelikli bir tahmin yapılabilmesi için kuplaj katsayısı tanımlanmıştır. Kuplaj katsayısı aşağıdaki gibi formülize edilmiştir.

$$k = \frac{M}{\sqrt{L_1 L_2}} \quad (5.5)$$



### 5.1.4 Endüktif Kuplaj -Pasif etiketlere güç kaynağı

Endüktif kuplajlanan etiket, genellikle tek bir mikroçip ve anten görevi gören geniş yüzeyli bir bobinden oluşan bir elektronik data taşıyıcısı olarak işlem görür. Endüktif kuplajlanan etiketlerin hemen hepsi pasif olarak çalışır. Bu da mikroçip için gereken enerjinin tamamının okuyucu tarafından sağlanması gerektiğini ifade eder. Bu amaçla, okuyucu etiket üzerindeki bilgiyi okuyabilmek için gerekli enerjiyi etiket doğrultusunda gönderir. Çünkü kullanılan frekans aralığındaki (<135 kHz: 2400 m, 13.56 MHz: 22.1m) dalgaboyu, okuyucu anteni ve etiket arasındaki mesafeden birçok kat daha büyük olduğu için, elektromanyetik alan, etiket ve anten arasındaki mesafeye bağlı olarak, değişken manyetik alan gibi davranabilir.



**Şekil 5.3** Okuyucu tarafından üretilen manyetik alan ile endüktif kuplajlanan etiket

#### 5.1.4.1 Kuplaj Katsayısı k

İletken döngülerinin geometrik yapılarına bağlı kuplajı hakkında nitelikli bir tahmin yapılabilmesi için kuplaj katsayısı tanımlanmıştır. Kuplaj katsayısı aşağıdaki gibi formulüze edilmiştir.

$$k = \frac{M}{\sqrt{L_1 L_2}} \quad (5.5)$$



L1 ve L2 iki bobinin self endüktansdır. M ise ; iki iletken döngüsünün akı değişimi için tanımlanan karşılıklı endüktanstır. Endüktans ve Karşılıklı endüktans 5.1.4.2 ve 5.1.4.3 de kısaca açıklanmıştır.

Kuplaj Katsayısı her zaman şu iki değer arasındadır:  $0 \leq k \leq 1$ .

- $k = 0$ : geniş mesafeye veya manyetik ekranlamaya bağlı tam ayırım
- $k = 1$ : toplam kuplaj

Şekil 5.4 "L" endüktansının tanımı

#### 5.1.4.2 Endüktans L

Endüktans iletken bobinlerin karakteristik özelliklerinden biridir. Bilindiği gibi bir iletkenden akım geçirildiğinde, iletken etrafında bir manyetik alan oluşur. Böylelikle de bir manyetik akı üretilir.

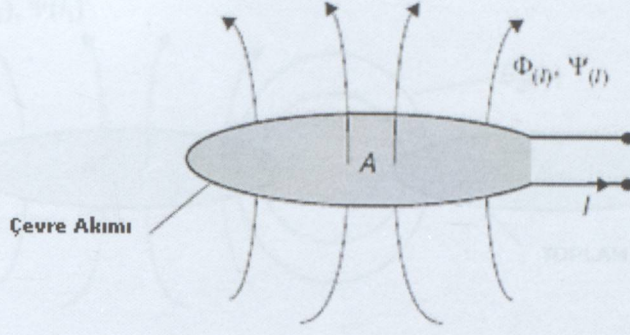
$$\psi = \sum_N \phi_N = N \cdot \phi = N \cdot \mu \cdot H \cdot A \quad (5.6)$$

Bu akının geçen akıma oranı endüktansı formulüze eder;

$$L = \frac{\psi}{I} = \frac{N \cdot \phi}{I} = \frac{N \cdot \mu \cdot H \cdot A}{I} \quad (5.7)$$

Bobinden geçen akımın oluşturduğu, bobin sargılarını çevreleyen bu manyetik alan kağıt üzerinde daireler şeklindeki kuvvet çizgileri ile sembolize edilir.





**Şekil 5.4** "L" endüktansının tanımı

Akımın artıp azalmasına ve yön değiştirmesine bağlı olarak bobinden geçen kuvvet çizgileri artıp azalır ve yön değiştirir. Bobinin sarım sayısı ve kesit alanı ne kadar büyük olursa, "L" o kadar büyük olur. Böylelikle okuyucu anten endüktansı  $L_1$  ve etiket anteninin endüktansı  $L_2$ 'nin büyük olması durumunda, kuplaj katsayısı küçülür.

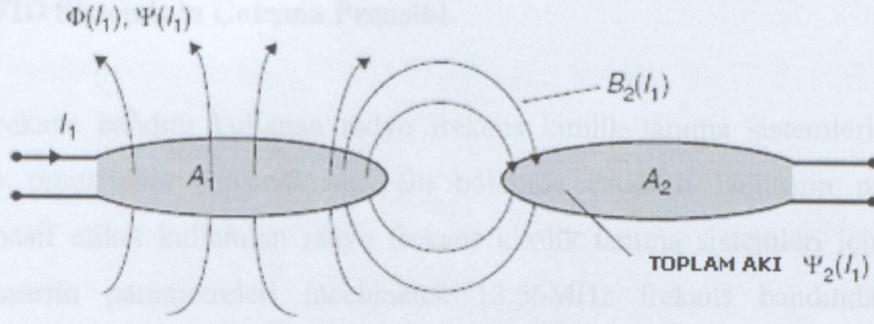
#### 5.1.4.3 Karşılıklı Endüktans (M)

Aynı nüve üzerine sarılı iki bobinin birinden akım geçirildiğinde, bunun nüvede oluşturduğu kuvvet çizgileri diğer sargıyı da etkileyerek, bu sargının iki ucu arasında bir gerilim oluşturur. Bu gerilime "endüksiyon gerilimi" denir.

Bu şekilde iletişim, karşılıklı (ortak) endüktans denen belirli bir değere göre olmaktadır. Karşılıklı endüktans M ile gösterilir ve şu şekilde ifade edilir:

$$M = L_1 . L_2 \quad (5.8)$$





Şekil 5.5 İki bobinin oluşturduğu karşılıklı endüktans

$$M = M_{12} = M_{21} \quad (5.9)$$

$$M_{12} = \frac{\mu_0 \cdot N_1 \cdot R_1^2 \cdot N_2 \cdot R_2^2 \cdot \pi}{2\sqrt{(R_1^2 + x^2)^3}} \quad (5.10)$$

$$M_{21} = \frac{\mu_0 \cdot N_1 \cdot R_1^2 \cdot N_2 \cdot R_2^2 \cdot \pi}{2\sqrt{(R_2^2 + x^2)^3}} \quad (5.11)$$



## 5.2 RFID Sisteminin Çalışma Prensibi

Alçak frekans bandını kullanan radyo frekans kimlik tanıma sistemleri endüktif bağlaşım prensibiyle çalışmaktadır. Bu bölümde endüktif bağlaşım prensibiyle çalışan pasif etiket kullanılan radyo frekans kimlik tanıma sistemleri için çerçeve anten tasarım parametreleri incelenerek 13.56MHz frekans bandında yapılan hesaplamalar ve optimizasyon anlatılmıştır.

### 5.2.1 Alçak Frekansta Anten Parametrelerinin Hesaplanması

13.56 MHz de çalışan endüktif bağlaşmalı radyo frekans kimlik tanıma sistemi etiket ve alıcı sistemi için hesaplamada kullanılan değerler;

$$I=1A$$

Alıcı verici anten yarıçapı 55cm, 7.5cm, 1cm

Alıcı verici ve etiket arasındaki uzaklık 0...20m

Etiket anten yarıçapı: 2cm

Rezonans devresi parametreleri;

$$L2=3.5mH$$

$$R2=5\Omega$$

$$RL=1.5k\ \Omega$$

Etiket özellikleri ISO 7810 standardına göre 85.72mmx54.03mmx0.76mm, çalışma frekansı 13.56 MHz alınarak hesaplamalar yapılmıştır.

Manyetik alan şiddetinin anten yarıçapı parametre olarak alındığında mesafeye göre değişimi şekil 5.6 de verilmektedir. Eğriden de görüleceği gibi çerçeve anten merkezine dik doğrultuda hareket edildiğinde merkezden uzaklaştıkça alan şiddeti azalmaktadır.

Yakın alanda ( $x < R$ ) manyetik alan şiddeti belli uzaklıklara kadar sabit değer almakta daha sonra ( $x > R$ ) hızla düşmektedir. Küçük yarıçapa sahip antenler anten merkezinde büyük manyetik alan yaratırken, büyük mesafelerde  $x > R$  büyük yarıçapa



sahip antenler büyük alan şiddeti yaratmaktadır. Bunun sonucu olarak RFID sistemlerinde verici/sorgulayıcı anten yarıçapları bu nedenle büyük seçilmelidir.

Manyetik alan şiddetinin mesafe parametre olarak alındığında anten yarıçapına göre değişimi şekil 5.7 de verilmektedir. Şekilden de görüleceği gibi optimum anten yarıçapının  $R=x\sqrt{2}$  değerinde elde edildiği görülmektedir.

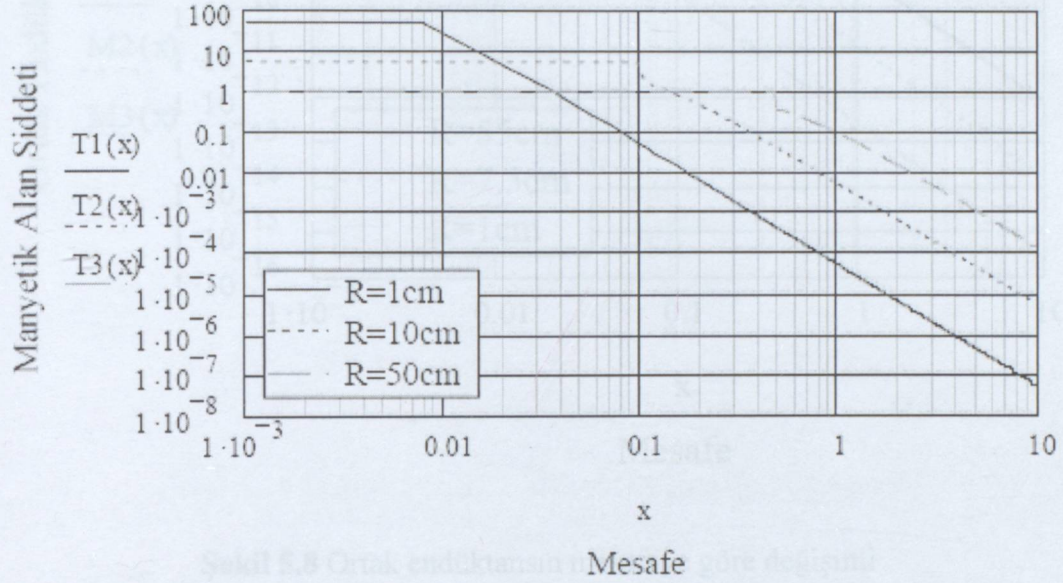
RFID sistemlerinde okuma mesafesini maksimum yapmak için anten yarıçapını büyütme her zaman çözüm olmamaktadır. Maksimum okuma mesafesini hesaplarken sorgulama alan şiddeti değeri de bilinmelidir. Aksi halde anten yarıçapının büyütülmesi alan şiddetinin  $x=0$  mesafesinde bile çok küçük olup sorgulama için gerekli enerjiyi sağlayamamasına sebep olur.

Verici ve okuyucu antenleri arasındaki ortak endüktansın anten yarıçapı parametre olarak alındığında mesafeye bağlı değişimi şekil 5.8 de verilmektedir. Ortak endüktansın mesafeye bağlı değişimi manyetik alan şiddetinin mesafeye bağlı değişimine benzemektedir.

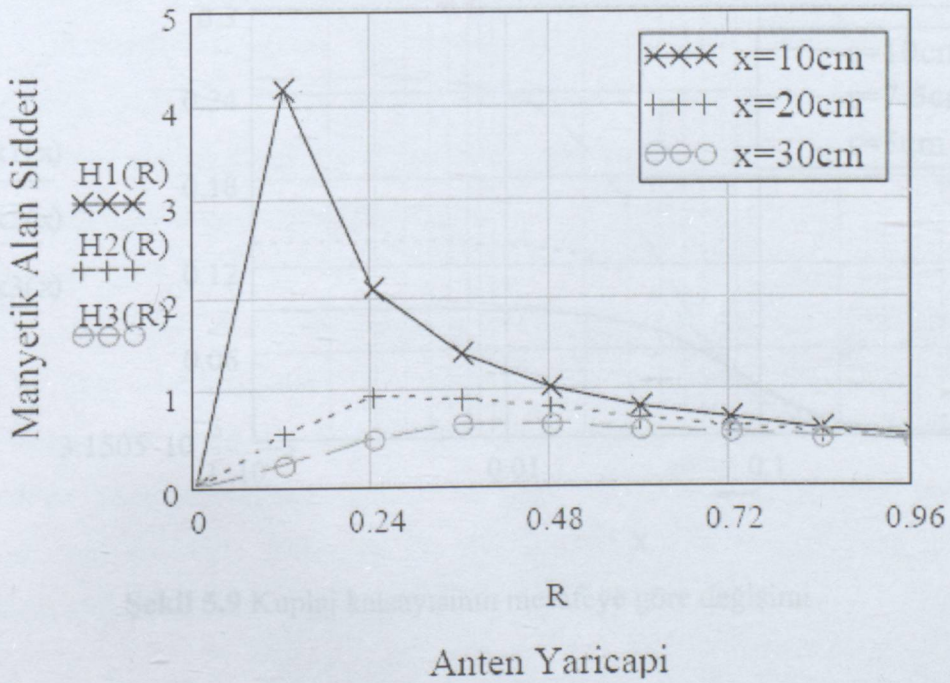
Etiket anten yarıçapı sabit okuyucu (alıcı-verici) anten yarıçapı parametre alındığında kuplaj katsayısının mesafeye bağlı değişimi şekil 5.9 de verilmektedir. Ortak endüktans okuyucu ve etiket antenleri arasındaki kuplajı nicel (quantitative) olarak tanımlarken kuplaj katsayısının antenlerin geometrik boyutlarından bağımsız nitel (qualitative) olarak tanımlamaktadır. Sıfır ile Bir arasında değer alan kuplaj katsayısı  $k=0$  durumunda her iki anten arasındaki mesafenin çok büyük olduğu ve/veya antenler arasında manyetik ekranlamanın mevcut olduğu duruma karşılık gelmektedir.  $k=1$  durumunda ise tam kuplaj söz konusudur. 13.56MHz de çalışan radyo frekans kimlik tanıma sistemi için sorgulama alan şiddetinin frekansa göre değişimi şekil 5.10 da verilmektedir. Okuyucu etiket haberleşmesinde okuyucunun haberleşmesi için gerekli minimum manyetik alan şiddeti bilindiğinde okuyucu ile etiket arasındaki mesafede hesaplanabilir. Etiket okuyucu ile haberleşmesi için gerekli olan rezonans frekansından sapma gösterdiğinde haberleşme için büyük



manyetik alan şiddetine ihtiyaç duyulur ki bu da haberleşme mesafesinin küçülmesine sebep olmaktadır.

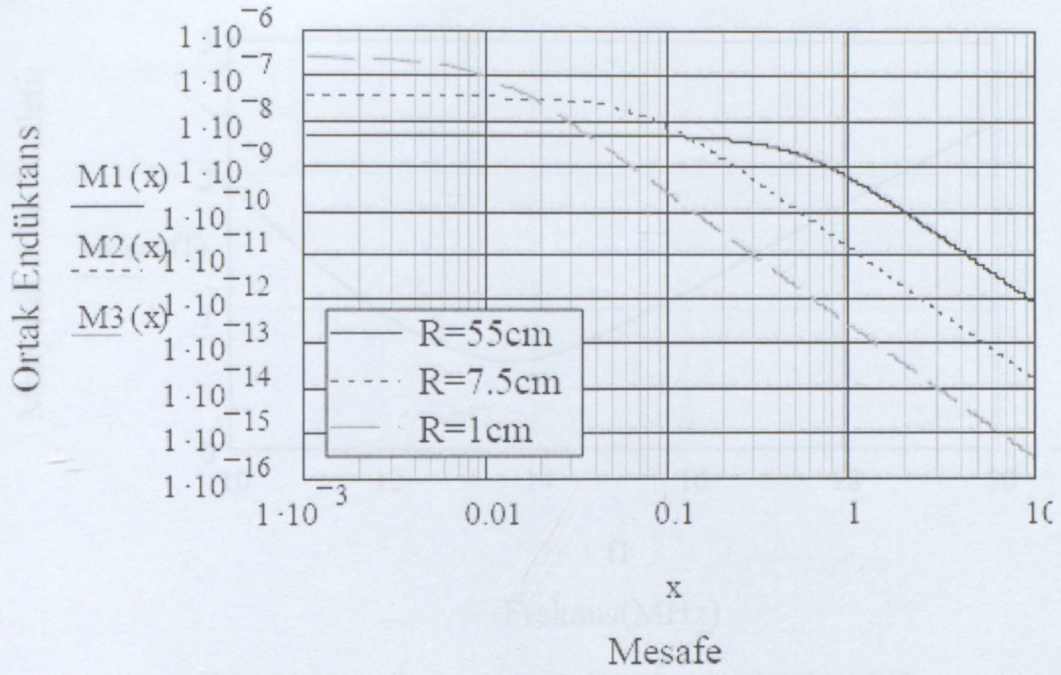


Şekil 5.6 Manyetik alan şiddetinin mesafeye göre değişimi

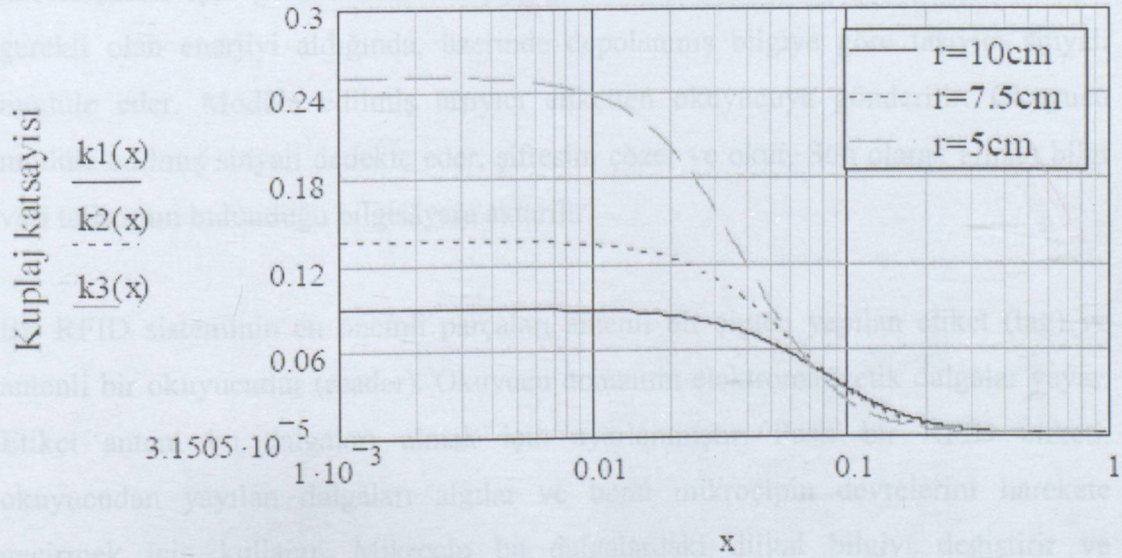


Şekil 5.7 Manyetik alan şiddetinin anten yarıçapına göre değişimi



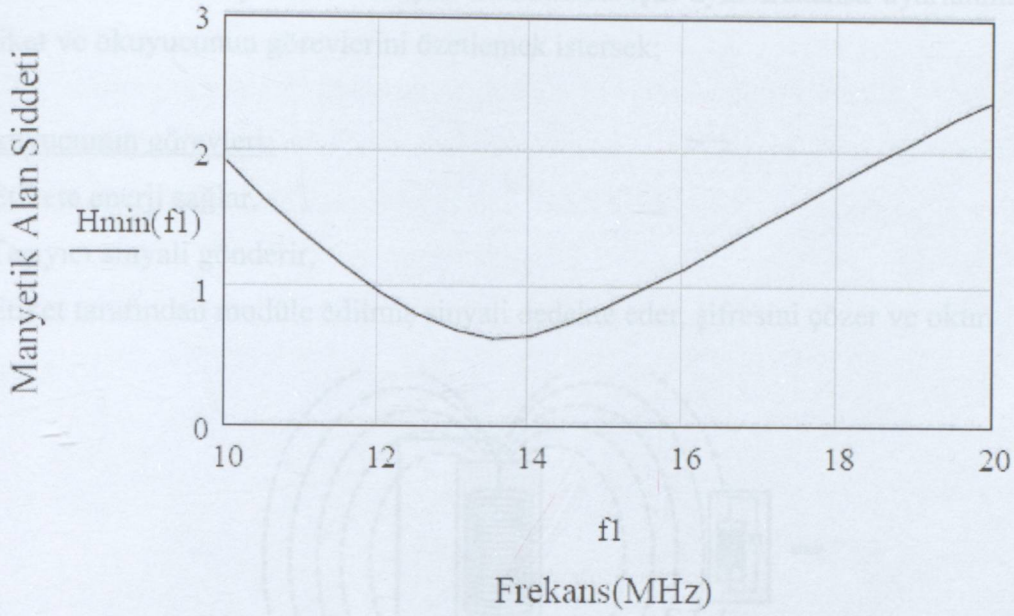


Şekil 5.8 Ortak endüktansın mesafeye göre değişimi



Şekil 5.9 Kuplaj katsayısının mesafeye göre değişimi





**Şekil 5.10** Manyetik alan şiddetinin frekansa göre değişimi

Radyo frekans kimlik tanıma sistem haberleşmesinde okuyucu radyo frekans sinyallerini gönderir. Okuyucunun radyo frekans alanına girmiş bulunan etiket, haberleşmesi için gerekli olan enerjiyi bu alandan alır. Etiket haberleşmesi için gerekli olan enerjiyi aldığı anda, üzerinde depolanmış bilgiye göre taşıyıcı sinyali modüle eder. Modüle edilmiş taşıyıcı etiketten okuyucuya gönderilir. Okuyucu modüle edilmiş sinyali dedekte eder, şifresini çözer ve okur. Son olarak alınan bilgi veri tabanının bulunduğu bilgisayara aktarılır.

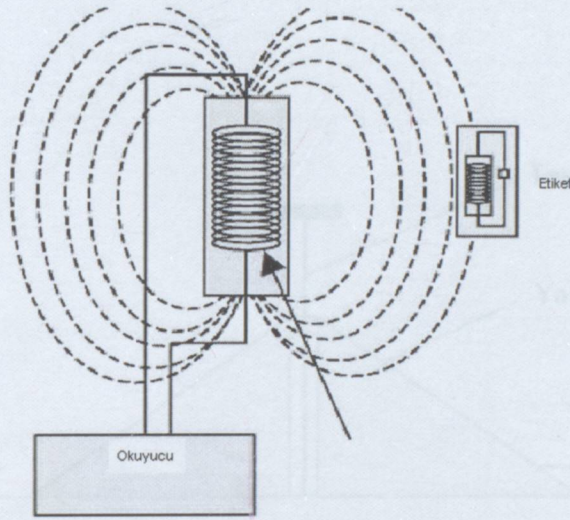
Bir RFID sisteminin en önemli parçaları antenli bir çipten yapılan etiket (tag) ve antenli bir okuyucudur (reader). Okuyucu donanımı elektromanyetik dalgalar yayar. Etiket anteni bu dalgaları almak için ayarlanmıştır. Pasif bir RFID etiketi, okuyucudan yayılan dalgaları algılar ve bunu mikroçipin devrelerini harekete geçirmek için kullanır. Mikroçip bu dalgalardaki dijital bilgiyi değiştirir ve okuyucuya geri gönderir.



RFID etiket ve okuyucuları iletişim kurabilmek için aynı frekansa ayarlanmalıdır. Etiket ve okuyucunun görevlerini özetlemek istersek;

Okuyucunun görevleri:

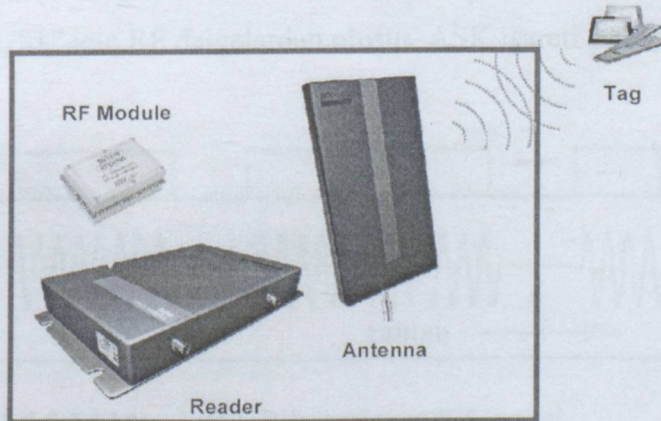
- Etikete enerji sağlar,
- Taşıyıcı sinyali gönderir,
- Etiket tarafından modüle edilmiş sinyali dedekte eder, şifresini çözer ve okur.



**Şekil 5.11** Etiket ve Okuyucu Etkileşimi

Etiket görevleri:

- Okuyucunun gönderdiği enerjiyi alır,
- Etiket içinde depolanmış bilgiye göre taşıyıcı sinyali modüle ederek okuyucuya gönderir.



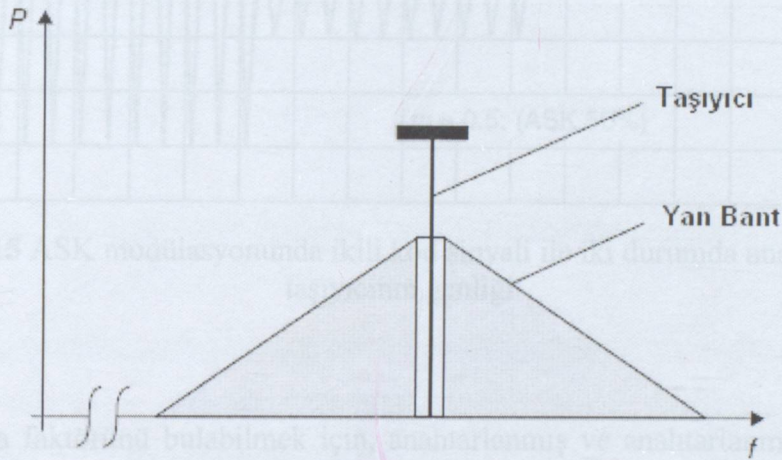
**Şekil 5.12** RFID Haberleşme Yapısı



## 5.2.2 RFID Sistemlerinde Kullanılan Modülasyon Yöntemleri

RFID Sistemlerinde Kullanılan modülasyon yöntemleri; Genlik Kaydırmalı Anahtarlama (ASK), Faz Kaydırmalı Anahtarlama (PSK) ve Frekans Kaydırmalı Anahtarlama (FSK) modülasyonlu sistemleridir.

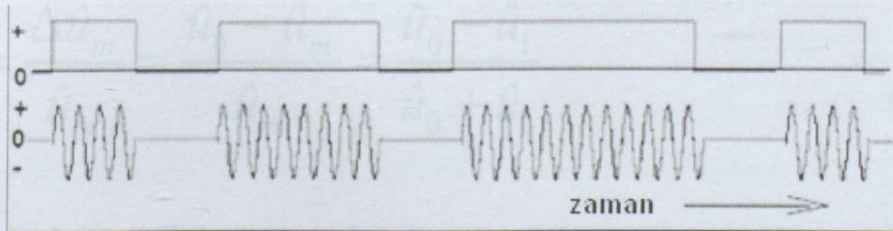
Her modülasyon prosedüründe simetri olduğundan taşıyıcının etrafında yan bantlar üretilir.



Şekil 5.13 Sinüzoidal sinyal modülasyonu (taşıyıcı ve yan bantlar)

### 5.2.2.1 ASK Modülasyonu : Genlik Kaydırmalı Anahtarlama (ASK)

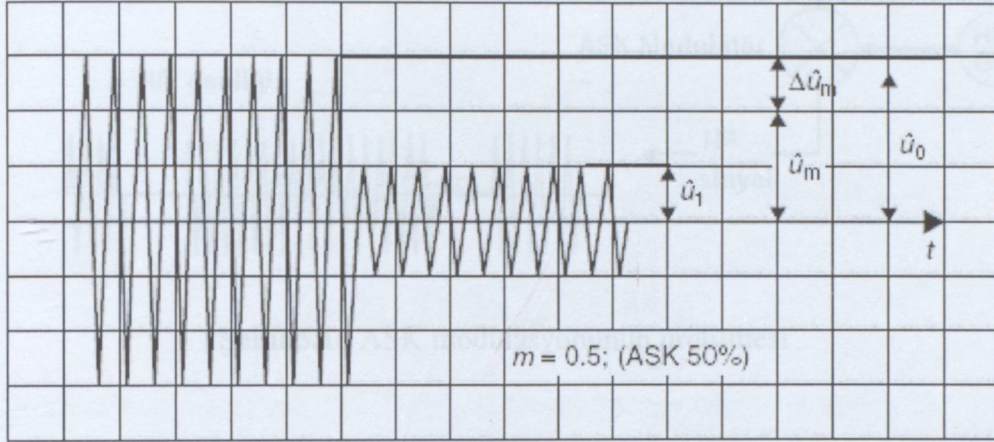
Bu Modülasyon tipinde, taşıyıcı işaretin genliği iki veya daha fazla değer arasında anahtarlanır. İkili durumunda genellikle var-yok anahtarlama kullanılır. ASK dalga biçimi "0" için boşluk, "1" için RF dalgalarından oluşur. ASK işareti şekildeki gibidir.



Şekil 5.14 Mesaj (Bilgi) işareti ve ASK işareti



Genlik kaydırmalı anahtarlama modülasyonunda, taşıyıcı salınımasının genliği  $u_0$  ve  $u_1$  durumlarında ikili kod sinyali ile anahtarlanır. " $u_1$ ";  $u_0$  ve 0 arasında değer alır.  $u_0$ ,  $u_1$  oranı " $m$ ", çalışma faktörü olarak bilinir.



**Şekil 5.15** ASK modülasyonunda ikili kod sinyali ile iki durumda anahtarlanan taşıyıcının genliği

" $m$ " çalışma faktörünü bulabilmek için, anahtarlanmış ve anahtarlanmamış taşıyıcı sinyal genliğinin aritmetik ortalaması hesaplanır.

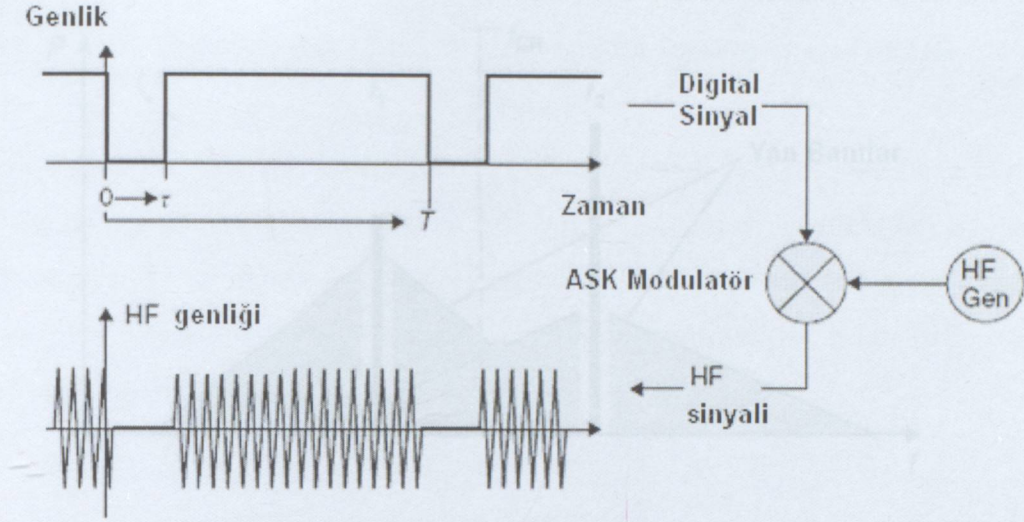
$$\hat{u}_m = \frac{\hat{u}_0 + \hat{u}_1}{2} \quad (5.12)$$

Daha sonra  $\hat{u}_0 - \hat{u}_m$  genlik değişiminin, elde edilen  $\hat{u}_m$  değerine oranı ile " $m$ " çalışma faktörü, bulunur.

$$m = \frac{\Delta \hat{u}_m}{\hat{u}_m} = \frac{\hat{u}_0 - \hat{u}_m}{\hat{u}_m} = \frac{\hat{u}_0 - \hat{u}_1}{\hat{u}_0 + \hat{u}_1} \quad (5.13)$$

Şekil 5.16 da ikili kod sistemi kullanan ASK modülatörü, HF generatöründen üretilen sinuzoidal taşıyıcı sinyali kullanarak HF sinyalini üretir.

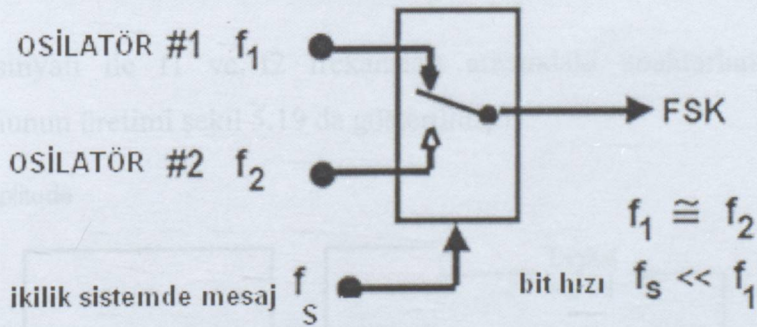




Şekil 5.16 ASK modülasyonunun üretilmesi

### 5.2.2.2 FSK Modülasyonu : Frekans Kaydırmalı Anahtarlama (FSK)

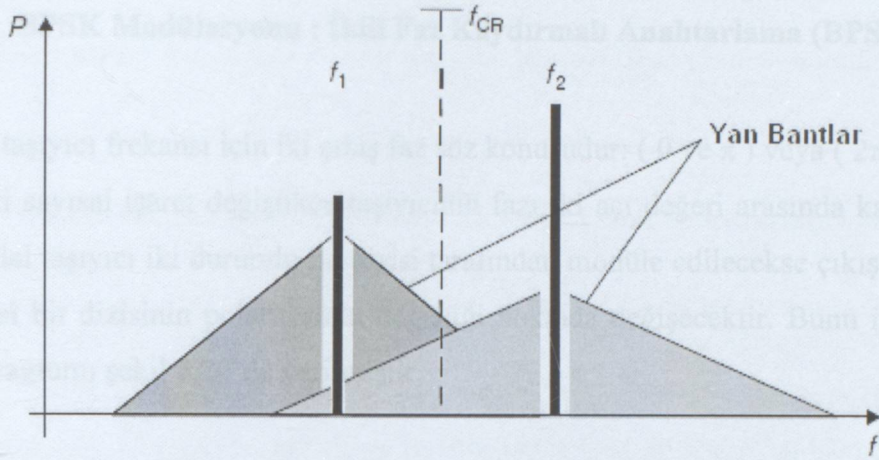
FSK modülasyonunda, taşıyıcı işaretin ani frekansı, sayısal işarete bağlı olarak iki veya daha çok değer arasında anahtarlanır. FSK işaretin üretimine ilişkin blok diyagram Şekil 5.17' de verilmiştir.



Şekil 5.17 FSK üretimi

2 FSK modülasyonunun spektrumu,  $f_1$  ve  $f_2$  frekanslarının genlik kaydırmalı anahtarlama osilasyonlarının bireysel spektrumlarının eklenmesiyle elde edilir.



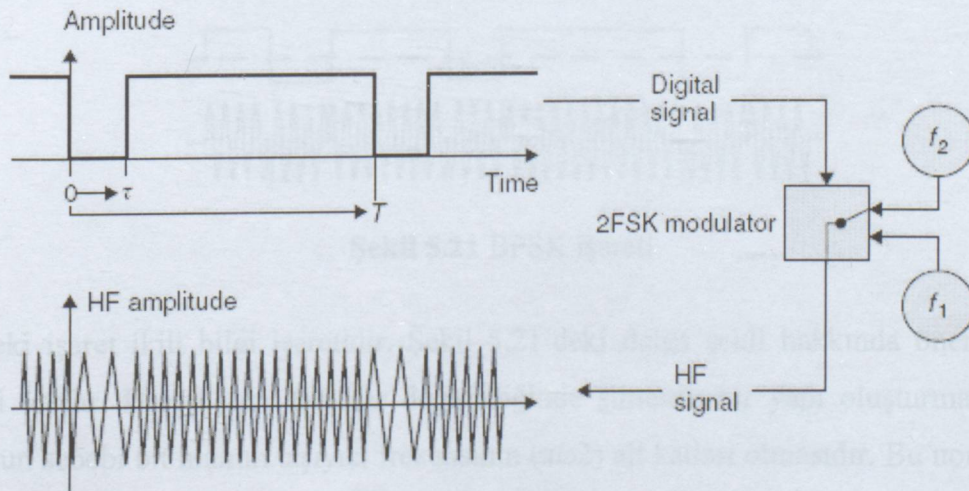


Şekil 5.18 FSK modülasyonu

Taşıyıcı frekansı  $f_{CR}$ ,  $f_1$  ve  $f_2$  karakteristik frekanslarının aritmetik ortalaması alınarak hesaplanır. Karakteristik frekanslar ve taşıyıcı frekans arasındaki fark frekans sapması olarak adlandırılır.

$$f_{CR} = \frac{f_1 + f_2}{2} \quad ; \quad \Delta f_{CR} = \frac{|f_1 - f_2|}{2} \quad (5.14)$$

İkili kod sinyali ile  $f_1$  ve  $f_2$  frekansları arasındaki anahtarlama ile 2 FSK modülasyonunun üretimi şekil 5.19 da gösterilmiştir.

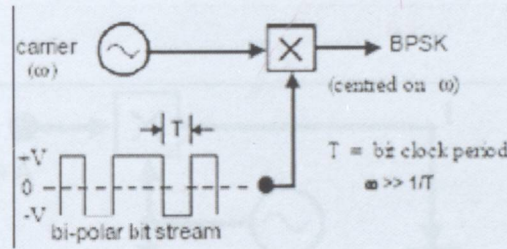


Şekil 5.19 2 FSK modülasyonunun üretimi



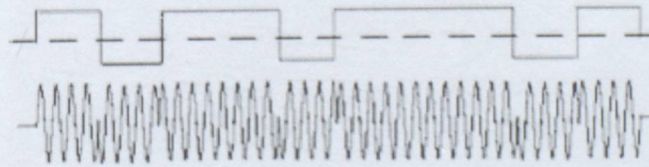
### 5.2.2.3 BPSK Modülasyonu : İkili Faz Kaydırmalı Anahtarlama (BPSK)

Tek bir taşıyıcı frekansı için iki çıkış faz söz konusudur: ( $0$  ve  $\pi$ ) veya ( $2\pi$  ve  $23\pi$ ). Girişteki sayısal işaret değiştikçe taşıyıcının fazı iki açı değeri arasında kayar. Eğer sinüzoidal taşıyıcı iki durumlu bit dizisi tarafından modüle edilecekse çıkış işaretinin polaritesi bit dizisinin polaritesinin değiştiği noktada değişecektir. Bunu ifade eden blok diyagramı şekil 5.20'de verilmiştir.



Şekil 5.20 BPSK işaretinin üretilmesi

Bit dizisi, hakkında bilgi gönderilecek BPSK işaretinin fazının değişimlerini içermektedir. Bir senkron demodülatör bu faz değişimlerine duyarlı olması gerekmektedir.



Şekil 5.21 BPSK işareti

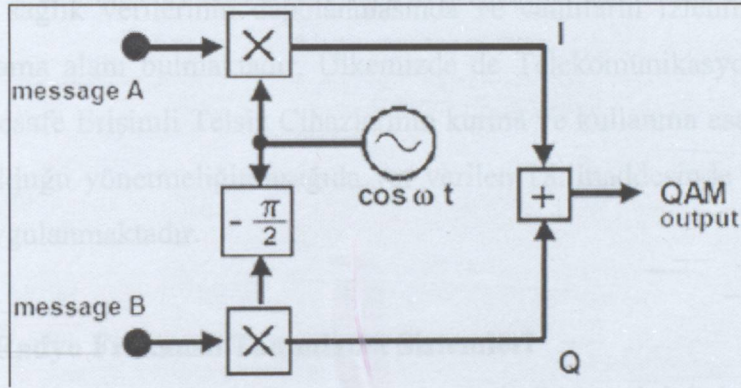
Üsteki işaret ikili bilgi işaretidir. Şekil 5.21'deki dalga şekli hakkında önemli bir bilgi vardır. Dalga şekli her faz değişikliğinde simetrik bir yapı oluşturmaktadır. Bunun sebebi bit hızının taşıyıcı frekansının ( $\pi\omega/2$ ) alt katları olmasıdır. Bu normalde özel bir durum olarak bakılabilir ve her zaman pratikte gözlemlenemeyebilir. Bu durum bize alınan işareten kolay bir şekilde bit dizisinin elde edilmesini



sağlamaktadır. Verimli haberleşme sağlamak için bir band sorunu olabilir, bu sorun (band sınırlanması) ise ya temel-band' da yada taşıyıcı frekansında halledilmektedir.

#### 5.2.2.4 QPSK Modülasyonu : Çeyrek Faz Kaydırmalı Anahtarlama (QPSK)

Bu modülasyonda birbirinden bağımsız iki tane A ve B analog işaret modülatörün girişine uygulanmaktadır. Modülatör önceleri QAM modülatörü olarak adlandırılmıştır. Daha sonra QPSK modülatörü olarak adlandırılmaya başlanmıştır.



Şekil 5.22 QAM modülatörü (QPSK modülatörü)

Tablo 5.1 Radyo Frekanslı Telekomünikasyon Sistemleri Teknik Kriterleri

Frekans Bandı	Çıkış gücü (erp)	Anten tipi	Kanal aralığı	Açıklama
2446-2454 MHz	500mW	Yarıdalgı yayıcı		



### 5.2.3 RFID Sistemlerine Telekomünikasyon Kurumunca Getirilen Standartlar

Radyo frekans tanımlama sistemleri için spektrum kullanımı Avrupa Posta ve Telekomünikasyon Birliği (European Conference of Postal and Telecommunications Administrations-CEPT) tarafından düzenlenmiş ve standartlar tanımlanmıştır. Spektrumun Türkiye’de kullanımı ise 06.03.2004 tarih 25394 sayılı Resmi gazetede yayınlanan “Kısa Mesafe Erişimli Telsiz Cihazlarının (KET) Kurma ve Kullanma Esasları” yönetmeliği uyarınca Telekomünikasyon Kurumu tarafından belirlenmiştir. RFID sistemleri tedarik zincirinde, lojistik uygulamalarında, envanter tutulmasında, perakende satışta ödeme sistemlerinde, otoyol ve VIP geçişlerinde, erişim kontrolünde, sağlık verilerinin depolanmasında ve canlıların izlenmesinde yaygın olarak uygulama alanı bulmaktadır. Ülkemizde de Telekomünikasyon Kurumunun KET-Kısa Mesafe Erişimli Telsiz Cihazlarının kurma ve kullanma esasları hakkında yayınlamış olduğu yönetmeliğin aşağıda yer verilen 18. maddesinde geçen esaslara tabi olarak uygulanmaktadır.

#### Madde 18- Radyo Frekanslı Tanımlama Sistemleri

Fabrika, depo, antrepo ve büyük alışveriş merkezleri gibi kapalı lokal alanlarda ya da mülkiyeti kullanıcıya ait kampüs veya açık alanda frekans sinyalleri yoluyla, veri iletimi, dosyalama, depolama, yer belirleme, depo arşivleme, yakınlık sensörü, el cihazlarından data transferi, kablosuz etiket vb. işlemleri yapan ve sadece dahili kullanıma izin verilen sistemler, aşağıdaki tabloda belirtilen kriterlere uygun olmak kaydıyla kullanılır.

**Tablo 5.1 Radyo Frekanslı Tanımlama Sistemleri Teknik Kriterleri**

Frekans Bandı	Çıkış gücü (erp)	Anten tipi	Kanal Aralığı	Açıklama
2446-2454 MHz	500mW	Tümleşik ve dahili	-	-



RF Algılayıcı (Dedektör) ve İkaz Cihazları için yönetmeliğin 11. maddesi uygulanmaktadır.

**Madde 11-** Kaybolması, çalınması veya belirli bir bölgeden geçişin önlemesi amacıyla, önceden etiketlenmiş nesnelere tespit etmeye yarayan cihazlar, aşağıdaki tabloda belirtilen kriterlere uygun olmak kaydıyla kullanılır.

**Tablo 5.2 RF Algılayıcı (Dedektör) ve İkaz Cihazları Teknik Kriterleri**

Frekans Bandı	Çıkış gücü (maksimum)	Anten tipi	Kanal Aralığı	Açıklama
2400-2483.5 MHz	25 mW	Tümleşik veya dahili	-	-
9200-9500 MHz	25 mW	Tümleşik veya dahili	-	-
9500-9975 MHz	25 mW	Tümleşik veya dahili	-	-
24.05-24.25 MHz	100mW	Tümleşik veya dahili	-	-

Endüktif Sistemler için yönetmeliğin 14. maddesi esas alınmaktadır.

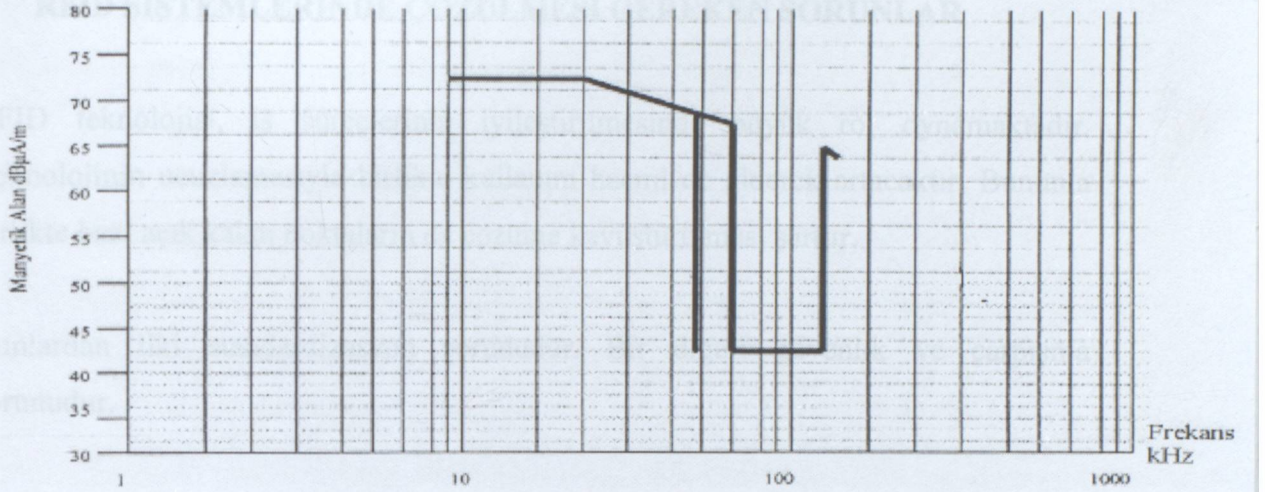
**Madde 14-** Bina içinde veya dışında ve dar bir alanda kullanılan, araç güvenlik sistemi, hayvan tanımlama, hırsız alarm sistemleri, çevre atık kontrolü, kablo dedektörü, kimlik tanımlama, kablosuz ses linkleri, giriş kontrolü, süreç kontrolü, sensörler, güvenlik sistemleri, otomatik madde tanımlama, kablosuz kontrol sistemleri, otomatik oto yol ücret toplama vb. uygulamaları kapsayan Endüktif Sistemler, tablo 5.3 de belirtilen kriterlere uygun olmak kaydıyla kullanılır.



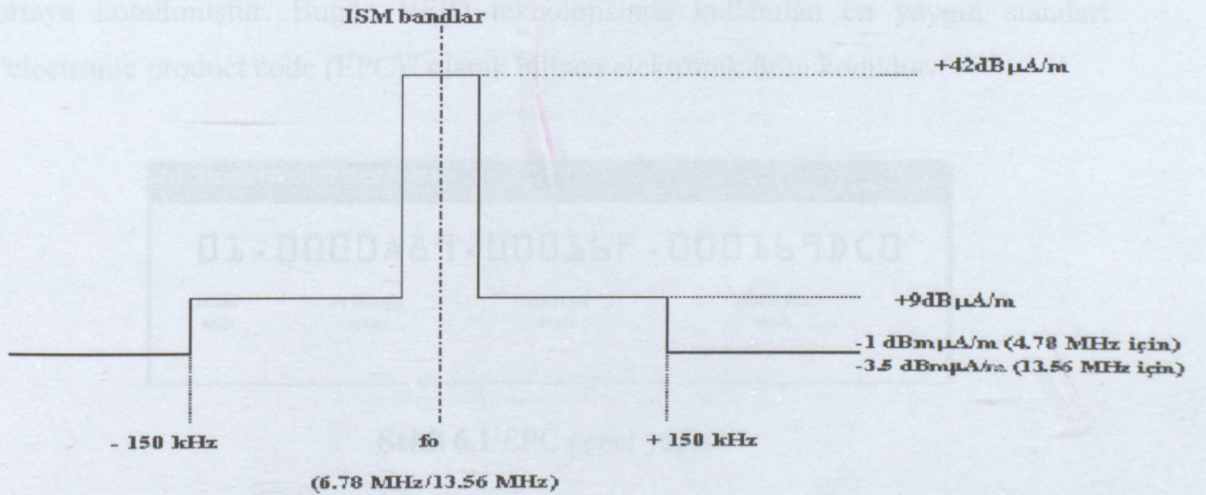
Tablo 5.3 Endüktif Sistemler Teknik Kriterleri

Frekans Bandı	Çıkış gücü (maksimum)	Anten tipi	Açıklama
9 - 59.750 kHz	10 metrede 72 dB $\mu$ A/m (30kHz de 3.5 dB/octave)	Tümleşik veya dahili	Çerçeve (Loop) anten kullanılması durumunda 0.05 m <sup>2</sup> ve 0.16 m <sup>2</sup> arasındaki alanda alan şiddeti 10xlog (alan/0.16 m <sup>2</sup> ) olacak şekilde azalır. Anten alanı 0.05 m <sup>2</sup> den küçük ise, alan şiddeti 10 dB azalır.  Çıkış karakteristiği şekil 5.23'te gösterilmiştir.
59.750 - 60.250 kHz	10 metrede 42 dB $\mu$ A/m	Tümleşik veya dahili	Çıkış karakteristiği şekil 5.23'te gösterilmiştir.
60.250 - 70 kHz	10 metrede 72 dB $\mu$ A/m (30kHz de 3.5 dB/octave)	Tümleşik veya dahili	Çerçeve (Loop) anten kullanılması durumunda 0.05 m <sup>2</sup> ve 0.16 m <sup>2</sup> arasındaki alanda alan şiddeti 10xlog (alan/0.16 m <sup>2</sup> ) olacak şekilde azalır. Anten alanı 0.05 m <sup>2</sup> den küçük ise, alan şiddeti 10 dB azalır.  Çıkış karakteristiği şekil 5.23'te gösterilmiştir.
70 - 119 kHz	10 metrede 42 dB $\mu$ A/m	Tümleşik veya dahili	Çıkış karakteristiği şekil 5.23'te gösterilmiştir.
119 - 135 kHz	10 metrede 72 dB $\mu$ A/m (30kHz de 3dB/octave)	Tümleşik veya dahili	Çıkış karakteristiği Şekil 5.23'te gösterilmiştir.
6765 - 6795 kHz	10 metrede 42 dB $\mu$ A/m	Tümleşik veya dahili	Çıkış karakteristiği şekil 5.24'te gösterilmiştir.
7400 - 8800 kHz	10 metrede 9 dB $\mu$ A/m	Tümleşik veya dahili	-
13.553 - 13.567 MHz	10 metrede 42 dB $\mu$ A/m	Tümleşik veya dahili	Çıkış karakteristiği şekil 5.24'te gösterilmiştir.
26.957-27.283 MHz	10 metrede 42 dB $\mu$ A/m	Tümleşik veya dahili	-





Şekil 5.23 9-135 kHz aralığında 10 metrede ölçülen manyetik alan sınır değerleri



Şekil 5.24 6.78 MHz ve 13.56 MHz bandlarında 10 metrede ölçülen manyetik alan sınır değerleri



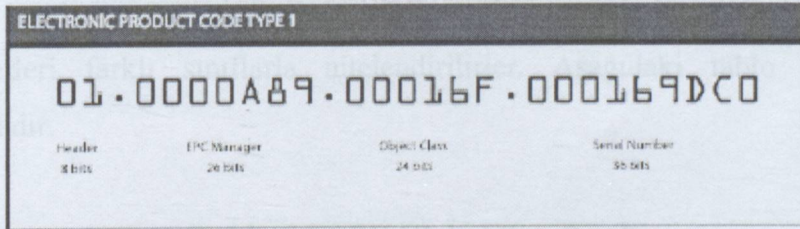
## 6 RFID SİSTEMLERİNDE ÇÖZÜLMESİ GEREKEN SORUNLAR

RFID teknolojisi, iş süreçlerinin iyileştirilmesinde büyük rol oynamaktadır. Teknolojinin ucuzlamasıyla birlikte kullanım hacmi de giderek artacaktır. Bununla birlikte bazı açık kalan noktaların da çözüme kavuşturulması şarttır.

Bunlardan ilki standardizasyon sorunudur. Bir diğeri güvenlik ve çarpışma sorunudur.

### 6.1 RFID Sisteminde Standardizasyon

RFID kullanımında küresellik göz önünde bulundurulmalı, RFID veri yapısı standartlara uygun olmalıdır. Standartların kullanımı okuyucu ve etiketlerin fiyatlarını düşüreceği gibi yeni buluşlarında artmasını sağlayacaktır. IEEE tarafından 1997 yılında 2 Mbps ve ardından 1999 yılında 11 Mbps hızlarındaki standartları ortaya konulmuştur. Bugün RFID teknolojisinde kullanılan en yaygın standart “electronic product code (EPC)” olarak bilinen elektronik ürün kodudur.



**Şekil 6.1** EPC genel yapısı

Birbiriyle uyumsuz RFID standartları bu teknolojinin daha yavaş büyümesine sebep olmaktadır. Çoğu öncü RFID üreticisi kendi sistemini farklı frekans ve protokollerle üretmektedir. Yinede hem ABD’de hem de Avrupa’da bazı kurumlar RFID kullanımı için standartlar geliştirmeye çalışmaktadır.

UHF teknolojisi ile ilgili konunun da standardizasyon açısından çözüme kavuşturulması gerekmektedir. Amerika’da bu teknolojinin kullanımı ile ilgili herhangi bir sorun yokken, Avrupa’da UHF kullanımı ile ilgili yasal bazı sınırlamalar bulunmaktadır. Kullanılan frekansın standartlaştırılabilmesi için, Avrupa



ülkelerinin bazı yasal değişiklikler yapması gerekmektedir. (RFID ISO standartları ve taslakları EK 1 ve EK 2 de verilmiştir.)

EPC Global'in tanımladığı standartlar şöyle özetlenebilir:

- EPC etiketleri için mantıksal veri formatı
- Aşağıdaki etiket frekans aralıkları için Etiket haberleşme protokolü
  - 900 MHz Sınıf 0
  - 13.56 MHz Sınıf 1
  - 860 MHz den 930 MHz'ye Sınıf 1 şeklindedir.
- "Savant" adlı standartlaşmış EPC ara katmanı için tanımlamalar

Okuyucu ile haberleşmede kullanılan:

- Fiziksel Fiyat Artış Dili - *Physical Markup Language* (PML) Tanımlaması: XML tabanlı dil olup, bir EPC ağındaki bileşenler arasında aktarılan bilginin formatını tanımlar.
- Nesne Tanımlama Servisi - *Object Name Service* (ONS) Tanımlaması : Dünyadaki herhangi bir EPC etiketine sahip ürün hakkındaki bilgiyi getiren küresel ağ tanımlamasıdır.

EPC etiketleri farklı sınıflarla nitelendirilirler. Aşağıdaki tablo bu sınıfları açıklamaktadır.

**Tablo 6.1 EPC Global 'Sınıfları'**

EPC Sınıfı	Açıklama	Programlama
Sınıf 0	"Yalnız okuma" pasif etiketler	Yarı iletken üretim işleminin bir parçası olarak programlanır.
* Sınıf 0+	EPC Sınıf 0'ın "Bir defa yazma, çoklu okuma" versiyonu	Müşteri tarafından 1 defa programlanır sonra kilitletlenir
Sınıf 1	"Bir defa yazma, çoklu okuma" pasif etiketler	Müşteri tarafından 1 defa programlanır sonra kilitletlenir



Sınıf 1 – Nesil 2	Küresel birlikte çalışabilirlik, çoklu okuma yazma ve arttırılmış veri iletim hızı sağlar.	Birçok defa programlanabilir
Sınıf 2	Tekrar yazılabilir pasif etiketler	Birçok defa programlanabilir
Sınıf 3	Yarı pasif etiketler	
Sınıf 4	Aktif etiketler	
Sınıf 5	Okuyucular	Mümkün değil
* EPC Global tanımlı bir sınıf değil		

## 6.2 RFID Sistemlerinde Güvenlik

RFID teknolojisinin yeni bir teknoloji olmamasına ve gün geçtikçe önem kazanıp üzerinde yapılan çalışmaların arttırılmasına rağmen gizlilik ve güvenlik ile ilgili sorunları tam olarak çözülememiştir. İnsan mahremiyetinin ihlal edilmesi konusunda oluşan çekincelerle Eylül 2003’de bazı insan hakları ve sivil toplum organizasyonları RFID teknolojisi kullanan marketleri dava etmiştir. Bu sistemin kötü yollar için kullanılabilceği öne sürülmüştür.

RFID teknolojisi kullanımında güvenlik ve gizlilik ihlali adına oluşabilecek sorunlardan bazılarını şöyle özetleyebiliriz:

1. Fiziksel Saldırıları: RFID etiketinin yırtılması, kazınması, devrelerinin parçalanması, radyasyona maruz kalması gibi dış etkiler.
2. Servisin engellenmesi (DoS): RF kanallarının sinyallerinin bozulması buna örnektir.
3. Taklit Etme : RFID etiketlerinin istenilen şekilde değiştirilebilmesi
4. Yanıltma : Etiketin taklit edilmesi yoluyla, okuyucunun aldatılması
5. Dinleme : Etiket ile okuyucu arasındaki mesajların izinsiz dinlenmesi



6. Veri trafiği analizi: Etiket ile okuyucu arasındaki iletişimdeki mesajların izlenerek veri analizi yapılması. Özellikle şifrelenmiş verilerin çözülmesinde önemli örnek elde etmek için kullanılır.

RFID insanların taşıdıklarının veya satın aldıklarının uzaktan ve habersiz izlenebilmelerini sağlayabildiği için özel yaşamı tehdit unsuru olarak görülebilmektedir ve kullanım karşıtları da bulunmaktadır. Ancak geliştiriciler ikinci nesil RFID' nin bu konuları da dikkate alarak gerçekleştirildiğini söylemektedirler; yeni nesil RFID etiketleri istenildiğinde okunamaz veya bir daha kullanılamaz hale getirilebilmektedirler.

### 6.2.1 RFID Teknolojisinde Güvenlik ve Gizlilik için Önerilen Çözümler

Güvenlik ve gizliliğin sağlanması için farklı çözüm yöntemleri önerilmektedir. Bu yöntemler burada derinlemesine incelenmeyecek olsa da önemli olarak görülenler üzerinde durulacaktır.

“Kill” Komutu bu çözüm Auto-ID Center ve EPC global tarafından önerilmiştir. Her bir etiketin tekil bir şifresinin olduğu, örneğin 24 bit, ve üretim aşamasında programlandığı bir yöntemdir. Doğru şifre verildiğinde etiket tamamen kullanılamaz hale gelmektedir.

“Faraday Kafesi” yaklaşımı adı verilen bir diğer yöntem etiketlerin herhangi bir elektromanyetik dalgaya maruz kalmasının engellenmesidir. Faraday Kafesi (FC) adı verilen metal bir ağ veya folyodan yapılmış olan bir kap birçok frekanstaki sinyali kırabilmektedir.

“Aktif Sinyal Bozma” Yaklaşımı, FC'ye alternatif olarak, elektromanyetik dalgaların engellenmesinin bir diğer yolu da radyo kanalının rahatsız edilerek, RF sinyal bozma yönetimin uygulanmasıdır. Bu işlem, aktif olarak radyo sinyalleri yayan bir cihaz kullanılarak yapılabilmektedir. Böylece RFID okuyucuların okuma işlemi yapmaları engellenmektedir.



Etiket Bloklama; bir okuyucu tarafından gönderilen sorguyu birden çok etiket yanıtlarsa, okuyucu çakışma olduğunu varsayacaktır. Etiket okumada kullanılan en önemli protokoller "ALOHA" (13.56 MHz) ve "tree-walking" protokolleridir (915 MHz). Bunlardan, kısa frekans kullanan "tree-walking" protokolünün çalışma mantığı kullanılarak pasif bir sinyal bozma yöntemi geliştirilmiştir. Etiket bloklama; "Blocker tag" adı verilen bu yöntem ile yeniden tasarlanan bir etiketin, olası tüm seri numaralarının benzetimini yapması ve RFID okuyucuyu yanıltması sağlanmıştır.

Ahlaki Kanun Tasarıları; Garfinkel tarafından ortaya konulan RFID ahlaki değerleri, RFID sistemler kullanılırken uyulması önerilen bazı maddeler içermektedir. Garfinkel, bu değerleri kanun haline getirme amacı olmasa da, firmaların uymasını önermektedir.

Klasik Şifreleme yöntemleri kullanılmaktadır. Yeniden yazılabilir bellek; her etiketin anonim (isimsiz) bir ID ye sahip olması, E(ID) gibi, böylece gerçek ID' nin saklanması düşüncesini savunur. "E", genel veya simetrik anahtar şifreleme algoritması içerebilir veya etiketin ID sine bağlanmış rasgele bir sayı olabilir. İzlenme sorununu çözmek için, etiket içerisindeki anonim ID yeniden şifreleme ile sıkça değiştirilmelidir.

Simetrik anahtar şifreleme: Feldhofer tarafından önerilen yetkilendirme mekanizması, basit bir iki taraflı sorun-yanıt algoritması üzerine kuruludur. Bu yaklaşımın sorunu, RFID etiketin AES özelliğinin olmasına ihtiyaç duymasıdır.

Simetrik anahtar şifreleme: Genel anahtar şifreleme kullanan yeniden şifreleme üzerine kurulu yapılar da vardır.

Hash Fonksiyonlarına Dayanan Yöntemleri; güvenlik sorunlarını aşmak için daha yaygın şekilde kullanılan çözümlerden biri de hash fonksiyonlarıdır.

Temel PRF Özel Yetkilendirme Yöntemleri: Molar tarafından önerilen yöntem, etiket ve okuyucular arasında ortak bir yetkilendirme mantığı üzerine kuruludur. Bu



protokol, etiket ve okuyucu arasındaki mesajların korunması için paylaşılan bir anahtar ve Pseudo-Random Function (PRF) kullanılır.

Ağaç Tabanlı Özel Yetkilendirme Ve Atama Ağacı: Hash yöntemlerinin önemli bir olumsuz yanı, etiketlerin tanımlanabilmesi için sunucuya fazla yüklenilmesidir. Molnar, bu yükün azaltılabilmesi için "Tree-Based Private Authentication" isimli bir yöntem önermiştir.

### 6.3 RFID Sistemlerinde Çarpışma ve Çarpışma Önleyici Algoritmalar

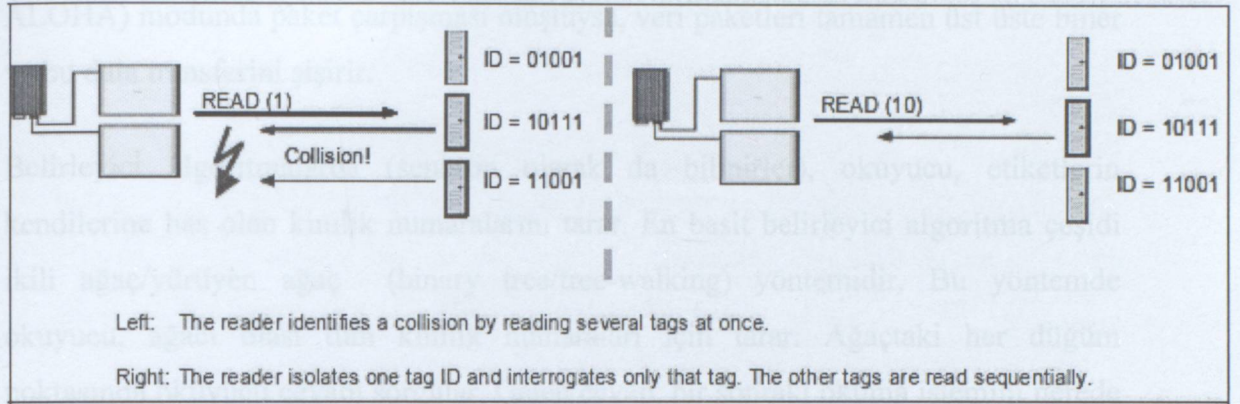
RFID uygulamalarında, sistemin bazı fiziksel özelliklerinden dolayı da sorunlar ortaya çıkabilir. Bunlardan biri farklı okuyuculardan gönderilen sinyallerin çakışması diğeri de çok fazla sayıda etiketin okuyucunun etki alanına girmesidir. Ayrıca RFID sisteminin kurulduğu ortam da önem taşımaktadır. Örneğin yüksek frekanslı dalgalar su içinde absorbe olurken, düşük frekanslı dalgalar da metal nesnelere etkilenmektedir. Bu nedenlerden dolayı sistemin tasarımı, uygulama başarısı için çok büyük önem taşımaktadır.

"Çarpışma" farklı yönlerden gelen Radyo dalgalarının birbiri ile karışması olarak tanımlanabilir. RFID' deki bir problemde okuyucu çarpışması ve etiket çarpışmalarıdır.

#### 6.3.1 Okuyucu Çarpışması

Okuyucu çarpışması, bir okuyucudan gelen sinyalin diğerinden gelen ile karışmasıdır. Bu problemi çözümlerin bir yolu zamanı birçok geçiş için bölmektir. Bu basit olarak okuyucuların farklı zamanlarda etiket ile iletişim kurmasıdır. Bu birbirleri ile çatışmalarını engeller. Ancak bu aynı zamanda iki okuyucunun çakıştığı bir yerde bir RFID etiketinin iki defa okunması anlamına da gelebilir. Bu yüzden sistem, bir etiket bir okuyucu tarafından okunduğu zaman diğer okuyucunun tekrar okumaması şeklinde kurulmalıdır.





**Şekil 6.2** RFID Okuyucu Çarpışması Protokolü

**Kaynak:** Siemens

### 6.3.2 Etiket Çarpışması

RFID etiketi çarpışması aynı anda birden fazla etiket okuyucuya sinyal gönderdiği zaman meydana gelir. Üreticiler etiketin okuyucuya tek bir anda cevap vermesi için değişik sistemler geliştiriyorlar. Bu sistemler etiketleri tekilleştiren algoritmaları içerir. Her etiket saniyenin binde birinde okunduğu için, eş zamanlı okunuyorlarmış gibi görünür.

### 6.3.3 Çarpışma Önleyici Algoritmalar

Çarpışma önleyici algoritmalar, olasılıksal ve belirleyici algoritmalar şeklinde iki sınıfta ifade edilebilir.

Olasılıksal algoritmalarda (asen kron olarak da bilinir), etiket rasgele üretilmiş zamanlarda cevap verir. Olasılıksal algoritmaların birçok çeşidi vardır. Birçoğu, ağ üzerindeki ALOHA metodu tabanlıdır. Bu yöntem, bir veri paketi aldıktan sonra bir başka veri paketi iletilen noktalar içerir. Eğer bir çarpışma olursa, bu düğüm donar ve yeni bir paketi gecikmeli gönderir. Etiket üzerinden okuyan okuyucu, çarpışma olmadığı sürece data transferini sürdürür. Okuyucunun cevap verdiği anlar, aralıklı (slotted) veya sürekli anlar olabilir. Bu mod özel veri paketlerini bağımsız transmisyonda biraz kısıtlama yapmaktadır. Eğer, aralıklı anlarda (slotted



ALOHA) modunda paket çarpışması oluştuysa, veri paketleri tamamen üst üste biner ve bu data transferini şişirir.

Belirleyici algoritmalarda (senkron olarak da bilinirler), okuyucu, etiketlerin kendilerine has olan kimlik numaralarını tarar. En basit belirleyici algoritma çeşidi ikili ağaç/yürüyen ağaç (binary tree/tree-walking) yöntemidir. Bu yöntemde okuyucu, ağacı olası tüm kimlik numaraları için tarar. Ağaçtaki her düğüm noktasında okuyucu cevabı sorgular. Gelen cevap, bir sonraki okuma işlemini nerede yapacağını işaretini verir.

Bunlardan başka iki ayrı çarpışma önleyici algoritma çeşidi vardır; FMO ve Miller Subcarrier (alt taşıyıcı). FMO, günümüzde de ISO standartlarında kullanılmaktadır. Bu algoritma hızlı fakat engellere karşı daha dayanıklıdır. Miller Subcarrier daha yavaştır ancak gürültülü ortamlarda RF de daha iyidir ve 2. jenerasyon okuyucular tarafından desteklenmektedir. Bu algoritma, etiketlerin geri sinyallerini göndermek üzere dar bir band spektrumu kullanır ve bu sinyalleri okuyucu tarafından kullanılan kanallara uyarlar. Böylelikle okuyucudan gelen RF sinyalleri, etiketten gelen sinyallerle karşılaşmaz. Miller Subcarrier (alt taşıyıcı) algoritması, etiketin cevabını, okuyucunun transmisyon sinyallerinden ve diğer gürültülerden ayırmak için, FMO'ya nazaran daha gelişmiş filtreleme teknikleri kullanır.

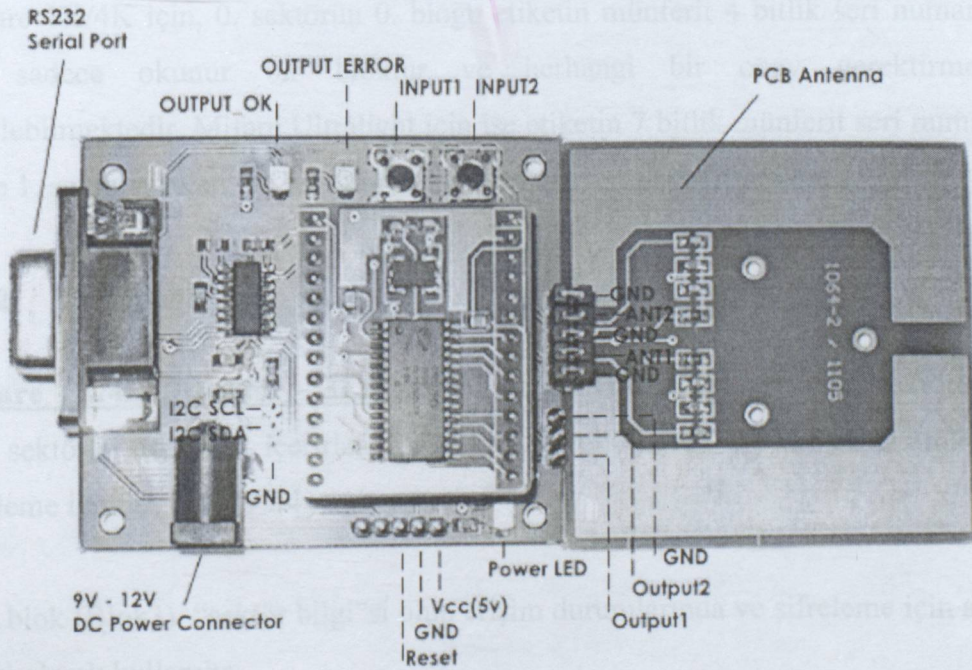


## 7 TEZ UYGULAMASINDA KULLANILAN DEMO KİT

Araştırmalar sonunda, yapılacak uygulamaya paralel olarak 13,56 MHz. de pasif etiket ile çalışan SM1013 demo kiti tercih edilmiştir. Bu demo kit ile Mifare® etiketlerini programlama ve okuma yapılabilmektedir. Bu kitte okuma-yazma mesafesi verilen anten ile 9cm'e kadar çıkabilmektedir.

Kit aşağıdaki parçalardan oluşmaktadır:

- Uygulama geliştirme tablosu
- SM130 Okuma- Yazma Modülü
- PCB Anten
- SMRFID Mifare Yazılımı
- RS232 Seri kablosu
- 9V DC Adaptör
- Mifare® 1K ve Mifare® 4K etiketler



**Şekil 7.1** SM 1013 Uygulama Geliştirme Kitinin Üstten Görünümü

Uygulama geliştirme tablosunda; 5V regülatör, RS232 ve I2C arayüzü, genel amaçlı giriş ve çıkışlar için 2 buton mevcuttur.



“MIFARE”; klasik 1K ve 1 Kb EEPROM okuma/yazma hafızasına sahip en fazla 10 cm’ e kadar okuma mesafesi olan, 13,56 MHz de işlem gören ve çarpışma önleyici özelliği olan pasif (bataryaya ihtiyaç duymayan), Philips üretilmiş beyaz kartlara verilen genel isimdir.

## 7.1 Mifare Blok Tanımlaması

Mifare 1K/4K blokları kendi içinde dört kategoriye ayrılır: Fabrika ayar bloğu, veri bloğu, değer bloğu ve sektör bilgi bloğu.

Mifare Ultralight, Mifare 1K/4K’lardan biraz farklıdır. Mifare Ultralight’ da sayfalar vardır. Bunlar fabrika ayar bloğu, kilit konfigürasyon bloğu, OTP blok ve veri bloğu olarak kategorize edilebilirler.

### 7.1.1 Fabrika Ayarı Bloğu

Mifare 1K/4K için, 0. sektörün 0. bloğu etiketin münferit 4 bitlik seri numarasıdır. Bu sadece okunur bir bloktur ve herhangi bir onay gerektirmeksizin erişilebilmektedir. Mifare Ultralight için ise etiketin 7 bitlik münferit seri numarasını 0. ve 1. sayfalar tutar. Bu sayfalar sadece okunurdur, değiştirilemez.

### 7.1.2 Veri Bloğu

**Mifare 1K/4K (0.sektör - 31.sektör)** : Bu kartlarda 0.sektörden 31.sektöre kadar tüm sektörler dört blok içerirler. İlk üç blok (Blok0-Blok1-Blok2) genel amaçlı veri yükleme içindir. (Tablo 7.1)

Son blok (Blok3) “sektör bilgi”si olup erişim durumlarında ve şifreleme için anahtar girişi olarak kullanılır.



**Tablo 7.1 Mifare 1K kartların Hafıza Dizayını**

Sektör	Blok	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Tanımı
0						0												Fabrika Ayarları Bloğu
1																		Veri Bloğu
2																		Veri Bloğu
3																		Anahtar A
																		Erişim Bitleri
																		Anahtar B
																		Sektör izleyici 0
1						0												Veri Bloğu
1																		Veri Bloğu
2																		Veri Bloğu
3																		Anahtar A
																		Erişim Bitleri
																		Anahtar B
																		Sektör izleyici 1
...						...												Veri Bloğu
...						...												Veri Bloğu
...						...												Veri Bloğu
...	...																	Anahtar A
																		Erişim Bitleri
																		Anahtar B
																		Sektör izleyici ...
14						0												Veri Bloğu
1																		Veri Bloğu
2																		Veri Bloğu
3																		Anahtar A
																		Erişim Bitleri
																		Anahtar B
																		Sektör izleyici 14
15						0												Veri Bloğu
1																		Veri Bloğu
2																		Veri Bloğu
3																		Anahtar A
																		Erişim Bitleri
																		Anahtar B
																		Sektör izleyici 15

Sıfırıncı sektörde ise bir istisna olarak genel amaçlı veri yükleme için iki blok (Blok1-Blok2) vardır. İlk blok olan 0.sektörün 0.bloğu (Blok0) fabrika ayar bloğu olarak ayrılmış olup münferit seri numara bilgisini tutmaktadır.

**Mifare 4K (32.sektör- 39.sektör):** Bu kartlarda ise 32.sektörden 39.sektöre kadar tüm sektörler 16 blok içerir. İlk 15 blok (Blok0-Blok1-Blok2-.....-Blok14) genel amaçlı veri yükleme içindir. 16.Blok olan Blok15, Mifare 1K'daki 3.blok gibi sektör izleyiciyi içeren özel bir blok olup erişim durumlarını ve belirli sektörün anahtarlama bilgilerini tutar.



Tablo 7.2 Mifare 4K kartların Hafıza Dizaynı

Sektör	Blok	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Tanım
0		0					Fabrika Ayar Bloğu											
1							Veri Bloğu											
2							Veri Bloğu											
3		Anahtar A			Erişim Bitleri			Anahtar B			Sektör İzleyici 0							
1		0					Veri Bloğu											
1							Veri Bloğu											
2							Veri Bloğu											
3		Anahtar A			Erişim Bitleri			Anahtar B			Sektör İzleyici 1							
...		...					Veri Bloğu											
...		...					Veri Bloğu											
...		...					Veri Bloğu											
3		Anahtar A			Erişim Bitleri			Anahtar B			Sektör İzleyici 30							
31		0					Veri Bloğu											
1							Veri Bloğu											
2							Veri Bloğu											
3		Anahtar A			Erişim Bitleri			Anahtar B			Sektör İzleyici 31							
32		0					Veri Bloğu											
1							Veri Bloğu											
...		...																
...		...																
15		Anahtar A			Erişim Bitleri			Anahtar B			Sektör İzleyici 32							
33		0					Veri Bloğu											
1							Veri Bloğu											
...		...																
...		...																
15		Anahtar A			Erişim Bitleri			Anahtar B			Sektör İzleyici 33							
...		...																
...		...																
...		...																
15		Anahtar A			Erişim Bitleri			Anahtar B			Sektör İzleyici 38							
39		0					Veri Bloğu											
1							Veri Bloğu											
...		...																
...		...																
15		Anahtar A			Erişim Bitleri			Anahtar B			Sektör İzleyici 39							

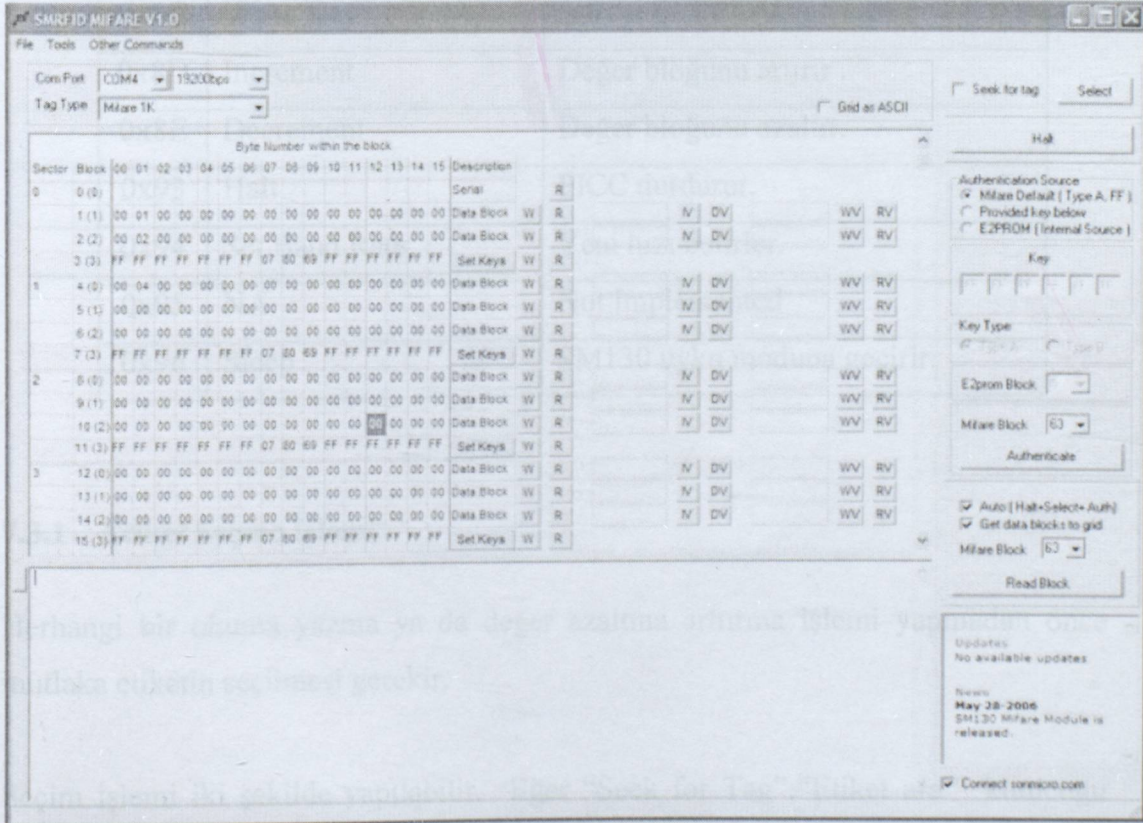


### 7.1.3 Değer Blokları

Değer blokları elektronik cüzdan uygulamalarında kullanılır. Belli formatlarda depolanırlar. Bu tez çalışmasında kullanılan SM130 modülü bu formatı otomatik yapar. Bir değer bloğuna, azaltma ve arttırma olarak iki tip işlem yapılabilir. Mifare Ultralight, değer blokları içermezler.

## 7.2 Smrfid Mifare Yazılımı

SMRFID Mifare Yazılımı, modülü kolay kontrol edebilmek için tasarlanmıştır. SMRFID Mifare yazılımı için SM1013 uygulama geliştirme kiti ve seri port bağlantısı gerekmektedir. SM1013 kiti bilgisayarın com portuna bağlandıktan ve yazılım çalıştırıldıktan sonra etiket seçme- tanıma, okuma, yazma... vb işlemleri yapmak mümkündür. Genel olarak Mifare etiketlerin okunması, programlanması ve text dosyalarından sisteme ya da sistemden text dosyası olarak veri aktarımı mümkündür.



Şekil 7.2 SMRFID Mifare Yazılımı Ekran Görüntüsü



### 7.3 Mifare Etiket Komutları ve İşlemleri

Mifare etiketleri üzerinde en çok yapılan işlem komutları aşağıdaki gibidir.

**Tablo 7.3 Mifare etiketleri üzerinde en çok kullanılan işlemler**

Kodu	Komutların Buton adı	Açıklaması
0x80	Reset	Modülü resetler.
0x81	Firmware	Modülün bağlantılarını kontrol eder.
0x82	Seek for Tag	Sürekli olarak alanda etiket arar.
0x83	Select Tag	Etiketi seçer.
0x85	Authenticate	Seçili bloğu onaylar.
0x86	Read Block	Belirtilen bloğu okur.
0x87	Read Value	Değer bloğunu okur.
0x89	Write Block	Seçilen bloğa veri yazar.
0x8A	Write Value	Değer bloğuna yazar.
0x8C	Write Key	Şifreyi EEPROM 'a yazar.
0x8D	Increment	Değer bloğunu artırır .
0x8E	Decrement	Değer bloğunu azaltır.
0x93	Halt	PICC durdurur.
0x94	Set Baud Rate	Yeni hızı belirler.
0x95	NA	Not Implemented
0x96	Sleep	SM130 uyku moduna geçirir.

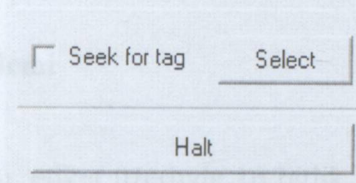
#### 7.3.1 Etiket Seçme İşlemi

Herhangi bir okuma yazma ya da değer azaltma artırma işlemi yapmadan önce mutlaka etiketin seçilmesi gerekir.

Seçim işlemi iki şekilde yapılabilir. Eğer “Seek for Tag” : “Etiket ara” kutucuğu seçili değilse, etiket bilgileri ekranda hemen görünmeyecektir. “Seek for Tag” : “Etiket ara” kutucuğunda check işareti konursa seçme işlemi hemen başlar. Ve



mevcut alanda bir etiket var ise etiket detayı ve seri numarası ekranda gözükür. Alanda bir etiket yok ise hata kodu gönderir.



**Şekil 7.3** Etiket seçme ve işlemi durdurma butonları / Select - Halt

### 7.3.2 İşlemi Durdurma

Kart üzerindeki işlemi durdurmak “Halt” butonu tıklanarak gerçekleşir. O anda kart üzerinde yapılmakta işlemi durur ve işleme, etiket baştan seçilerek devam edilir hale gelir.

### 7.3.3 Onaylama İşlemi

Mifare 1K ve Mifare 4K kartlar seçme işleminden sonra “authenticate”- onay butonu tıklanarak onay işlemine tabi tutulur. Mifare Ultralight kartlar böyle bir onay işlemi geçirmezler. SM130 modülü onay işlemi “Mifare Default” seçeneği tıklanarak ya da şifre sorarak yapılabilmektedir. Şifrelemek için “provided key below” seçeneği ya da kaynaktan şifreyi okuması için “E2PROM” seçeneği işaretlenmelidir.

Authentication Source	
<input type="radio"/>	Mifare Default ( Type A, FF )
<input checked="" type="radio"/>	Provided key below
<input type="radio"/>	E2PROM ( Internal Source )
Key	
FF	FF
FF	FF
FF	FF
Key Type	
<input checked="" type="radio"/>	Type A
<input type="radio"/>	Type B
E2prom Block	0
Mifare Block	1
Authenticate	

**Şekil 7.4** Onay İşlem Butonu



Eğer “Mifare Default” seçeneği seçilmiş ise onay alınırken onaltılı sistemden (hexadecimal) 6 bitlik FF FF FF FF FF FF şifresi, anahtar tipi “Type A”; A tipi seçilerek kullanılır.

### 7.3.4 Okuma / Yazma İşlemi

Okuma veya yazma komutu, etiket üzerinde 16 bitlik bir blok için işlem yapar. Bu işlemler için öncelikle etiketin “Select” butonu tıklanarak karın seçilmesi ve bloğun onaylanması gerekmektedir. Okuma – yazma, onaylama işlemi ile istenen şifre ve şifre tipi girilerek blok tarafından izin verilerek gerçekleştirilebilir. Eğer blok okuma yazmaya karşı korumalı ise işlem gerçekleşmeyecektir.

Mifare 1K/4K kartlarda okuma işlemi “Read Block” butonu tıklanarak, “Bloğu Oku” komutunun, yazma işlemi ise “Write Block” butonu tıklanarak “Bloğa yaz” komutunun verilmesi ile ya da okuma için “R” butonunun, yazma için “W” butonunun çift tıklanması ile gerçekleştirilebilir.

1	4 (0)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R
	5 (1)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R
	6 (2)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R
	7 (3)	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	Set Keys	W	R

Şekil 7.5 Mifare 1K /4K kartlarda okuma işlemi ("R" çift tıklanır.)

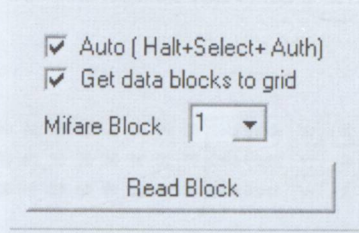
1	4 (0)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R
	5 (1)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R
	6 (2)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R
	7 (3)	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	Set Keys	W	R

Şekil 7.6 Mifare 1K/4K kartlarda yazma işlemi ("W" çift tıklanır.)

Eğer “Auto” kutucuğu işaretlenmiş ise, etiket otomatik olarak seçilir, yine otomatik olarak onaylama işlemi yapılır ve okuma/ yazma işlemi gerçekleşir.



Bu işlemi başlatmadan önce eğer aşağıdaki gibi “Get data blocks to grid”: “Verileri kutucuklara at” bölümü işaretlenmiş ise, okunan ya da yazılan değerler otomatik kutucuklara transfer olunur.



Şekil 7.7 Okuma İşlemi Butonu

### 7.3.5 Değer Okuma ve Değer Yazma İşlemi

Mifare 1K/4K kartlarda değer bloğundan, değeri okuma komutu RV butonu ile, değeri yazma komutu WV butonu ile gerçekleştirilir.

1	4 (0)	00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R			IV	DV			WV	RV
	5 (1)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R			IV	DV			WV	RV
	6 (2)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R			IV	DV			WV	RV

Şekil 7.8 Değer Oku “Read Value- RV” Butonu

1	4 (0)	00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R			IV	DV			WV	RV
	5 (1)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R			IV	DV			WV	RV
	6 (2)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R			IV	DV			WV	RV

Şekil 7.9 Değer Yaz “Write Value –WV” Butonu



### 7.3.6 Değer Arttırma ve Değer Azaltma İşlemi

Değer bloğunu, istenen bir değer ile arttırmak için IV butonu, azaltmak için DV butonu çift tıklanır. İşlem için öncelikle etiket seçili olmalı ve blok, yazma ve okumaya izin vermelidir.

1	4 (0)	00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R	IV	DV	WV	RV
	5 (1)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R	IV	DV	WV	RV
	6 (2)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R	IV	DV	WV	RV

Şekil 7.10 Değer Arttırma “Increment Value – IV” Butonu

1	4 (0)	00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R	IV	DV	WV	RV
	5 (1)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R	IV	DV	WV	RV
	6 (2)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R	IV	DV	WV	RV

Şekil 7.11 Değer Azaltma “Decrement Value – DV” Butonu

### 7.3.7 Şifreleme

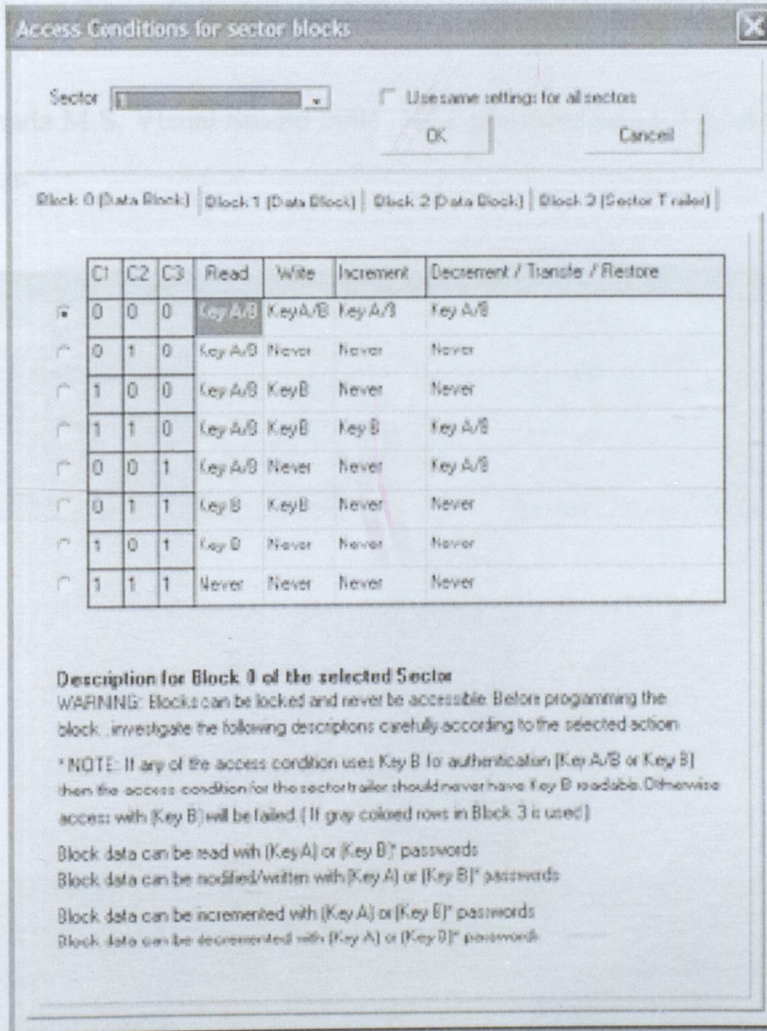
Şifrelemenin yapıldığı özel pencereye aşağıda görülen “set keys” butonu tıklanarak erişilir.

1	4 (0)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R				
	5 (1)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R				
	6 (2)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Data Block	W	R				
	7 (3)	FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF	Set Keys	W	R				

Şekil 7.12 Şifreleme Butonu



Şekil 7.13 deki şifreleme penceresi açıldığında erişim koşulları girilebilir. Belli sektörler için ya da tüm sektörler için şifre atanabilir. 4 blok içeren sektörler (Mifare 1K ve Mifare 4K, Sektör 0 – Sektör 31) için veri blokları tek tek tanımlanmaktadır. Ancak 16 blok içeren sektörler için (Mifare 4K, Sektör 32 – Sektör 39) veri bloklarının beşi birden tanımlanmaktadır : Blok0-1-2-3-4 , Blok5-6-7-8-9 , Blok10-11-12-13-14 , Blok15 (Sektör izleyici).



**Şekil 7.13** Erişim Koşulları Penceresi

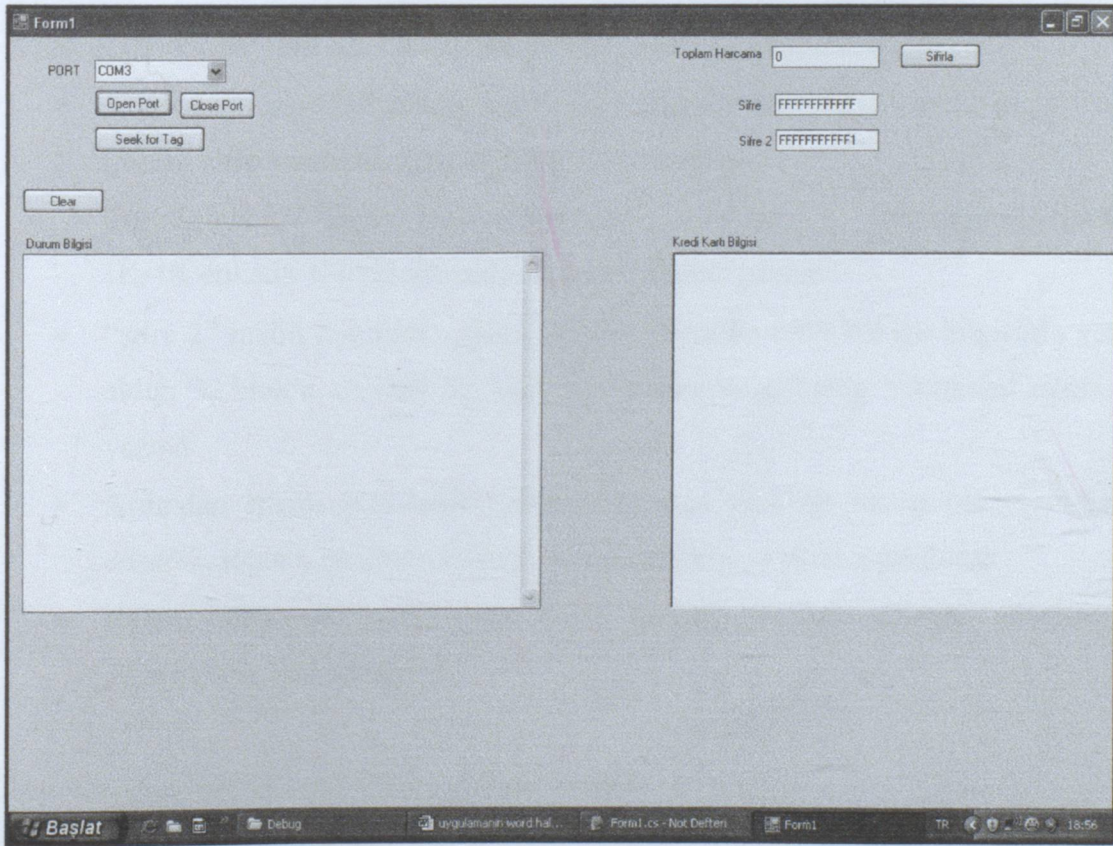


## 8 TEZ UYGULAMASI

Tez için 13,56 MHz (HF), yüksek frekansta çalışan pasif etiket kullanılarak, bu yapının en uygun olduğu kredi kartı benzeri bir uygulama seçilmiştir. Yapılan uygulamada temelde, ürün etiketi okutuldukça ürünlerin fiyatlarını toplayan ve kredi kartında belirtilen bakiyeden doğru şifre girildiği takdirde işlem yaparak hesaptan rakamı düşen ve kalan bakiyeyi karta işleyen bir yazılım geliştirilmiştir.

### 8.1 Uygulama için geliştirilen yazılım

Programlamada M.S. Visual Studio 2005. NET platformunda C# (Csharp) dili kullanılmıştır.



Şekil 8.1 Yazılımın çalıştırıldığında bilgilerin sergileneceği ekranın görüntüsü



Yazılım ilk önce kartın kredi kartı mı yoksa ürün kartı mı olduğu bilgisini ayırt etme işlemini gerçekleştirir. Kartın,

- 2.bloğuna WV komutu ile değer girilmiş ise bu bir üründür, 2.bloktaki değer de ürünün fiyatıdır.
- 32.bloğuna WV komutu ile değer girilmişse bu bir kredi kartıdır, 32. bloktaki değer de hesap bakiyesidir.

#### **Ürün kartı varsayılan kart üzerinde yapılan işlemler aşağıdaki gibidir:**

- Ürünün okuduğu fiyatını; “ürün fiyatı” olarak ekrana yazma
- Ürün kartlarının etiketleri arka arkaya okutuldukça, ürün fiyatlarını toplama
- Bu rakamı toplam harcama olarak ekrandaki “toplam harcama” metin kutusuna yazma

#### **Kredi kartı varsayılan kart üzerinde yapılan işlemler aşağıdaki gibidir:**

- Kredi kartı okutulduğunda; kredi kartı bilgileri için “şifre” metin kutusuna geçerli şifre yazılması koşuluyla kredi kartındaki:  
Kart Sahibi: / Hesap No: / Banka adı: / Şube Adı: bilgilerini (Mifare 1K/4K etiketin 1-10 bloklarını) okuyarak ekrana yazma
- “şifre 2” metin kutusuna girilen şifrenin, kredi kartının bakiye bilgisinin yer aldığı 32.blok’a ait şifre ile eşleşmesi durumunda, hesap bakiyesini ekrana yazma
- Ardından işlemi başlatarak toplam harcanan meblağı hesap bakiyesinden düşerek, toplam harcanan miktarı ve kalan bakiyeyi ekrana yazdırma
- Kalan bakiyenin aynı anda kredi kartına; Mifare 1K/4K etiketinin 32.blok’una geri işlenmesi

Tüm bu işlemleri yapan yazılım programı aşağıda verilmiştir:

SOFTWARE – Yazılım

```
using System;
using System.Collections.Generic;
```



```

using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Windows.Forms;
using System.IO.Ports;
using System.Threading;

namespace WindowsApplication1
{
    public partial class Form1 : Form
    {
        static SerialPort _serialPort;
        // _serialPort = new SerialPort();

        public Form1()
        {
            InitializeComponent();
        }

        private void button1_Click(object sender, EventArgs e)
        {
            if (_serialPort.IsOpen)
            {
                textBox1.Text += "Com port zaten açık" + Environment.NewLine;
                return;
            }

            _serialPort.PortName = "COM1";
            _serialPort.BaudRate = 19200;
            _serialPort.ReadTimeout = 1000;

```



```

if (_serialPort.WriteTimeout = 500;
{
    _serialPort.Open();
    textBox1.Text += "Com port açıldı" + Environment.NewLine;
    timer1.Enabled = true; //Zamanlayıcıyı Aç, zamanlayıcı kodunun içinde her 500ms
de bir, }

```

```

private byte select_continuos_tag()

```

```

{ else

```

```

    byte[] command = new byte[5];

```

```

    int[] response = new int[6];

```

```

    string mystring;

```

```

    int i;

```

```

//_serialPort.Close(); //Portu kapat

```

```

timer1.Enabled = false; //Zamanlayıcıyı kapat, çünkü port kapandı.

```

```

    command[0]=0xFF;

```

```

    command[1]=0x00;

```

```

    command[2]=0x01;

```

```

    command[3]=0x82;

```

```

    command[4]=0x83;

```

```

    _serialPort.Write(command, 0, 5);

```

```

private byte authenticate(byte block_no, string sifre)

```

```

//Continous Select komutunun beklenen "response" u 6 byte dir...

```

```

//RX < FF 00 02 82 4C D0

```

```

mystring = "RX <";

```

```

for (i = 0; i < 6; i++)

```

```

{

```

```

    response[i] = _serialPort.ReadByte();

```

```

    mystring = mystring + " "+response[i].ToString("X2");

```

```

//X2 means int converted to hex as two digit

```

```

}

```



```

if (response[4] == 0x4C)
{
    textBox1.Text += mystring + " (Select işlemi başarılı)" + Environment.NewLine;
    timer1.Enabled = true; //Zamanlayıcıyı Aç , zamanlayıcı kodunun içinde her 500ms
    de bir, kart okutuldu mu diye kontrol yapılacak.

    return 0;
}
else
{
    textBox1.Text += "Hata: Select Tag komutuna modulden cevap gelmedi." +
    Environment.NewLine;
    //_serialPort.Close(); //Portu kapat
    timer1.Enabled = false; //Timer açıksa kapatılması gerek, çünkü port kapandı.

    return 1;
}

private byte authenticate(byte block_no,string sifre)
{
    byte[] command = new byte[13];
    int[] response = new int[6];
    int i;
    byte checksum;
    string mystring;
    string temp_string;
    //TX > FF 00 09 85 02 AA FF FF FF FF FF FF 34
    command[0] = 0xFF;

```



```

command[1] = 0x00;
command[2] = 0x09;
command[3] = 0x85;
command[4] = block_no;
command[5] = 0xAA;
temp_string = sifre.Substring(0, 2);
command[6] =
byte.Parse(temp_string, System.Globalization.NumberStyles.HexNumber); //0xFF;

temp_string = sifre.Substring(2, 2);
command[7] = byte.Parse(temp_string,
System.Globalization.NumberStyles.HexNumber); //0xFF;

temp_string = sifre.Substring(4, 2);
command[8] = byte.Parse(temp_string,
System.Globalization.NumberStyles.HexNumber); //0xFF;

temp_string = sifre.Substring(6, 2);
command[9] = byte.Parse(temp_string,
System.Globalization.NumberStyles.HexNumber); //0xFF;

temp_string = sifre.Substring(8, 2);
command[10] = byte.Parse(temp_string,
System.Globalization.NumberStyles.HexNumber); //0xFF;

temp_string = sifre.Substring(10, 2);
command[11] = byte.Parse(temp_string,
System.Globalization.NumberStyles.HexNumber); //0xFF;

checksum = 0;
for (i = 2; i <= 11; i++)
checksum += command[i];

```



```

int[] response = new int[10];

command[12] = checksum;

serialPort.Write(command, 0, 13);

//Authentication komutunun cevabı 6 byte dir.
//RX <FF 00 02 85 4C D3
mystring = "RX <";
for (i = 0; i < 6; i++)
{
    response[i] = serialPort.ReadByte();
    mystring = mystring + " " + response[i].ToString("X2");
    //X2 means int converted to hex as two digit
}
if (response[4] == 0x4C)
{
    textBox1.Text += mystring + " (Authentication işlemi başarılı)" +
Environment.NewLine;
    return 0;
}
else
{
    textBox1.Text += "Hata:Authentication işlemi başarısız." +
Environment.NewLine;
}

return 1;
}

private byte read_value(byte block_no,ref long fiyat)
{
    byte[] command = new byte[6];

```



```

int[] response = new int[10];
byte checksum;
int i;
string mystring;
string fiyat_str;

return i;

//TX > FF 00 02 87 01 8A

command[0] = 0xFF;
command[1] = 0x00;
command[2] = 0x02;
command[3] = 0x87;
command[4] = block_no;

checksum = 0;
for (i = 2; i <= 4; i++)
    checksum += command[i];

command[5] = checksum;

_serialPort.Write(command, 0, 6);

//Value block cevabı başarısızsa 6 byte , başarılı ise 10 byte dir.
//RX <FF 00 02 87 49 D2 I INVALID VALUE BLOCK
mystring = "RX <";
for (i = 0; i < 6; i++)
{
    response[i] = _serialPort.ReadByte();
    mystring = mystring + " " + response[i].ToString("X2"); //X2 means int
    converted to hex as two digit
}

```



```

if (response[4] == 0x49)
{
    textBox1.Text += mystring + " Hata: Bu bir VALUE block değil" +
Environment.NewLine;
    return 1;
}

//Bu bir değer bloğu -value block , geri kalan byteları da seriportun
bufferından çek.
for (i = 6; i < 10; i++)
{
    response[i] = _serialPort.ReadByte();
    mystring = mystring + " " + response[i].ToString("X2"); //X2 means int
converted to hex as two digit
}

fiyat_str=response[8].ToString("X2");
fiyat_str+=response[7].ToString("X2");
fiyat_str+=response[6].ToString("X2");
fiyat_str+=response[5].ToString("X2");
fiyat = long.Parse(fiyat_str,
System.Globalization.NumberStyles.HexNumber);

//textBox1.Text += "Fiyat" + fiyat_str + Environment.NewLine;
//textBox1.Text += "Fiyat" + fiyat.ToString() + Environment.NewLine;

return 0;

}
private byte write_value(byte block_no,long net_bakiye, ref long yeni_bakiye)
{

```



```

temp_str = net_bakiye_str[6].ToString() + net_bakiye_str[7].ToString();
byte[] command = new byte[10];
System.Int[] response = new int[10];
byte checksum;
int i;
string mystring;
string net_bakiye_str;
string temp_str;
string yeni_bakiye_str;

command[0] = checksum;

net_bakiye_str = net_bakiye.ToString("X8");
//mystring = ""
//for (i = 0; i < 9; i++)
//nextBlock.Text = "TX > " + mystring + Environment.NewLine;

command[0] = 0xFF;
command[1] = 0x00;
command[2] = 0x06;
command[3] = 0x8A;
command[4] = block_no;

temp_str = net_bakiye_str[6].ToString() + net_bakiye_str[7].ToString();
command[5] = byte.Parse(temp_str,
System.Globalization.NumberStyles.HexNumber);

temp_str = net_bakiye_str[4].ToString() + net_bakiye_str[5].ToString();
command[6] = byte.Parse(temp_str,
System.Globalization.NumberStyles.HexNumber);

temp_str = net_bakiye_str[2].ToString() + net_bakiye_str[3].ToString();
command[7] = byte.Parse(temp_str,
System.Globalization.NumberStyles.HexNumber);

```



```

temp_str = net_bakiye_str[0].ToString() + net_bakiye_str[1].ToString();
command[8] = byte.Parse(temp_str,
System.Globalization.NumberStyles.HexNumber);

checksum = 0;
for (i = 2; i <= 8; i++)
    checksum += command[i];

command[9] = checksum;

mystring = "";
for (i = 0; i <= 9; i++)
    mystring += command[i].ToString("X2") + " ";
textBox1.Text += "TX > " + mystring + Environment.NewLine;

return 0;

_serialPort.Write(command, 0, 10);

//RX <FF 00 06 8A 20 00 02 00 00 B2 WRITE OK
mystring = "RX <";
for (i = 0; i < 6; i++)
{
    response[i] = _serialPort.ReadByte();
    mystring = mystring + " " + response[i].ToString("X2"); //X2 means int
    converted to hex as two digit
}
if (response[4] == 0x49)
{

```



```

        textBox1.Text += mystring + "Hata:Değer yazılamadı" +
Environment.NewLine;
        return 1;
    }

    //Bu bir value block , geri kalan byteları da seriportun bufferından çek.
    for (i = 6; i < 10; i++)
    {
        response[i] = _serialPort.ReadByte();
        mystring = mystring + " " + response[i].ToString("X2"); //X2 means int
converted to hex as two digit
    }

    yeni_bakiye_str = response[8].ToString("X2");
    yeni_bakiye_str += response[7].ToString("X2");
    yeni_bakiye_str += response[6].ToString("X2");
    yeni_bakiye_str += response[5].ToString("X2");
    yeni_bakiye = long.Parse(yeni_bakiye_str,
System.Globalization.NumberStyles.HexNumber);

    //textBox1.Text += "Fiyat" + fiyat_str + Environment.NewLine;
    //textBox1.Text += "Fiyat" + fiyat.ToString() + Environment.NewLine;

    return 0;

}

private byte read_block(byte block_no, ref string block_str)
{

```



```

byte[] command = new byte[6];
int[] response = new int[22];
byte checksum;
int i;
string mystring;

//TX > FF 00 02 86 0A 92

command[0] = 0xFF;
command[1] = 0x00;
command[2] = 0x02;
command[3] = 0x86;
command[4] = block_no;

checksum = 0;
for (i = 2; i <= 4; i++)
    checksum += command[i];

command[5] = checksum;

mystring = "";
for (i = 0; i <= 5; i++)
    mystring += command[i].ToString("X2") + " ";
textBox1.Text += "TX > " + mystring + Environment.NewLine;

_serialPort.Write(command, 0, 6);

//Read block cevabi başarısızsa 6 byte , başarılı ise 22 byte dir.
//RX <FF 00 02 86 46 CE

```



```

mystring = "RX <";
for (i = 0; i < 6; i++)
{
    response[i] = _serialPort.ReadByte();
    mystring = mystring + " " + response[i].ToString("X2"); //X2 means int
converted to hex as two digit
}
_serialPort.Close();
textBox1.Text += "Com port kapatıldı." + Environment.NewLine;
if (response[4] == 0x46)
{
    textBox1.Text += mystring + " (Hata:Blok okunamadı.Tekrar deneyin)" +
Environment.NewLine;
    return 1;
}

```

//Bu bir değer bloğu-value block , geri kalan byteları da seriportun  
bufferından çek.

```

for (i = 6; i < 22; i++)
{
    response[i] = _serialPort.ReadByte();
    mystring = mystring + " " + response[i].ToString("X2"); //X2 means int
converted to hex as two digit
}
//Console.WriteLine("Available Ports");
textBox1.Text += mystring + " (Blok okundu)" + Environment.NewLine;
comboBox1.Items.Add(s);
block_str = ((char)response[5]).ToString();
for(i=6;i<=20;i++)
block_str+=((char)response[i]).ToString();
private void btnStart_Click(object sender, EventArgs e)
return 0;
}

```



```

private void button2_Click(object sender, EventArgs e)
{
    string serial;

    if (_serialPort.IsOpen)
    {
        timer1.Enabled = false;
        _serialPort.Close();
        textBox1.Text += "Com port kapatıldı." + Environment.NewLine;
    }
    else
    {
        textBox1.Text += "Com port zaten kapalı" + Environment.NewLine;
    }
}

private void Form1_Load(object sender, EventArgs e)
{
    _serialPort = new SerialPort();

    comboBox1.Items.Clear();
    //comboBox1.Items.Add("test");

    //Buradaki kodlar her 500ms de bir çalışıyor
    //Console.WriteLine("Available Ports:");
    foreach (string s in SerialPort.GetPortNames())
    {
        comboBox1.Items.Add(s);
        comboBox1.SelectedIndex = 0;
    }
}

private void timer1_Tick(object sender, EventArgs e)
{
    byte[] command = new byte[5];
}

```



```

int[] response = new int[32];
string mystring;
string serial;
string firmware;
string block_str;
int buffercount;
int i;
byte status;
byte block_count;
int block_mod;
long fiyat;
long bakiye;
long toplam_harcama;
long net_bakiye;
long yeni_bakiye;

fiyattoplam = ((char)response[4]).ToString();
bakiyepoz = ((char)response[5]).ToString();
bakiyeminus = ((char)response[6]).ToString();
yeni_bakiyepoz = ((char)response[7]).ToString();
yeni_bakiyeminus = ((char)response[8]).ToString();
block_str = ((char)response[9]).ToString();
firmware = ((char)response[10]).ToString();
net_bakiye = ((char)response[11]).ToString();

//Buradaki kodlar her 500ms de bir çalıştırılır.
//Her 500ms de bir , seriporta bilgi gelmiş mi bakılır
//Eğer gelmişse, toplam gelen bit kadar okuma yapılır.

buffercount = _serialPort.BytesToRead;
if (buffercount!=0)
{
    mystring = "RX <";
    for (i = 0; i < buffercount; i++)
    {

```



```

response[i] = _serialPort.ReadByte();
mystring = mystring + " " + response[i].ToString("X2"); //X2 means int
converted to hex as two digit
}
serial += response[6].ToString("X2");
serial += response[5].ToString("X2");
mystring += "(Seri No: " + serial + ")";
textBox1.Text += mystring + Environment.NewLine;

//Bu gelen , modulün firmware versiyonu olabilir , modüle reset atılınca bu
bilgi gelir.
mystring="";
if ( (response[2]==0x0C) && (response[3]==0x81) )
{
// (0) (1) (2) (3) (4) (5) (6) (7) (8) (9) (10) (11) (12) (13) (14) (15)
// RX < FF 00 0C 81 55 4D 20 31 2E 31 20 42 45 54 41 1B
status=authenticate(2,txt_sifre.Text); //2 no.lu bloğu authenticate et.
firmware = ((char)response[4]).ToString();
firmware += ((char)response[5]).ToString();
firmware += ((char)response[6]).ToString();
firmware += ((char)response[7]).ToString();
firmware += ((char)response[8]).ToString();
firmware += ((char)response[9]).ToString();
firmware += ((char)response[10]).ToString();
firmware += ((char)response[11]).ToString();
firmware += ((char)response[12]).ToString();
firmware += ((char)response[13]).ToString();
firmware += ((char)response[14]).ToString();
mystring += "(Firmware: " + firmware + ")";
}
//Bu gelen seri numarası mı?
if ((response[2] == 0x06) && (response[3] == 0x82))
{
//Bu bir kredi kartı

```



```

//Seri numarası alınıyor...
serial = response[8].ToString("X2");
serial += response[7].ToString("X2");
serial += response[6].ToString("X2");
serial += response[5].ToString("X2");
mystring += "(Seri No: " + serial +)";
textBox1.Text += mystring + Environment.NewLine;

mystring="";
//Simdi Authenticate-onaylama işlemleri yapılacak; Block 2 okunacak.
Block 2 de bir değer (value) varsa , bu bir üründür, yoksa kredi kartı demek.
//Önce timer'ı disable ederiz işlemler yarım kalmasın
//timer1.Enabled = false;
status=authenticate(2,txt_sifre.Text); //2 no.lu bloğu authenticate et.
if (status==0)
{
//Auth işlemi başarılı. Şimdi block 2 Value block mu kontrol et ,
öyleyse bu bir ürün kartı demek.
status=read_value(2,ref fiyat);
if (status == 0) // Bu bir Ürün kartı
{
mystring = "Ürünün fiyatı:";
mystring += fiyat.ToString();
toplam_harcama = long.Parse(txt_toplam_harcama.Text,
System.Globalization.NumberStyles.Integer);
toplam_harcama += fiyat;
txt_toplam_harcama.Text = toplam_harcama.ToString();
}
else
{
//Bu bir kredi kartı

```







```

//Bakiye Bilgisini oku
status = authenticate(32,txt_sifre2.Text); //32 no.lu bloğu
authenticate et.
if (status != 0)
{
    richTextBox1.Text += Environment.NewLine + "Bakiye
bilgisine ulaşılamadı.Yanlış şifre girilmiş olabilir";
    return;
}
status = read_value(32, ref bakiye);
if (status != 0)
{
    mystring = "Geçersiz Kart. Urun ya da Kredi kartı değil";
    textBox1.Text += mystring + Environment.NewLine;
    return;
    //richTextBox1.Text += Environment.NewLine + "Bakiye
bilgisine ulaşılamadı.";
    //return;
}
richTextBox1.Text += Environment.NewLine;
richTextBox1.Text += "Bir önceki bakiye:" + bakiye.ToString();
toplam_harcama = long.Parse(txt_toplam_harcama.Text,
System.Globalization.NumberStyles.Integer);
net_bakiye = bakiye - toplam_harcama;
if (net_bakiye < 0)
{
    richTextBox1.Text += Environment.NewLine;
    richTextBox1.Text += "Kalan Bakiye:" + net_bakiye.ToString();
    richTextBox1.Text += Environment.NewLine;
}

```



```

        richTextBox1.Text += "Bakiye yetersiz!";
        return;
    }

    //Kalan Bakiye karta yazılıyor...
    status = write_value(32,net_bakiye,ref yeni_bakiye);
    if (status != 0)
    {
        richTextBox1.Text += Environment.NewLine;
        richTextBox1.Text += "Hata:Yeni Bakiye yazılamadı!" +
        toplam_harcama.ToString();
        return;
    }

    if (yeni_bakiye != net_bakiye)
    {
        richTextBox1.Text += Environment.NewLine;
        richTextBox1.Text += "Hata:Yeni Bakiye yanlış yazıldı!!!" +
        toplam_harcama.ToString();
        return;
    }

    richTextBox1.Text += Environment.NewLine;
    richTextBox1.Text += "Harcanan Miktar:" +
    toplam_harcama.ToString();

    richTextBox1.Text += Environment.NewLine;
    richTextBox1.Text += "Kalan Bakiye:" + net_bakiye.ToString();

```



```

txt_toplam_harcama.Text = "0";
//KALAN BAKIYEEYI , KARTA YAZ.
//BAKIYE SIFIR İSE İŞLEM YAPILAMAZ.
}
}
}

```

### 6.2.1 Onaltılık sayıyı Onaltılık Sistemde Çevirme

```

textBox1.Text += mystring + Environment.NewLine;
}
}
private void button3_Click(object sender, EventArgs e)
{
if (_serialPort.IsOpen)
select_continuos_tag(); //"Sürekli kart okuma" modu açılıyor
else
textBox1.Text += "Com port açık değil" + Environment.NewLine;
}

```

```
private void button1_Click_1(object sender, EventArgs e)
```

12/16	70	70	0,5	8	(0,5 X 16 = 8)
70/16	4,375	4	0,375	6	(0,375 X 16 = 6)
4/16	0,25	0	0,25	4	(0,25 X 16 = 4)

```
private void btn_sıfırla_Click(object sender, EventArgs e)
```

```

{
txt_toplam_harcama.Text = "0";
}
}
}

```



## 8.2 Kartlara Bilgilerin Girilmesi

SMRFID programında değerler onaltılık sistemde (hexadecimal) olarak girilmektedir. Bu yüzden ürün fiyatlarının ve kredi kartı bakiyesinin onaltılık sistemdeki karşılıkları aşağıdaki gibi hesaplanarak girişleri yapılmıştır.

### 8.2.1 Ondalık sayıyı Onaltılık Sisteme Çevirme:

- Sayı 16'ya bölünür.
- Kalan kısım 16 ile çarparak bir kenara yazılır.
- Bölüm tekrar 16 ya bölünür, kalan kısım tekrar 16 ile çarpılıp bir kenara yazılır.
- Bölüm sıfır olana kadar işlem sürdürülür.
- Ondalık sayının onaltılık sistemdeki karşılığı; bir kenara yazılan kalanların (yani 16 ile çarpılmış (hexa) karşılıklarının) tersten sıralanması ile elde edilen rakamdır.

Örneğin: 1128 in onaltılık sistemdeki karşılığı aşağıdaki tabloda hesaplanmıştır.

**Tablo 8.1 "1128" in onaltılık sistemdeki karşılığının hesaplanması**

İşlem	Sonuç	Bölüm	Kalan	Kalan (onaltılık sistemde)
1128/16	= 70,5	70	0,5	<b>8</b> (0,5 X 16 =8)
70/16	= 4,375	4	0,375	<b>6</b> (0,375 X 16 =6)
4/16	= 0,25	0	0,25	<b>4</b> (0,25 X 16 =4)
1128 in onaltılık sistemdeki karşılığı				<b>468</b>

Ayrıca otomatik hesaplama için aşağıdaki adres kullanılabilir :

<http://www.permadi.com/tutorial/numConvJs/index.html>



## 8.2.2 Uygulama için Seçilen Rakamların Onaltılık Sistemdeki Karşılıkları

Tezin uygulamasında kredi kartı ile alımı yapılacak ve fiyat toplamı hesaplatılacak üç adet ürün olması öngörülmüş olup, bunların fiyatları ve uygulamada kullanılacak iki kredi kartının bakiyeleri aşağıdaki gibi seçilmiştir. Tabloda bu rakamların onaltılık sistemdeki karşılıkları belirtilmektedir.

**Tablo 8.2 Uygulamada kullanılan ondalık değerlerin onaltılık sistemdeki karşılıkları**

	<u>Ondalık Değeri</u>	<u>Birimi</u>	<u>Onaltılık Değeri</u>
<b>Ürün etiket fiyatları</b>			
Şapka	69	YTL	45
Saat	280	YTL	118
Kitap	147	YTL	93
<b>Bakiyeler</b>			
Kredi kartı 1	2800	YTL	AF0
Kredi kartı 2	6000	YTL	1AC2

## 8.3 Ürün etiketlerine Veri yükleme

Ürün fiyatları Mifare 1K/4K etiketlerin 2.bloklarına fiyatların üzerinde toplama işlemi yapılabilmesi için “write value”-“değer yaz” komutu ile istenen değer in onaltılık sistemdeki karşılıkları olarak girilmiştir.

### 8.3.1 Birinci ürün kartına bilgi girilmesi

Kitap-147 YTL için onaltılık sistemdeki karşılığı 93 rakamı “değer yaz”-“write value” komutu ile aşağıdaki gibi işlenmiştir.

TX > FF 00 01 83 84

(Select Command)



RX <FF 00 06 83 03 A6 DD 5A C9 32    □İZÉ TAG TYPE: 03 SERIAL:  
C95ADDA6

TX > FF 00 03 85 02 FF 89    (Authentication Command)

RX <FF 00 02 85 4C D3    L    AUTHENTICATION OK

TX > FF 00 02 87 02 8B    (Read Value Block: 2 )

RX <FF 00 06 87 02 93 00 00 00 22    □“    VALUE READ OK

### 8.3.2 İkinci ürün kartına bilgi girilmesi

Saat - 280 YTL için onaltılık sistemdeki karşılığı olan 118 rakamı “değer yaz”-“write value” komutu ile aşağıdaki gibi işlenmiştir.

TX > FF 00 01 83 84    (Select Command)

RX <FF 00 06 83 02 24 0C 8E 55 9E    □\$ □U    TAG TYPE: 02 SERIAL:  
558E0C24

TX > FF 00 03 85 02 FF 89    (Authentication Command)

RX <FF 00 02 85 4C D3    L    AUTHENTICATION OK

TX > FF 00 06 8A 02 18 01 00 00 AB    □□□ (Write Value Block: 2 )

RX <FF 00 06 8A 02 18 01 00 00 AB    □□□ WRITE OK

### 8.3.3 Üçüncü ürün kartına bilgi girilmesi

Şapka - 69 YTL için, onaltılık sistemdeki karşılığı 45 rakamı “değer yaz”-“write value” komutu ile aşağıdaki gibi işlenmiştir.

TX > FF 00 01 83 84    (Select Command)

RX <FF 00 06 83 02 E2 97 95 37 D0    □â—•7    TAG TYPE: 02 SERIAL:  
379597E2

TX > FF 00 03 85 02 FF 89    (Authentication Command)

RX <FF 00 02 85 4C D3    L    AUTHENTICATION OK

TX > FF 00 06 8A 02 45 00 00 00 D7    □E    (Write Value Block: 2 )

RX <FF 00 06 8A 02 45 00 00 00 D7    □E    WRITE OK



## 8.4 Kredi Kartlarına Veri Yükleme

“Kart Sahibi : ” / “Hesap No: ” / “Banka adı: ” / “Şube Adı: ” bilgileri, "Write all blocks"- tüm bloklara birden yazma komutu ile 1.blok ve 10.blok arasına şifresiz olarak yazdırılırken; hesap bakiyesi bilgisi "Write Value"; "Değer yaz" komutu ile 32. blok'a şifreli olarak işlenerek, iki adet kredi kartı varsaydığımız kartlar yüklenmiştir.

### 8.4.1 Birinci kredi kartına bilgi girilmesi

Notepad dosyasına yazılan aşağıda verilen bilgiler import komutuyla 1. blok'tan 10. Blok'a kadar olan aralığa girilmiştir.

```
>>>>>>Imported text from C:\Documents and Settings\ KART BİLGİLERİ GİRİS
FORMU2.txt>>>>>
```

Kart Sahibi : Aktul KAVAS

Hesap No : 854976521

Banka adı : Yapi Kredi

Şubesi : Zeynep Kamil

```
TX > FF 00 01 83 84 (Select Command)
RX <FF 00 06 83 02 62 43 95 37 FC □bC•7 TAG TYPE: 02 SERIAL:
37954362
TX > FF 00 01 93 94 (Halt Command)
TX > FF 00 02 93 4C E1 L PICC HALTED
TX > FF 00 01 83 84 (Select Command)
RX <FF 00 06 83 02 62 43 95 37 FC □bC•7 TAG TYPE: 02 SERIAL:
37954362
TX > FF 00 03 85 00 FF 87 (Authentication Command)
RX <FF 00 02 85 4C D3 L AUTHENTICATION OK
TX > FF 00 12 89 01 4B 61 72 74 20 53 61 68 69 62 69 3A 20 41 6B 74 18 □Kart
Sahibi: Akt (Write Command) Block:1
```



RX <FF 00 12 89 01 4B 61 72 74 20 53 61 68 69 62 69 3A 20 41 6B 74 18 □Kart  
 Sahibi: Akt WRITE OK (Write Command) Block:9

TX > FF 00 12 89 02 75 6C 20 4B 41 56 41 53 0D 0A 48 65 73 61 70 20 3C □ul  
 KAVAS Hesap (Write Command) Block:2

RX <FF 00 12 89 02 75 6C 20 4B 41 56 41 53 0D 0A 48 65 73 61 70 20 3C □ul  
 KAVAS Hesap WRITE OK (Write Command) Block:10

TX > FF 00 12 89 03 FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF 81  
 □yyyyyy□Eyyyyyy (Write Command) Block:3

RX <FF 00 02 89 55 E0 FF FF FF U READ AFTER WRITE IS FAILED

TX > FF 00 03 85 04 FF 8B (Authentication Command)

RX <FF 00 02 85 4C D3 L AUTHENTICATION OK

TX > FF 00 12 89 04 4E 6F 20 20 20 3A 20 38 35 34 39 37 36 35 32 31 F5 □No :  
 854976521 (Write Command) Block:4

RX <FF 00 12 89 04 4E 6F 20 20 20 3A 20 38 35 34 39 37 36 35 32 31 F5 □No :  
 854976521 WRITE OK

TX > FF 00 12 89 05 0D 0A 42 61 6E 6B 61 20 61 64 69 20 20 3A 20 59 D5 □  
 Banka adi : Y (Write Command) Block:5

RX <FF 00 12 89 05 0D 0A 42 61 6E 6B 61 20 61 64 69 20 20 3A 20 59 D5 □  
 Banka adi : Y WRITE OK

TX > FF 00 12 89 06 61 70 69 20 4B 72 65 64 69 20 0D 0A 53 75 62 65 B0 □api  
 Kredi Sube (Write Command) Block:6

RX <FF 00 12 89 06 61 70 69 20 4B 72 65 64 69 20 0D 0A 53 75 62 65 B0 □api  
 Kredi Sube WRITE OK

TX > FF 00 12 89 07 FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF 85  
 yyyyyyy Eyyyyyy (Write Command) Block:7

RX <FF 00 02 89 55 E0 U READ AFTER WRITE IS FAILED

TX > FF 00 03 85 08 FF 8F (Authentication Command)

RX <FF 00 02 85 4C D3 L AUTHENTICATION OK

TX > FF 00 12 89 08 73 69 09 20 20 20 3A 20 5A 65 79 6E 65 70 20 4B 28 si :  
 Zeynep K (Write Command) Block:8

RX <FF 00 12 89 08 73 69 09 20 20 20 3A 20 5A 65 79 6E 65 70 20 4B 28 si :  
 Zeynep K WRITE OK







TX > FF 00 01 82 83 (Auto Select Command)  
RX <FF 00 02 82 4C D0 L SEEKING FOR TAG  
RX <FF 00 06 82 02 22 3D 95 37 B5 □"=•7 FIRMWARE VERSION  
TX > FF 00 01 82 83 (Auto Select Command)  
RX <FF 00 02 82 4C D0 L SEEKING FOR TAG  
RX <FF 00 06 82 02 22 3D 95 37 B5 □"=•7 TAG TYPE: 02 SERIAL:  
37953D22  
TX > FF 00 01 93 94 (Halt Command)  
TX > FF 00 02 93 4C E1 L PICC HALTED  
TX > FF 00 01 83 84 (Select Command)  
RX <FF 00 06 83 02 22 3D 95 37 B6 □"=•7 TAG TYPE: 02 SERIAL:  
37953D22  
TX > FF 00 03 85 00 FF 87 (Authentication Command)  
RX <FF 00 02 85 4C D3 L AUTHENTICATION OK  
TX > FF 00 12 89 01 4B 61 72 74 20 53 61 68 69 62 69 20 3A 20 42 75 CF □Kart  
Sahibi : Bu (Write Command) Block:1  
RX <FF 00 12 89 01 4B 61 72 74 20 53 61 68 69 62 69 20 3A 20 42 75 CF □Kart  
Sahibi : Bu WRITE OK  
TX > FF 00 12 89 02 72 63 75 20 54 55 47 41 43 0D 0A 4D 75 73 74 65 A0 □rcu  
TUGAC Hesap (Write Command) Block:2  
RX <FF 00 12 89 02 72 63 75 20 54 55 47 41 43 0D 0A 4D 75 73 74 65 A0 □rcu  
TUGAC Hesap WRITE OK  
TX > FF 00 12 89 03 FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF 81  
□ÿÿÿÿÿÿ□ÿÿÿÿÿÿ (Write Command) Block:3  
RX <FF 00 02 89 55 E0 U READ AFTER WRITE IS FAILED  
TX > FF 00 03 85 04 FF 8B (Authentication Command)  
RX <FF 00 02 85 4C D3 L AUTHENTICATION OK  
TX > FF 00 12 89 04 72 69 20 4E 6F 20 20 3A 20 32 35 34 36 39 38 33 66 □  
No : 2546983 (Write Command) Block:4  
RX <FF 00 12 89 04 72 69 20 4E 6F 20 20 3A 20 32 35 34 36 39 38 33 66 □  
No : 2546983 WRITE OK  
TX > FF 00 12 89 05 31 37 0D 0A 42 61 6E 6B 61 20 61 64 69 20 20 20 AA□17



Banka adi (Write Command) Block:5  
RX <FF 00 12 89 05 31 37 0D 0A 42 61 6E 6B 61 20 61 64 69 20 20 20 AA □17

Banka adi WRITE OK  
TX > FF 00 12 89 06 3A 20 47 61 72 61 6E 74 69 20 0D 0A 53 75 62 65 87 □:

Garanti Sube (Write Command) Block:6  
RX <FF 00 12 89 06 3A 20 47 61 72 61 6E 74 69 20 0D 0A 53 75 62 65 87 □:

Garanti Sube WRITE OK  
TX > FF 00 12 89 07 FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF 85  
□ÿÿÿÿÿÿ□ÿÿÿÿÿÿ (Write Command) Block:7

RX <FF 00 02 89 55 E0 U READ AFTER WRITE IS FAILED

TX > FF 00 03 85 08 FF 8F (Authentication Command)

RX <FF 00 02 85 4C D3 L AUTHENTICATION OK

TX > FF 00 12 89 08 73 69 09 20 20 20 20 3A 20 41 79 61 7A 61 67 61 20 si :  
Ayazaga (Write Command) Block:8

RX <FF 00 12 89 08 73 69 09 20 20 20 20 3A 20 41 79 61 7A 61 67 61 20 si :  
Ayazaga WRITE OK

TX > FF 00 03 85 0C FF 93 (Authentication Command)

RX <FF 00 02 85 4C D3 L AUTHENTICATION OK

32. blok için ait olduğu sektörün 3. bloğu olan 35.blok'a 112011FFFFFF şifresi girilerek kart işlemi şifrelenmiştir. Bu durumda "Provided key" seçeneği seçilerek ancak verilen şifre girilmesi durumunda değer atanabilmektedir.

TX > FF 00 01 83 84 (Select Command)

RX <FF 00 06 83 02 22 3D 95 37 B6 □"=•7 TAG TYPE: 02  
SERIAL:37953D22

TX > FF 00 03 85 20 FF A7 (Authentication Command)

RX <FF 00 02 85 4C D3 L AUTHENTICATION OK

TX > FF 00 06 8A 20 F0 0A 00 00 AA ğ (Write Value Block: 32 )

RX <FF 00 06 8A 20 F0 0A 00 00 AA ğ WRITE OK



## 9 YAZILIMIN ÇALIŞTIRILMASI VE YAPILAN RFID UYGULAMASI

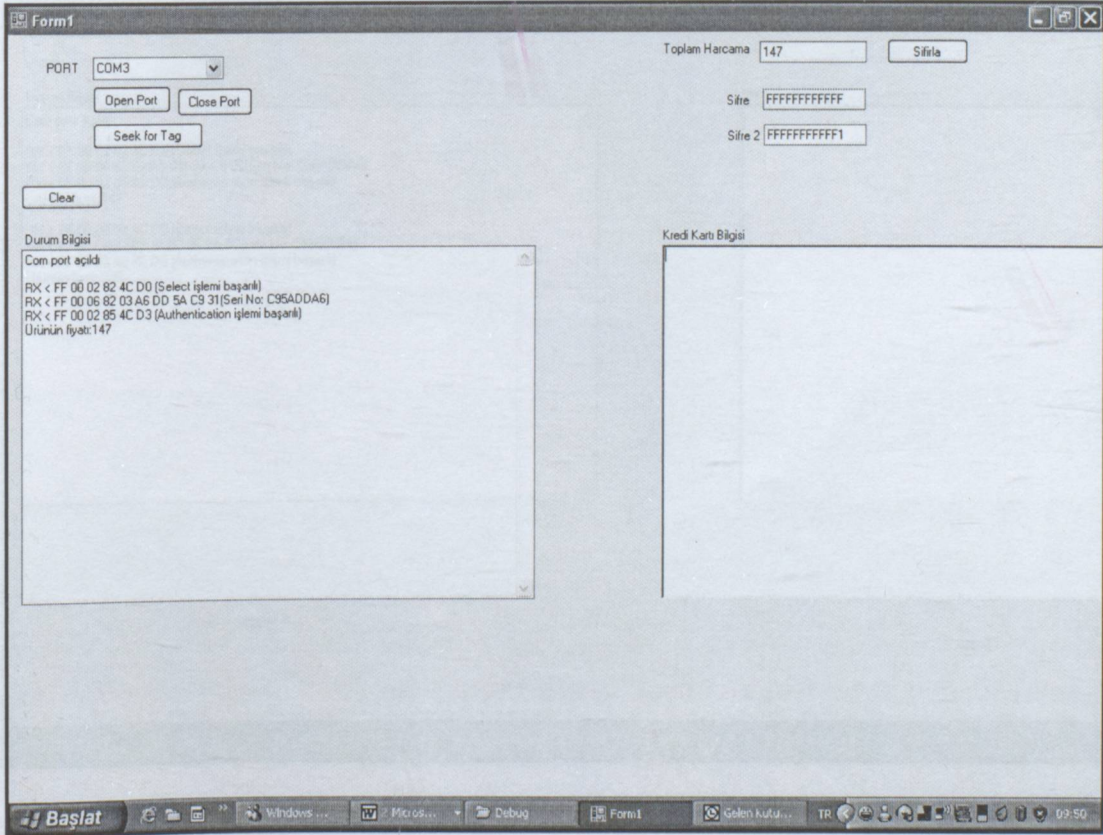
Radyo frekansı ile kimlik tanıma tez uygulaması için geliştirilen yazılım ile örnek olarak iki adet kredi kartı varsayılan kart ile satın alım uygulaması yapılarak, hem kimlik tanımaya, hem ürün tanımaya, hem de kart üzerinde işlem yapabilmeye ilişkin başarılı bir uygulama gerçekleştirilmiştir.

### 9.1 Örnek Uygulama 1

Burcu Tuğaç şahsına düzenlenmiş kredi kartı ile 147 YTL' lik bir kitap ve 280 YTL fiyatlı bir saat alımı yapılması ve hesap bakiyesinden düşülmesi gerçekleştirilecektir.

#### 9.1.1 Birinci Ürünün Okuyucuya Okutulması

Yazılım çalıştırılarak 147 YTL etiket fiyatlı kitap okuyucuya okutulduğunda, ekranın "Toplam harcama" kutucuğuna 147 yazılır. Durum bilgisi tablosundaki veriler de şekil 9.1 deki gibi dolar.



Şekil 9.1 Ürün okutulduğunda yazılım ekranının görüntüsü



Durum bilgisi kutusunda yer alan aşağıdaki komutlarla okuma işleminin gerçekleştiği görülebilmektedir.

RX < FF 00 02 82 4C D0 (Select işlemi başarılı)

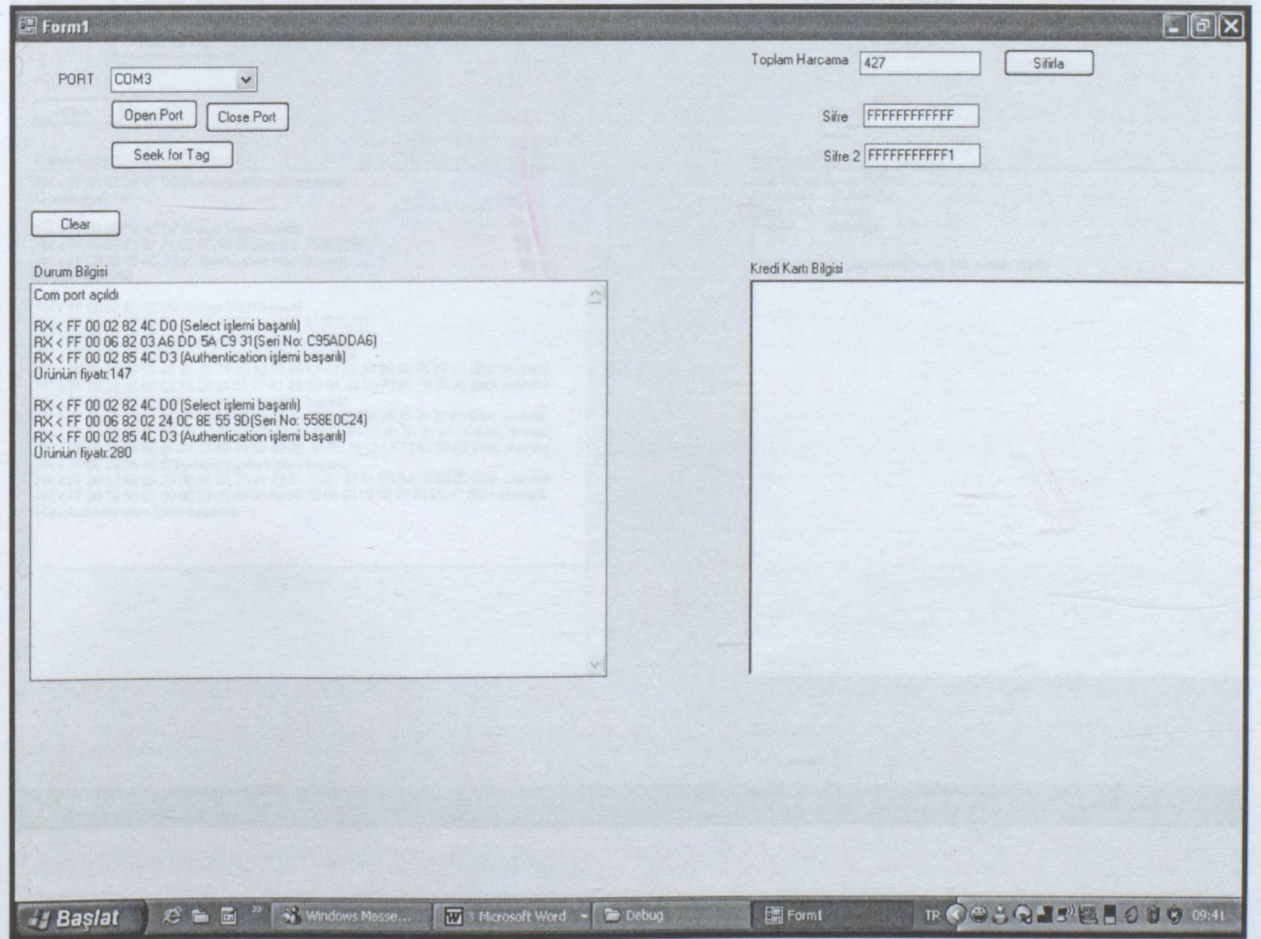
RX < FF 00 06 82 03 A6 DD 5A C9 31(Seri No: C95ADDA6)

RX < FF 00 02 85 4C D3 (Authentication işlemi başarılı)

Ürünün fiyatı:147

### 9.1.2 İkinci Ürünün Okuyucuya Okutulması

280 YTL etiket fiyatlı saat okuyucuya okutulduğunda; bir önce okutulan 147 YTL etiketli kitabın fiyatı ile ikisini toplar ve toplam harcama kutusunda  $280+147 = 427$  rakamı belirir.



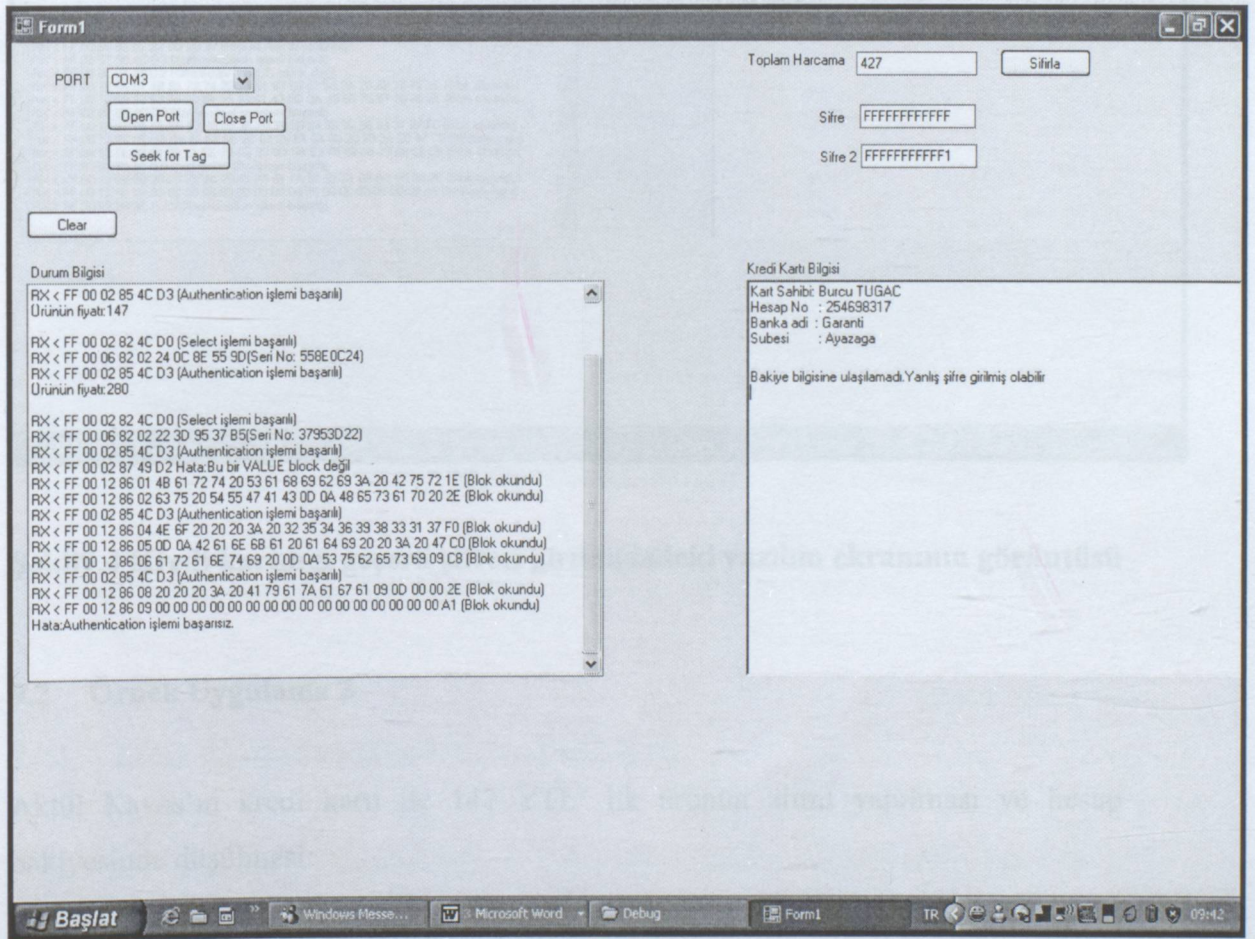
Şekil 9.2 Ürün okutulduğunda yazılım ekranının görüntüsü



### 9.1.3 Kredi Kartından Harcamanın Düşülmesi

Burcu Tuğaç' ın kredi kartı bilgileri, kart okuyucuya okutulduğunda bilgi giriş blokları ayrıca şifrelenmediği için durum bilgisinde bakiye bloğuna kadar ki okuma işlemleri gerçekleşebilmiş ve ekrana yazdırılmıştır. Ancak bakiye bloğu şifreli olduğu ve şifre2 metin kutusuna geçerli şifre girilmediğinden, hem bakiyenin okunma işlemi, hem de hesaptan harcama düşme işlemi engellenmiştir.

Kredi kartı bilgileri ekranında, bilgiler görünürken, bakiye kısmı için “Bakiye bilgisine ulaşılamadı.Yanlış şifre girilmiş olabilir.” mesajı çıkmaktadır.



Şekil 9.3 Kredi kartı yanlış şifre girişinde yazılım ekranının görüntüsü



Şifre2 bloğuna bakiye bloğu için geçerli şifre olan 112011FFFFFF girildiğinde ve kredi kartı tekrar okutulduğundaki durum Şekil 9.4 de gösterilmiştir. Yazılım kalan bakiyeyi hesaplar, toplam harcama ile birlikte ekrana yazar ve kalan bakiyeyi de kredi kartına işler.

**Şekil9.4 Kredi kartının geçerli şifresi girildiğindeki yazılım ekranının görüntüsü**

## 9.2 Örnek Uygulama 2

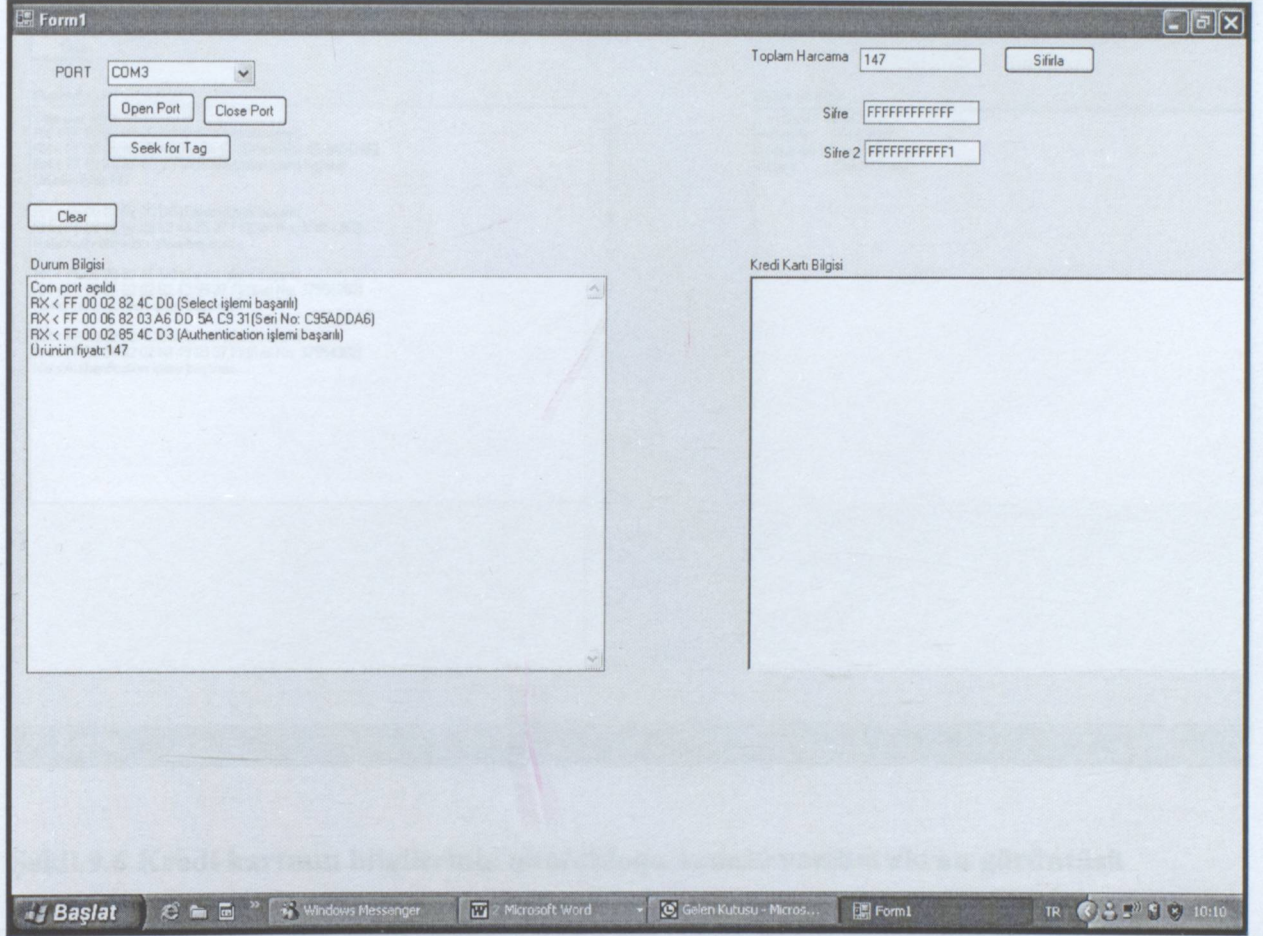
Aktül Kavas'ın kredi kartı ile 147 YTL' lık ürünün alımı yapılması ve hesap bakiyesinde düşülmesi:

### 9.2.1 Ürünün okuyucuya okutulması:

Yazılım çalıştırıldığında 147 YTL etiket fiyatlı kitap okuyucuya okutulur ve ekranın "Toplam harcama" kutucuğunda 147 yazar.



Durum bilgisi kutusunda da aŖağıdaki Ŗekilde komutlarla okuma iŖleminin nasıl gerçekteŖtiği grlmektedir.

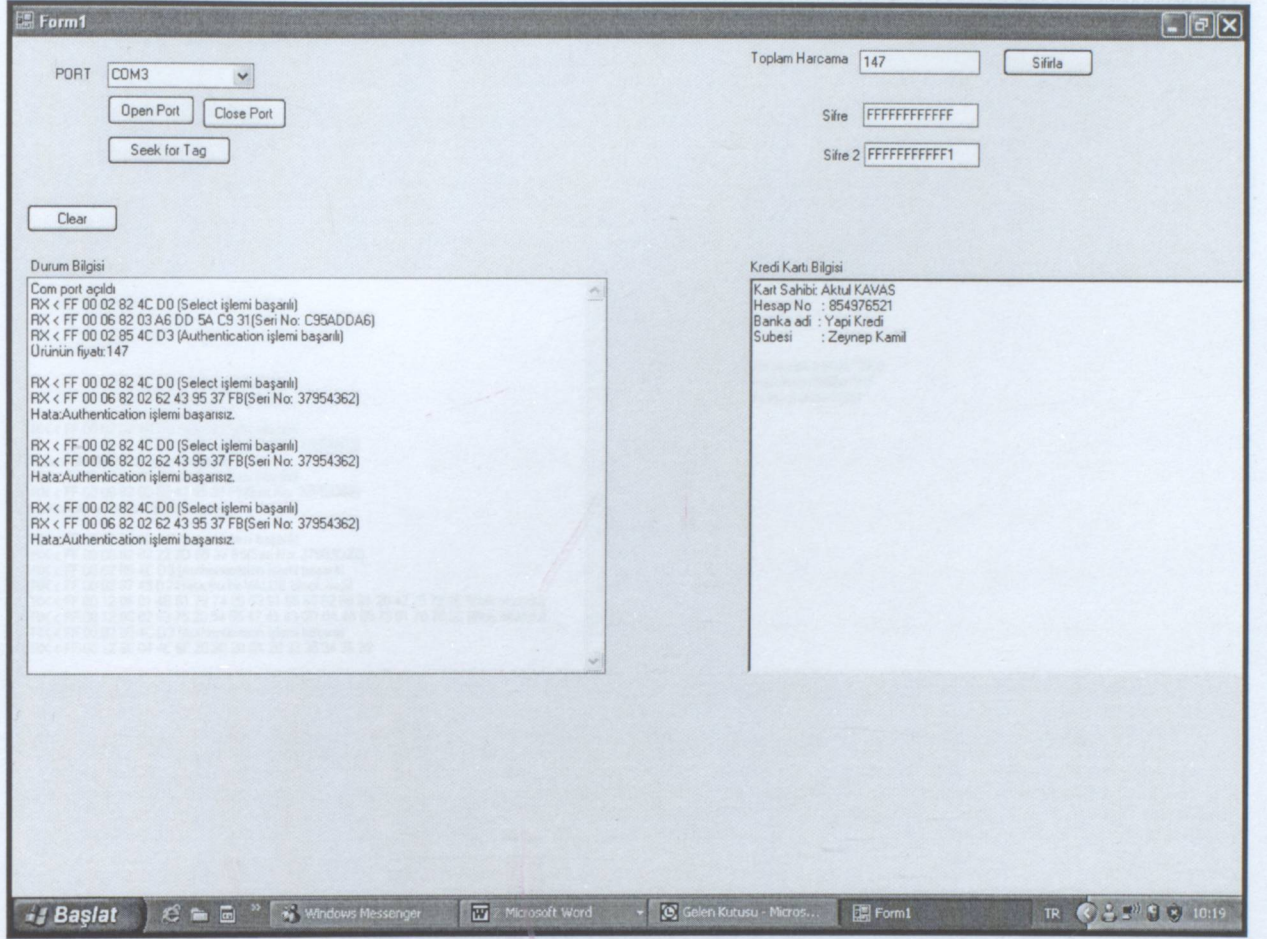


**Ŗekil 9.5 rn etiketinin okunması anındaki yazılım ekranının grnts**

### 9.2.2 Kredi Kartından Harcamanın DŖlmesi

Aktl Kavas'ın kredi kartı bilgileri, kart okuyucuya okutulduėunda bilgi giriŖ blokları ayrıca Ŗifrelenmediėi iin durum bilgisinde bakiye bloėuna kadar ki okuma iŖlemleri gerçekteŖebilmiŖ ve ekrana yazdırılmıŖtır (Ŗekil 9.6).





**Şekil 9.6 Kredi kartının bilgilerinin okutulduğu andaki yazılım ekran görüntüsü**

Ancak bakiye bloğu şifreli olduğu ve şifre2 metin kutusuna geçerli şifre girilmediğinden, hem bakiye okunamamıştır, hem de hesaptan harcama düşme işlemi engellenmiştir. Bu sebeple kredi kartı bilgileri ekranında, bilgiler görünürken, bakiye kısmı için “Bakiye bilgisine ulaşılamadı.Yanlış şifre girilmiş olabilir.” mesajı çıkarır.

Şifre2 bloğuna bakiye bloğu için geçerli şifre olan FFFFFFFFFFFFF girildiğinde ve kredi kartı tekrar okutulduğundaki durum şekil 9.7 deki gibidir. Bu durumda kalan bakiyeyi hesaplar, toplam harcama ile birlikte ekrana yazar ve kalan bakiyeyi de kredi kartına işler.



Form1

PORT: COM3

Open Port Close Port

Seek for Tag

Clear

Toplam Harcama: 147

Sifre: FFFFFFFFFF

Sifre 2: FFFFFFFFFF1

Durum Bilgisi

```

Com port açıldı
RX < FF 00 02 82 4C D0 (Select işlemi başarılı)
RX < FF 00 06 82 03 A6 DD 5A C9 31(Seri No: C95ADDA6)
RX < FF 00 02 85 4C D3 (Authentication işlemi başarılı)
Ürünün fiyatı:147

RX < FF 00 02 82 4C D0 (Select işlemi başarılı)
RX < FF 00 06 82 02 62 43 95 37 FB(Seri No: 37954362)
Hata:Authentication işlemi başarısız.
RX < FF 00 02 82 4C D0 (Select işlemi başarılı)
RX < FF 00 06 82 02 62 43 95 37 FB(Seri No: 37954362)
Hata:Authentication işlemi başarısız.
RX < FF 00 02 82 4C D0 (Select işlemi başarılı)
RX < FF 00 06 82 02 62 43 95 37 FB(Seri No: 37954362)
Hata:Authentication işlemi başarısız.
RX < FF 00 02 82 4C D0 (Select işlemi başarılı)
RX < FF 00 06 82 02 62 43 95 37 FB(Seri No: 37954362)
Hata:Authentication işlemi başarısız.

RX < FF 00 02 82 4C D0 (Select işlemi başarılı)
RX < FF 00 06 82 02 22 3D 95 37 B5(Seri No: 37953D22)
RX < FF 00 02 85 4C D3 (Authentication işlemi başarılı)
RX < FF 00 02 87 49 D2 Hata:Bu bir VALUE block değil
RX < FF 00 12 86 01 48 61 72 74 20 53 61 68 69 62 69 3A 20 42 75 72 1E (Blok okundu)
RX < FF 00 12 86 02 63 75 20 54 55 47 41 43 0D 0A 48 65 73 61 70 20 2E (Blok okundu)
RX < FF 00 02 85 4C D3 (Authentication işlemi başarılı)
RX < FF 00 12 86 04 4E 6F 20 20 20 3A 20 32 35 34 36 39

```

Kredi Kartı Bilgisi

Kart Sahibi: Aktül KAVAS  
Hesap No : 854976521  
Banka adı : Yapı Kredi  
Subesi : Zeynep Kamil

Bir önceki bakiye:5500  
Harcanan Miktar:147  
Kalan Bakiye:5353

Başlat Windows Messenger Microsoft Word Gelen Kutusu - Micros... Form1 TR 10:23

**Şekil 9.7 Kredi kartına bakiye için geçerli şifre girişindeki yazılım ekranının görüntüsü**



## 10 SONUÇ

Son yıllarda RFID (Radyo Frekansı ile Kimlik Tanıma) Teknolojisi sağladığı kullanım kolaylıkları, üretim ve stoklama bantlarında, ürün takibinde sağladığı kesinlik ve performans sebebiyle diğer kimlik tanıma sistemlerine nazaran daha çok ön plana çıkmıştır.

RFID halen gelişmekte olan bir teknoloji olduğundan kullanım modelleri ve bütünleşik mimarisi sürekli değişmektedir. RFID teknolojisinin bugüne kadar yaygınlaşmamasındaki etkenlerden biri olan etiket maliyetleri de geliştirilen nano teknolojisi ile ortadan kalkmaktadır. RFID etiketlerin antenlerinin nano boyutlarda üretilmesi ile etiket fiyatları oldukça düşecek ve RFID kullanımının yaygınlaşmasında önünü tıkayan engeller bir bir giderilecektir. RFID' nin çözüme kavuşturulması gereken, "standartlar", "güvenlik-gizlilik prensibi" ve "okuyucu/etiket çarpışmaları" gibi diğer sorunlarına da gelişen teknoloji yeni çözümler üretmektedir.

Şu anda çok büyük perakendeciler, market zincirleri ve ordu RFID teknolojisini etkin bir şekilde kullanmak için çalışmalar yapmaktadır. RFID teknolojisinin kullanımında 2009 yılına kadar %120'lik bir artış beklenmektedir.

Lojistik araç takiplerinin RFID sistemlerle yapıldığı, otobanların otomatik geçiş sistemlerinin, şirket, okul girişlerinin, marketlerde ürün etiketlerinin takibinin ve bankalarla ilgili birçok işlemde RFID sisteminin kullanıldığını düşünürsek, bu tez çalışması için en güzel uygulama örneğinin; hem ürünün okutulduğu, hem kimlik tanıma işlemin yapıldığı, hem de kredi kartı işlemlerini birleştiren bir e-money; "elektronik para" uygulaması olduğu düşünülmüştür.

Bu sebeple tez uygulamasında Visual Studio 2005. NET platformunda C# dilinde geliştirilen bir yazılım ile RFID teknolojisi kullanılarak kredi kartı ile ürün satın alım uygulaması yapılmıştır. Ürün etiketi okutuldukça ürünlerin fiyatlarını toplayan ve kredi kartı bakiyesinden doğru şifre girildiği takdirde işlem yaparak hesaptan düşen ve kalan bakiyeyi karta işleyen bir yazılım geliştirilmiştir.



Elektronik para uygulaması için kartın okutulma mesafesinin uzun olması gerekmediğinden, uygulamada yaklaşık 10 cm' ye kadar başarı ile okuyabilen, adaptöre ihtiyaç duymadan çalışan (pasif etiket) olan Mifare kartlar tercih edilmiştir. Tez uygulamasında, gerekli anten ve okuyucuyu da beraberinde içeren, yüksek frekanslarda çalışan, 13,56 MHz de işlem yapan, SM1013 demo kiti kullanılmıştır. Ürünler ve kişiler için ayrı ayrı kartlar tanımlanarak, ürün kart bilgileri ve kredi kartı için kimlik ve bakiye bilgileri demo kitin SMRFID programı ile işlenmiştir.

C# (Csharp) dilinde geliştirilen yazılımda, bir kart, okuyucuya okutulduğunda, kartın kredi kartı mı yoksa ürün kartı mı olduğu bilgisini ayırt edip, okuduğu ürün fiyatını ekrana yazması ve ürün kartlarının etiketleri arka arkaya okutuldukça, ürün fiyatlarını toplayarak bunu toplam harcama olarak ekrana yazması sağlanmıştır.

Radyo frekansı ile kimlik tanınması, kart bilgilerinin okutulması ve kredi kartından bakiyenin görülmesi veya bakiye üzerinden işlem yapılması işlemleri de iki ayrı şifreye tabi tutulmuştur. Yazılım, kart bilgilerine erişim için gerekli şifrenin doğru olması şartıyla kart bilgilerinin okunmasına ve ancak bakiye bloğu için tanımlanan şifrenin girilmesi şartıyla bakiyeden harcamanın düşülmesine izin verecek şekilde tasarlanmıştır. Aksi durumda, kart bilgilerine ve bakiye bilgilerine erişim ve işlem yapılabilmesi engellenmiştir.

Radyo frekansıyla kimlik tanıma ile şifre doğrulama tamamlandığında, yazılım, kredi kartı bilgilerinin ve hesap bakiyesinin ekrana yazılması ile işlemi başlatır. Toplam harcanan meblağın hesap bakiyesinden düşülmesi ile toplam harcanan miktar ve kalan bakiye ekrana yazdırıldıktan sonra, kalan bakiyenin aynı anda kredi kartına da işlenmesi ile de son bulur.

Bu tez çalışmasında, tez danışmanı ve öğrencisinin adlarına iki kredi kartı düzenlenmiştir. Ancak bu uygulamada kartlar bankaların veri tabanı ile haberleşmemektedir. Bu para kartları ile üç ayrı ürün için alışveriş yapıldığı kabul edilerek RFID teknolojisi ile örnek bir uygulama gerçekleştirilmiştir. Böylelikle



radio frekansı ile hem kimlik tanıma, hem ürün tanıma hem de kartta girilmiş olan bilgiler ile işlem yapabilme, başarılı olarak gösterilmiştir.

Erdoğan, Mustafa, "RFID: Deploying Radio Frequency Identification Systems"

Ellis, Wolfgang, René, Wolfgang, "Smart Card Handbook, Smart Card Handbook"

Ehrsam, Adrien, Gery, Urs, Jacomet, Marcel, "Contactless Identification Device With Anticollision Algorithm", University of Applied Sciences, Switzerland

Estevez-Tamayo, Juan M., Hernandez-Castro, Julio Cesar, Rodriguez, Arnau, Peris-Lopez, Pedro, "RFID Systems: A Survey on Security Threats and Proposed Solutions"

Finkenzeller, Klaus, "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification 2nd Edition (Hardcover)"

Glover, Bill, "RFID Essentials (Theory in Practice (O'Reilly))"

Haghiri, Yahya, Tarantino, Tammara, "Smart Card Manufacturing Card Production"

Harper, Jim, (June 21, 2004, ), "RFID Tags and Privacy", Competitive Enterprise Institute, No. 89, Washington DC.

Kraus, John D., Marhefka, Roland J., Antenna

Shepard, Steven, "RFID (McGraw-Hill Networking Professional)"

Sweeney, Patrick J. II, "RFID For Dummies"

David M Pozar, "Microwave Engineering", John Wiley & Sons ISBN 0-471-17096-8 Second Edition 1998.

"Kısa Mesajlı Erşimli Telix Cihazlarının(KET) Kurma ve Kullanma İrselleri" Mucemelligi-06.03.2004 tarih 25394 sayılı Resmî gazete

John D.Kraus Ronald J.Marhefka "Antenna for Air Applications" McGraw Hill, ISBN 0-07-212103-2 Third Edition, 2002.

Constance A. Balanis "Antenna Theory" John Wiley & Sons, ISBN 0-471-59268-4 1997.

Kavaz Arslan, "Endüktif Kaptajlı Radyo Frekans Kimlik Tanıma Sistem Optimizasyonu"



## KAYNAKLAR

Bhuptani, Manish, "RFID Field Guide: Deploying Radio Frequency Identification Systems"

Effing, Wolfgang, Rankl, Wolfgang, "Smart Card Handbook Smart Card Handbook"

Ehrsam, Adrian, Gehrig, Urs, Jacomet, Marcel, "Contactless Identification Device With Anticollision Algorithm", University of Applied Sciences Berne, Switzerland

Estevez-Tapiador, Juan M., Hernandez-Castro, Julio Cesar, Ribagorda, Arturo, Peris-Lopez, Pedro, "RFID Systems: A Survey on Security Threats and Proposed Solutions"

Finkenzeller, Klaus, "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification 2nd Edition (Hardcover)"

Glover, Bill, "RFID Essentials (Theory in Practice (O'Reilly))"

Haghir, Yahya, Tarantino, Tarantino, " Smart Card Manufacturing Card Production"

Harper, Jim, (June 21, 2004, ), "RFID Tags and Privacy", Competitive Enterprise Institute, No. 89, Washington DC.

Kraus, John D., Marhefk, Roland J., Antenna

Shepard, Steven, "RFID (McGraw-Hill Networking Professional)"

Sweeney, Patrick J. II, "RFID For Dummies"

David M Pozar, "Microwave Engineering", John Wiley & Sons ISBN 0-471-17096-8 Second Edition 1998.

"Kısa Mesafe Erişimli Telsiz Cihazlarının(KET) Kurma ve Kullanma Esasları" yönetmeliği 06.03.2004 tarih 25394 sayılı Resmi gazete

John D.Kraus,Ronald J.Marhefka "Antenna for All Applications" McGraw Hill, ISBN 0-07-232103-2 Third Edition, 2002,

Constantine A.Balanis "Antenna Theory" John Wiley&Sons,ISBN 0-471-59268-4 1997.

Kavas Aktül; "Endüktif Kuplajlı Radyo Frekans Kimlik Tanıma Sistem Optimizasyonu"



## INTERNET KAYNAKLARI

- [1] [http://www.tgdaily.com/2006/08/21/infineon\\_supplies\\_rfid\\_chips\\_to\\_us\\_government/](http://www.tgdaily.com/2006/08/21/infineon_supplies_rfid_chips_to_us_government/)
- [2] <http://www.permadi.com/tutorial/numDecToHex/> açıklaması
- [3] <http://www-128.ibm.com/developerworks/wireless/library/wi-rfid/>
- [4] [http://tech.monstersandcritics.com/news/article\\_1006608.php/Nano\\_World\\_Nano\\_will\\_boost\\_RFID\\_tags](http://tech.monstersandcritics.com/news/article_1006608.php/Nano_World_Nano_will_boost_RFID_tags)
- [5] [http://en.wikipedia.org/wiki/Radio\\_Frequency\\_Identification](http://en.wikipedia.org/wiki/Radio_Frequency_Identification)
- [6] <http://rfid-handbook.de/rfid/index.html>
- [7] [http://media.wiley.com/product\\_data/excerpt/27/04708440/0470844027.pdf](http://media.wiley.com/product_data/excerpt/27/04708440/0470844027.pdf)
- [8] [www.dyna-sys.com](http://www.dyna-sys.com)
- [9] [www.rfidusa.com](http://www.rfidusa.com)
- [10] <http://www.ti.com/rfid/shtml/prod-trans.shtml>
- [11] <http://www.microchip.com/>
- [12] <http://www.cs.berkeley.edu/~dmolnar/library.pdf>
- [13] <http://www.bosgrup.com/pdf/otvtrfid.pdf>
- [14] <http://ww1.microchip.com/downloads/en/AppNotes/00680b.pdf>
- [15] <http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=24>
- [16] [http://www.autoid.org/2002\\_Documents/sc31\\_wg4/docs\\_501-520/520\\_18000-7\\_WhitePaper.pdf](http://www.autoid.org/2002_Documents/sc31_wg4/docs_501-520/520_18000-7_WhitePaper.pdf)



**EKLER****EK 1 ISO RFID Standartları (03.02.2005)**

Standart	Açıklama	Aşama
10536	Tanımlama kartları – İletişimsiz bütünleşik devre(ler) kartları. -10 cm ye kadar.	İnceleme 2004-12-31
11784	Hayvanların Radyo frekans tanımlama ile tanımlanması – Kod yapısı	İnceleme 2003-11-07
11785	Hayvanların Radyo frekans tanımlama ile tanımlanması – Teknik kapsam	İnceleme 2001-09-19
14443-1	Tanımlama kartları – İletişimsiz bütünleşik devre(ler) kartları–“Proximity” kartları –Bölüm1 : Fiziksel özellikleri	İnceleme 2003-10-13
14443-2	Tanımlama kartları – İletişimsiz bütünleşik devre(ler) kartları – “Proximity” kartları – Blüm2: Radyo frekans gücü ve sinyal arayüzü	Yayımlandı 2001-06-28
14443-3	Tanımlama kartları – İletişimsiz bütünleşik devre(ler) kartları – “Proximity” kartları – Bölüm 2 : İlkeme ve kalabalığı önleme	Yayımlandı 2001-02-01
15693-1	Tanımlama kartları – İletişimsiz bütünleşik devre(ler) kartları – “Vicinity” kartları - Bölüm 1 : Fiziksel özellikleri 1998’de, Philips ve Texas Instruments firmaları ISO-15693 ile uygulamalar geliştirdi. Amaç tek antenli bir okuyucu ile 50-70cm ye kadar başarılı okuma yapabilmek.	İnceleme 2003-10-14
15693-2	Tanımlama kartları – İletişimsiz bütünleşik devre(ler) kartları – “Vicinity” kartları – Bölüm 2 : Hava arayüzü ve ilkeme	İnceleme 2003-10-14
15693-3	Tanımlama kartları – İletişimsiz bütünleşik devre(ler) kartları–“Vicinity” kartları– Bölüm 3 : Kalabalıklık önleme ve iletim protokolü	Yayımlandı 2001-03-29



15961	Ürün yönetimi için Radyo frekans tanımlama (RFID) – Veri protokolü: uygulama arayüzü	Yayımlandı 2004-10-18
15962	Ürün yönetimi için Radyo frekans tanımlama (RFID)– Veri protokolü: Veri kodlama kuralları ve mantıksal hafıza fonksiyonları	Yayımlandı 2004-10-18
15963	Ürün yönetimi için Radyo frekans tanımlama (RFID) – RF tagları için tekil tanımlama	Yayımlandı 2004-09-08
18000-1	Ürün yönetimi için Radyo frekans tanımlama (RFID) – Bölüm 1: Referans mimarisi ve standartlaştırılacak parametrelerin tanımlanması	Yayımlandı 2004-09-13
18000-2	Ürün yönetimi için Radyo frekans tanımlama (RFID) – Bölüm 2: 135 kHz altı hava arayüzü haberleşmesi için parametreler	Yayımlandı 2004-09-13
18000-3	Ürün yönetimi için Radyo frekans tanımlama (RFID) – Bölüm 3: 13,56 MHz'de hava arayüzü haberleşmesi için parametreler	Yayımlandı 2004-09-13
18000-4	Ürün yönetimi için Radyo frekans tanımlama (RFID) – Bölüm 4: 2,45 GHz'de hava arayüzü haberleşmesi için parametreler	Yayımlandı 2004-08-31
18000-6	Ürün yönetimi için Radyo frekans tanımlama (RFID) – Bölüm 6: 860 MHz - 960 MHz arası hava arayüzü haberleşmesi için parametreler	Yayımlandı 2004-08-31
18000-7	Ürün yönetimi için Radyo frekans tanımlama (RFID) – Bölüm 7: 433 MHz'de etkin hava arayüzü haberleşmesi için parametreler	Yayımlandı 2004-08-31



## EK 2 ISO RFID Standart Taslakları (03.02.2005)

Standart	Açıklama	Aşama
17358	RFID için tedarik zinciri uygulaması – Uygulama gereksinimleri	20 - Hazırlık
17363	RFID için tedarik zinciri uygulaması – Taşıma konteynerleri	20 – Hazırlık
17364	RFID için tedarik zinciri uygulaması – Nakil birimleri	20 – Hazırlık
17365	RFID için tedarik zinciri uygulaması – Geri dönüşümlü nakil ürünleri	20 – Hazırlık
17366	RFID için tedarik zinciri uygulaması – Ürün paketleme	20 - Hazırlık
17367	RFID için tedarik zinciri uygulaması – Ürün etiketleme	20 - Hazırlık
18047-7	Otomatik tanımlama ve veri yakalama teknikleri – RFID cihazı uyumluluk test yöntemleri – Bölüm 7: 433 MHz’de hava arayüzü haberleşme sınama yöntemleri	30 - Komite
19762-3	Otomatik tanımlama ve veri yakalama teknikleri – Ortaklaştırılmış terimler – Bölüm 3: Radyo frekans tanımlama (RFID) (sadece İngilizce)	50 - Onama
24710	Otomatik tanımlama ve veri yakalama teknikleri – Ürün yönetimi için Radyo frekans tanımlama	40- Araştırma



**ÖZGEÇMİŞ**

Doğum tarihi	07.01.1980	
Doğum yeri	İstanbul	
Lise	1991-1997	Kadıköy Anadolu Lisesi
Lisans	1997- 2001	Yıldız Teknik Üniversitesi Elektrik-Elektronik Fak. Elektronik ve Haberleşme Mühendisliği Bölümü
Yüksek Lisans	2005-2007	Yıldız Teknik Üniv. Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Müh. Ana Bilim Dalı Haberleşme Programı

**Çalıştığı Kurumlar**

2006- Devam	RETURN Bilişim Genel Koordinatörü (TÜBİTAK- Teknoloji Geliştirme Bölgesi)
2000- 2002	TURKCELL
2000 – Staj	ALCATEL
1999 – Staj	TURCOM-Telecom-İntcom



