T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YAKIN ALAN HABERLEŞMESİ (NFC) VE UYGULAMALARI

YÜKSEK LİSANS TEZİ

Elektrik ve Elektronik Müh. Mehmet Suyuti DİNDAR

Enstitü Anabilim Dalı	**:**	**ELEKTRONİK MÜHENDİSLİĞİ**
Enstitü Bilim Dalı	**:**	**ELEKTRONİK**
Tez Danışmanı	**:**	**Prof. Dr. Uğur ARİFOĞLU**

Nisan 2010

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YAKIN ALAN HABERLEŞMESİ (NFC) VE UYGULAMALARI

YÜKSEK LİSANS TEZİ

Elektrik ve Elektronik Müh. Mehmet Suyuti DİNDAR

Enstitü Anabilim Dalı : ELEKTRONİK MÜHENDİSLİĞİ

Enstitü Bilim Dalı : ELEKTRONİK

Bu tez 28 / 04/2010 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

.....	.....	.....
Jüri Başkanı	**Üye**	**Üye**

ÖNSÖZ

Yakın alan iletişimi (NFC) kablosuz bir iletişim teknolojisidir. NFC, elektronik cihazlar arasında yakın mesafeli haberleşmeyi sağlar. ISO/IEC tarafında 8 Aralık 2003 tarihinde standart olarak kabul edilmiştir. NFC teknolojisi, cihazların birbirine dokunacak kadar yaklaştıkları zaman etkin olmakta ve cihazların birbirleri ile konuşabilmeleri sağlamaktadır. Bu cihaz sahipleri için prikolojik rahatlık, kullanım kolaylığı ve güvenlik sağlamaktadır. NFC teknolojisi şu tip uygulamalar için yaygın bir şekilde kullanılacaktır. Evler, arabalar, otel odaları ve garajlar için elektronik anahtarlar, Cep telefonları ve diğer mobil cihazlara entegre olarak kullanılabilecek Elektronik cüzdanlar, Elektronik biletler, elektronik kümlük dokümanları ve mobil ticaret uygulamaları. NFC tipik olarak bir kaç santimetre olan kısa mesafe kapsamında çalışır. Radyo frekansı ile tanımlama (RFID) ve Temassız Akıllı kart alt yapısında çalışır.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

APDU	Application Protocol Data Unit
API	Application Programming Interface
ASD	Application Security Domain
ASK	Amplitude Shift Keying
BASK	Binary Amplitude Shift Keying
CAPI	Cryptographic API
CDC	Connected Device Configuration
CDMA	Code division Multiple Access
CEPT	European Conference of Postal and Telecommunications Administrations
CLDC	Connected Limited Device Configuration
COS	Card Operating System
CRC	Cyclic Redundancy
CSP	Communicating Sequential Process
CVM	Compact Virtual Machine
CVM	Card Verification Method
DSA	Digital Signature Algorithm
ECDSA	Elliptic curve Digital Signature Algorithm
EDGE	Enhanced Data for GSM Evolution
EEPROM	Electronically Erasable Programmable Read Only Memory
EMV	Europay Mastercard Visa
ETSI	European Telecommunications Standards Institue
GC	Garbage Collector
GCF	Generic Connection Framework
GGSN	GPRS Gateway System Node

GND	Ground
GPRS	General Packet Radio Service
GSM	Global System for Mobile
HF	High Frequency
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
I/O	Input / Output
I2C	Inter Integrated Circuit
ICC	Integrated Circuit Card
IrDA	Infrared Data Association
ISD	Issuer Security Domain
ISO	International Organization of Standardization
J2EE	Java 2 Enterprise Edition
J2ME	Java 2 Micro Edition
J2SE	Java 2 Standard Edition
JAD	Java Application Descriptor
JAR	Java Archive
JCOP	Java Card Operating System
JCP	Java Community Process
JNI	Java Native Interface
JSR	Java Specifications Requests
JVM	Java Virtual Machine
LAN	Local Area Network
LF	Low Frequency
MA	Mobile Application
MAC	Message Authentication Cryptogram
MIDlet	MIDP Application
MIDP	Mobile Information Device Profile
MIM	Man-in-the-Middle
MIME	Multipurpose Internet Mail Extensions
MMC	Multimedia Card
MNO	Mobile Network Operator

MPA	Mobile Payment Application
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
OS	Operating System
OTA	Over-the-Air
PA	Payment Application
PC	Personal Computer
PCB	Printed Circuit Board
PCD	Proximity Coupling Device
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PCSC	Personal Computer Smart Card
PIN	Personal Identification Number
PN	Payment Network
POS	Point Of Sale
qVSDC	Quick Visa Smartcard Debit Credit
RFC	Request For Comments
RFID	Radio Frequency Identification
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman
RST	Reset
RTD	Record Type Definition
S2C	Sign In-Sign Out Connection
SATSA	Security And Trust Service API
SC	Secure Channel
SCSI	Smart Computer System Interface
SD	Secure Digital
SDD	Single Device Detection
SDK	Software Development Kit
SE	Secure Element
SIM	Subscriber Identity Module
SK	Session Key

SMSC	Short Message Service Center
SPI	Serial Peripheral Interface
SSA	Service Activation Application
SWP	Single Wire Protocol
TSM	Trusted Service Manager
UHF	Ultra High Frequency
UICC	Universal Integrated Circuit Card
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
VCC	Common Collector Voltage
VCD	Vicinity Coupling Device
VIS	Visa ICC Spects.
VMG	Visa Mobile Gateway
VMP	Visa Mobile Platform
VSDC	Visa Smartcard Debit Credit
WI	Wired Interface
XML	Extensible Markup Language

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Yakın alan haberleşmesi, NFC, RFID, Akıllı kartlar, Mobil cihazlar,

Mobil ödeme sistemleri

Yakın Alan Haberleşmesi (NFC) radyo frekansları kullanılarak elektronik cihazlar arasında gerçekleştirilen kısa mesafeli bir haberleşme teknolojisidir. Mobil teknolojilerin yaygınlaşması ile beraber NXP ve Sony firmalarının öncülüğünde güvenli ve basit haberleşme teknolojisi olan NFC geliştirilmeye başladı. Mevcut RFID teknolojilerini de destekleyen NFC, üzerinde bulundurduğu Güvenli Eleman sayesinde bankacılık gibi güvenliğin üst seviyede ihtiyaç duyulduğu uygulamaları gerçekleştirme imkanını sağladı. NFC teknolojilerinin yayılması ile bir çok son kullanıcı etkileşimli, yüksek güvenlik gerektiren mobil uygulama üretilmeye başlandı. NFC teknolojisinin önümüzdeki yıllarda özellikle ödeme sistemlerinde büyük imkanlar ve fırsatlar oluşturması beklenmektedir. Halen bir çok ülkede pilot çalışmaları devam etmektedir.

NEAR FIELD COMMUNICATIONS

SUMMARY

Key Words: Near Field Communication, RFID, Smartcard, Mobile Payment

Near Field Communication (NFC) is a short-range wireless connectivity technology standard designed for intuitive, simple and safe communication between electronic devices. NFC communication is enabled by bringing two NFC compatible devices within a few centimeters of one another. Applications of NFC technology include contactless transactions such as payment and transit ticketing, simple and fast data transfers including calendar synchronization or electronic business cards and access to online digital content.

BÖLÜM 1. GİRİŞ

Çok hızlı hareket eden bir dünyada yaşıyoruz. İnsanlar bulmak istedikleri şeyleri tek bir cihaz üzerinde arıyor, buluyor, satın alıyor ve paylaşıyor. Mobil cihazlar sürekli erişim imkanları, bütünleşik olmaları, sağladıkları multimedya özellikleri ile tüm bu ihtiyaçları karşılamak için en uygun ortamlardır.

Günümüzde insanların bir çoğu neredeyse bir mobil cihaz taşımaktadırlar. Geçtiğimiz on yıl içerisinde de mobil servis sağlayıcılar basit ses iletişimi ve SMS işlemlerinden multimedya servisleri, TV, internet ve hatta çevrim içi sağlık izleme teknolojilerine kadar çeşitli alanlarda gelişmeler gösterdiler.

Son yirmi yılda mikroişlemci temelli akıllı kartların kullanımının belirgin özelliği veri erişim kontrolleri ve işlem takibi idi. Önceleri basit hafıza kartları, sonra akıllı temaslı kartlar ve daha sonra da akıllı temassız kartların kullanımı ile akıllı kart teknolojileri de gelişti.

Tüm bu uygulamaların geliştirilmesinin ve kullanılmasının önündeki en büyük problem kullanıcıların her bir servis için ayrı kartlar taşıması gerekliliği idi. Ulaşım, sinema, market, kütüphane, bina erişimi için ayrı akıllı kartlar olmalıydı. 1990'lı yıllarda elektronik cüzdan ve çoklu uygulamalı akıllı kart denemeleri bu sosyal hayalin gerçekleştirilebileceğinin ışığını gösterdi.

Aranan cevap tüm işlemlerin yapılabileceği bir işlem gücü ve birden fazla bağımsız uygulama çalıştırabilen akıllı kartlar veya tüm bu uygulamaları taşıyabilecek mobil bir cihaz idi. Mantıklı çözüm cep telefonları idi.

NFC, yakın alan haberleşmesi anlamına gelen Near Field Communication'ın baş harflerinden oluşur. NFC teknolojisi 2004 yılında NXP ve Sony'nin katkıları ile

geliştirildi. NFC, yapılan çalışmalarla kısa mesafe yüksek frekanslı haberleşme ile radyo frekansları kullanılarak temassız tanımlama teknolojilerini bir araya getirerek uluslararası standartlara kavuşturuldu.

NFC, iki cihaz arasında 10 santimetreye kadar mesafeden temassız olarak veri alışverişinin yapılmasını sağlar. Bu kısa mesafede NFC cihazlar endüktif bağlantı ile (inductive-coupling) çalışma için güç ve veri paylaşırlar.

NFC iki temel standart ile tanımlanmış açık platform bir teknolojidir. Bu satndartlar ECMA - 340 ve ISO / IEC 18092 isimli standartlardır. Bu standartlar daha önceden yayınlanmış olan ISO 14443 A ve B standartlarını da barındırmaktadır. Temassız akıllı kartı ve okuyucusunu tek bir cihaz üzerinde toplamak diğer temassız akıllı kartlar ve diğer NFC cihazlar ile haberleşmeyi mümkün kılmaktadır. NFC teknolojisi halen başarılı bir şekilde kullanılmakta olan RFID ve temassız akıllı kart teknolojisine çok benzemekle beraber yepyeni özellikleri de kazandırmıştır. Ayrıca Bluetooth, Wi-Fi ve RFID gibi temassız teknolojilerle de uyumludur. NFC haberleşmesi tüm dünyada lisans gerektirmeyen 13.56 MHz frekansında çalışmaktadır.

NFC basit temassız akıllı kartların sağladığı özelliklere ilaveten uçtan uca bağlantı, yüksek hızlı çift yönlü haberleşme ve üzerinde çalıştığı mobil cihazın diğer özelliklerine erişebilme imkanı sağlar. Bu sayede çok daha gelişmiş ve nitelikli, yeni özelliklere sahip mobil uygulamalar oluşturulabilmektedir.

GSMA'nın mobil cihazlardaki ödeme uygulamaları için güvenli eleman (Secure Element) önerisi SIM kart olarak da bilinen Universal Integrated Circuti Card (UICC)'dir. Günümüzde UICC'ler hızla gelişerek işlem gücü, sağladıkları güvenlik seviyeleri ve hafıza imkanları artmaktadır. UICC'lerin üzerindeki uygulamaların birbirinden bağımsız olarak kurulabilmesi ve çalıştırılabilmesi sayesinde üçüncü parti hizmet sağlayıcılar mobil servis sağlayıcılardan bağımsız olarak uygulama geliştirebilmektedirler.

Bu çalışmada NFC teknolojisini meydana getiren unsurlar, teknoloji temelleri, donanımsal mimari, uygulama geliştirme ortamları ve örnek bir NFC uygulaması incelenmiştir.

İkinci bölümde NFC'nin temel unsurlarından biri olan RFID teknolojisi kısaca tanıtılmaktadır. Bölümde RFID'nin çalışma prensibi ve kullanım alanları konu edilmiştir. NFC teknolojisi RFID teknolojisini geriye uyumlu olarak desteklemektedir. NFC donanımları mevcut, kullanılmakta olan RFID etiketlerini okuyup yazabilmektedir. Bir çok NFC uygulaması sahada RFID etiketler kullanılarak gerçekleştirilmektedir.

Üçüncü bölümde NFC teknolojisinin bir diğer önemli unsuru olan akıllı kart teknolojisi incelenmiştir. Akıllı kartlar veri taşıma, güvenlik işlemleri ve otonom karar verebilme yetenekleri ile özellikle bankacılık alanında oldukça yoğun şekilde kullanılmaktadır. Sağladıkları yüksek güvenlik özellikleri ile değerli bilgileri taşıma özelliklerine sahiptirler. Bölümde bir akıllı kartın yapısı, temel özellikleri, işletim sistemi, dosya sistemi, programlanması ve haberleşmesi konusunda bilgiler verilmektedir.

Dördüncü bölümde yakın alan haberleşmesi, NFC, konusunda temel bilgiler verilmektedir. NFC'nin kullanım alanları, standartları ve geliştirilme süreçleri incelenmektedir. NFC cihazların aktif ve pasif haberleşme modları, kullanılan modülasyon ve kodlamalar, çakışma önleme gibi protokol incelemesi yapılmıştır. NFC, Bluetooth, IrDA gibi diğer temassız haberleşme teknolojileri ile karşılaştırılmıştır. Bölümde NFC'nin kart emulasyonu, okuyucu ve uçtan uca çalışma modları incelenmiştir. Ayrıca mobil cihazlardaki NFC-WI ve NFC-SWP donanım mimarileri de detaylı olarak incelenmiştir.

Beşinci bölümde temassız haberleşmede önemli bir unsur olan güvenlik konu edilmiştir. Bankacılık gibi değerli verilerin taşındığı ve temassız olarak gerçekleşen haberleşmenin güvenliği oldukça önemlidir. Radyo frekansları ile gerçekleşen haberleşme üçüncü şahıslar tarafından izlenebilmektedir. NFC'nin kısa mesafeli haberleşmesi hernekadar davetsiz misafirleri haberleşmeden uzak tutsa da önlenemez

değildir. Bölümde veri bozma, veri dinleme, veri enjeksiyonu, Man-in-the-Middle gibi saldırı tipleri incelenmiş ve alınabilecek önlemler zikredilmiştir. Ayrıca haberleşme güvenliği gibi mobil uygulamanın da güvenliği konu edilmiş, alınabilecek önlemler sıralanmıştır.

Altıncı bölümde NFC özellikli mobil yazılımların geliştirilmesinden bahsedilmiştir. Günümüzdeki mobil cihazların çeşitliliğinin yol açtığı karmaşıklık ve sorunların yazılımsal boyutta çözümü ve üretilen yeni yazılımsal teknolojiler konu edilmiştir. Temelde Sun Microsystems tarafından geliştirilen Java paketleri, özellikle JSR-257 incelenerek bir NFC haberleşmesinin nasıl gerçekleştirildiği örnek kodlarla gösterilmiştir.

Yedinci ve son bölümde Visa tarafından geliştirilen bir NFC mobil uygulaması olan Visa Mobile Payment Application (VMPA) detaylı olarak incelenmiştir. Bölümde uygulamanın kullanıcı tarafından nasıl kullanıldığı, ne tür özellikleri haiz olduğu incelenmiş, uygulamanın içinde bulunduğu ekosistem tanımlanmıştır.

BÖLÜM 2. RFID SİSTEMLER

RFID (Radio Frequency Identification) teknolojisi, okuyucunun (reader) radyo frekanslı dalgalar göndererek, etiket (Tag) üzerindeki chip'i aktive edip, içinde bulunan, daha evvel yazıcı (writer) tarafından kaydedilmiş veriyi okuma teknolojisidir. Bu teknoloji, kişi ve nesneleri tanıma ve takip etme anlamında, temel olarak kablosuz iletişim ve yarıiletken teknolojilerinin entegrasyonundan oluşmaktadır. Standart bir RFID sisteminde aşağıdaki donanım bileşenleri yer almaktadır:

- RF Etiketi (Tag) : Bilgi depolama özelliğine sahip yarıiletken
- Anten: Okuyucunun etiket ile haberleşmesini sağlayan donanım
- Okuyucu: Etiket ile haberleşerek bilgi alışverişini gerçekleştiren donanım
- Etiket Programlama Donanımı: Okuyucu, yazıcı(printer)

2.1. RFID Teknolojisine Genel Bir Bakış

RFID, temel olarak nesnelerin ve kişilerin kimlik ve tanımlama gibi bilgilerini elektronik bir etiket yardımı ile tanımlamaya yarayan teknolojiye verilen addır. Bu etiketler bir verici, yani anten içermektedir. Antenlerinden yaydıkları mesajlar, RFID okuyucuları tarafından alınıp işlenebilecek niteliktedir. Bu elektronik etiketler en basit anlamda okuyucu tarafından nesnenin tanınmasını sağlayan tanımlama, yani kimlik bilgilerini içermektedir.

Nesneyi perakende sektöründe bir ürün, bu bilgiyi de ürün stok numarası olarak düşünebiliriz. Bu tip etiketler bir defa kodlanabilen etiketlerdir. Ayrıca bazı RFID etiketleri tekrar yazılabilir hafızaya sahiptir. Ve böylece bu etikette bulunan kimlik

bilgilerinde kolaylıkla değişiklik yapılabilir. Bu tanımlamalara göre RFID teknolojisinin sınırsız kullanım alanına sahip olduğu ortaya çıkmaktadır.

RFID etiketleri; sahip oldukları güç kaynaklarına göre aktif ve pasif etiketler olmak üzere iki genel kategoriye ayrılır.

Aktif RFID etiketleri kendi güç kaynaklarını yapısında bulundurur ve bu genellikle anakart üzerinde bulunan bir pildir.

Pasif etiketler ise bilginin iletimi için gereken gücü okuyucunun yaydığı sinyalden almaktadır.

Aktif ve pasif etiketler de sahip oldukları bilginin okunma tipine göre ve frekans okuma mesafelerine göre kendi arasında çeşitli gruplara ayrılmaktadır.

2.2. RFID Teknolojisinin Tarihçesi

Radyo frekansı ile tanımlama sistemleri ilk 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 [1].

2.3. RFID Sistem Bileşenleri

Radyo frekans tanımlama sistemleri, radyo frekansı ile yapılan sorguları almaya ve cevaplamaya olanak tanıyan etiket (transponder), okuyucu (alıcı- verici) ve alınan bilgilerin depolandığı veri tabanından oluşmaktadır. Radyo frekans kimlik tanıma sistem haberleşmesinde okuyucu radyo frekans sinyallerini gönderir. Okuyucunun radyo frekans alanına girmiş bulunan pasif etiket, haberleşmesi için gerekli olan enerjiyi bu alandan alır. Etiket haberleşmesi için gerekli olan enerjiyi aldığında, üzerinde depolanmış bilgiye göre taşıyıcı sinyali modüle eder. Modüle edilmiş taşıyıcı etiketten okuyucuya gönderilir. Okuyucu modüle edilmiş sinyali algılar,

şifresini çözer ve okur. Son olarak alınan bilgi veri tabanının bulunduğu bilgisayara aktarılır.

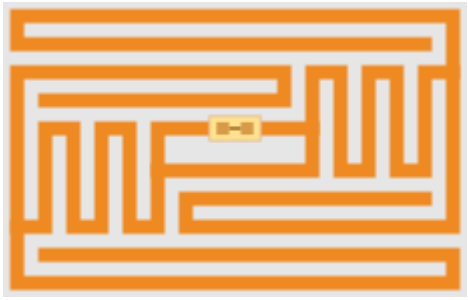
2.3.1. Etiket (Tag) ve Transponder

RFID etiketi, radyo frekansı kullanılarak yapılan sorgulamaları alan cevaplayan sınırlı kapasitede belleğe sahip, taşınabilen, içinde bilgi barındıran, mikro yonga, anten ve taban malzemesinden oluşmaktadır. Mikro yonga etiketin üzerinde yer aldığı nesneye ilişkin bilgileri depolar. Anten radyo frekansı kullanarak nesneye ait bilgilerin okuyucuya gönderilmesini sağlar. Taban malzemesi ise etiketin nesne üzerine yerleştirilebilmesi için mikro yonga ve anteni çevreler. Şekil 2.1' de bir RFID etiket yapısı gösterilmektedir. Etiketler kullanım yerlerine bağlı olarak değişik boyut ve fonksiyonda olabilmektedir.

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

RFID etiketleri fonksiyonları bakımından
- Pasif etiketler
- Aktif etiketler
- Yarı pasif etiketler

olarak sınıflandırılırlar.



Şekil 2.1 RFID etiket yapısı

Pasif Etiketler

Günümüzde mevcut üretilen pasif etiketler 2 Kbit hafızaya sahiptir. Bu bellek, sıradan tanımlama bilgileri dışında, daha karmaşık bilgileri tutmak için çok küçüktür. Halen bellek miktarını daha da büyütebilmek için çalışmalar yapılmaktadır.

Pasif bir etiket okuyucu sinyaller yaymaktadır. Pasif bir etiket, bu alıcının okuma mesafesi içerisinde ise etiketin anteni yayılan bu elektromanyetik sinyalden etkilenerek uyarılır. Gelen sinyaldeki enerji anten tarafından kart üzerindeki kondansatöre aktarılarak indüklenir. Bu kapasitör, yeterli miktarda enerji depoladığında elektronik devreyi çalıştırarak modüle edilmiş sinyali yayar. Etiketin belleğine bulunan bu bilgiyi oluşturan bu sinyal okuyucu tarafından alınır ve böylece pasif etiket ile okuyucu arasındaki iletişim tamamlanır.

Okuyucu ve pasif etiket arasında yapılan bu haberleşmede kimlik bilgisini module etmenin iki yolu vardır. Düşük frekans kullanan pasif etiketlerde (100 MHz den küçük) kondansatör üzerinde tutulan enerji değişen şiddetlerle kart üzerindeki bobine aktarılır.

Bu olay etiket tarafından emilen radyo frekansını etkiler. Okuyucu, yayılan bu değişik sinyalleri algılar ve kodu demodüle etmek için bu değişken sinyalleri kullanır. Yüksek frekans kullanan pasif etiketlerde (100MHz'den yüksek frekanslar) ise etiket gerisaçınım ile sinyali gönderir. Bu olay etiketin anteninin direncini değiştirir. Rezistanstaki bu değişim okuyucunun alabileceği ve demodüle edebileceği bir RF yayılmasına neden olur.

RFID etiketleri birçok malzemeden kaplanabilir. Pasif etiketler aktif etiketlere göre oldukça ucuzdur. Az miktarda üretildiği zaman yaklaşık 20-25 cent gibi bir maliyeti vardır. Fakat perakende ve marketçilik sektöründe tedarik zinciri yönetiminde, envanter kontrolünde ve bu gibi oldukça geniş bir ürün yelpazesini kapsayan uygulamalarda kullanıldığında daha çok üretim olacağı ve maliyetin 5 cent 'in altına kadar düşeceği, yapılan Ar-ge çalışmaları sonucunda tespit edilmiştir.

Bu yüzden etiketlerin teknik yanına değinirken daha çok pasif etiketlerin çalışma prensibi üzerinde durulacaktır. Pasif etiketlerin, düşük maliyetinin yanında küçük boyutlara sahip olması da önemli bir avantajdır.

Günümüzde 0,4mm x 0,4mm boyutunda ve kağıttan ince pasif RFID etiketleri üretilebilmektedir. Etiketin boyutunu büyüttükçe anten boyu da büyüyecektir. Böylece alıcı ile arasındaki mesafenin daha uzun olması sağlanacaktır. Fakat yaydığı sinyalin aktif etiketin yaydığı sinyal kadar güçlü olmaması sebebi ile okuyucu ile etiket arasındaki mesafe 10mm ile 5 m arasında kalmaktadır. Pasif etiketler genellikle 128 KHz, 13,6 MHz, 915 MHz veya 2,45 GHz' de çalışır.

Plastik RFID için en yaygın olarak kullanılan malzemedir. Plastik kaplanmış bu RFID kartların birçoğunu kimlik kartları, bina giriş kartları ve kredi kartları gibi kartlar oluşturmaktadır.

Aktif Etiketler

Aktif denilmesinin sebebi, sahip oldukları kimlik bilgilerinin iletimi için gereken gücü kendi kartı üzerinde bulunan pilden sağlamalarıdır. Aktif elektronik etiketler güçlü sinyaller yaymaktadır ve okuyucu bu sinyalleri çok uzaktan bile okuyabilir. Fakat üzerinde bulunan güç kaynağı, etiketin daha geniş ve pahalı olmasına neden olmaktadır. Bu yüzden aktif etiketler sadece bilginin iletimi için uzun mesafeler gerektiğinde kullanılır.

Elektronik kartları üzerinde kendi güç kaynaklarını bulundurduklarından yüksek frekanslarda çalışırlar. Genellikler çalıştıkları frekanslar 455 MHz, 2,45 GHz veya 5,8 GHz dir. Hangi frekansta çalışmaları gerektiği, mesafeye ve gerekli hafızaya göre değişmektedir. Aktif RFID okuyucuları 20-100 metreye kadar aktif etiketlerle iletişim kurabilir.

Yarı Pasif Etiketler

Yarı-pasif etiketler güç kaynağı içerirler. Üzerlerinde yer alan pil sadece mikro yonganın devrelerine güç sağlamaktadır. Haberleşme pasif etiketlerde olduğu gibi okuyucudan gelen sinyallerle aktif olan etiketle sağlanır. Söz konusu etiketler sıcaklık ve hareket bilgisi gibi algılayıcı (sensör) giriş bilgilerini depolamak için kullanılırlar. Yarı pasif etiketlerin haberleşme mesafeleri büyük olup güvenilirdirler. Üzerlerinde yer alan güç kaynağı dolayısı ile okuyucuya daha hızlı cevap verebilmektedirler. Tablo 2.1'de yukarıda anlatılan RFID etiketlerinin karşılaştırma tablosu yer almaktadır.

Tablo 2.1 RFID Sistemlerde Farklı Etiketlerin Karşılaştırılması

Etiket	Aktif	Pasif	Yarı-pasif
Güç kaynağı	Pil	Okuyucudan yayılan elektromanyetik dalgalarla oluşan indüksiyon	Pil ve indüksiyon
Okuma mesafesi	30 kadar	3 metre	30 metre kadar
Yakınlık bilgisi	Zayıf	İyi	Zayıf
Frekans çatışması	Yüksek	Orta	Yüksek
Depolanan bilgi miktarı	34k veya daha fazla (okuma/yazma)	2K (sadece okuma)	32k veya daha fazla (okuma/yazma)
Maliyet / Etiket	2$ - 100$	25cent	-

2.3.2. Hafıza tiplerine göre RFID etiket türleri

RFID etiketleri depoladıkları bilgiler açısından
- Sadece okunabilen
- Okunabilen/Yazılabilen
- Okunabilen/Yazılabilen/Yeniden yazılabilen

olarak sınıflandırılırlar.

Sadece okunabilen etiketler

Sadece okunabilen etiketler, genellikle pasif RFID etiketleridir. Bilgi depolama kapasiteleri küçüktür. Üretim sırasında üzerlerine yazılan bilgiyi saklarlar ve bu bilgi değiştirilemez. Bu nedenle uygulamalarda tanıtıcı etiket olarak kullanılmaktadırlar.

Sadece okunabilen etiketlerin kullanıldığı sistemlerde merkezi bilgisayar sistemi ve veritabanı radyo frekans tanımlama sisteminde kullanılan nesnelerle ilgili tüm işlemlerin kontrolünü gerçekleştirir.

Okunabilen/Yazılabilen etiketler

Okunabilen/Yazılabilen etiketler, bilgi depolama kapasiteleri yüksek etiketlerdir. Yazılabilme özelliği olan bu etiketlere okuyucu kapsama alanındayken yeni bilgiler eklenebilir ya da etiket üzerinde var olan bilgiler değiştirilebilir. Bu özellikleri dolayısı ile hareketli veri tabanı gibi davranabilirler. Maliyetleri sadece okunabilen etiketlere göre yüksektir.

Okunabilen/Yazılabilen/Yeniden yazılabilen etiketler

Okunabilen/Yazılabilen/Yeniden yazılabilen etiketler üzerindeki bilgilerin değiştirilebilme özelliği ve yüksek depolama kabiliyetleri dolayısıyla geniş uygulama alanına sahiptirler. Haberleşme açısından cevap verme süreleri kısadır. Maliyetleri diğer etiketlere göre fazladır.

2.3.3. RFID okuyucu (Reader)

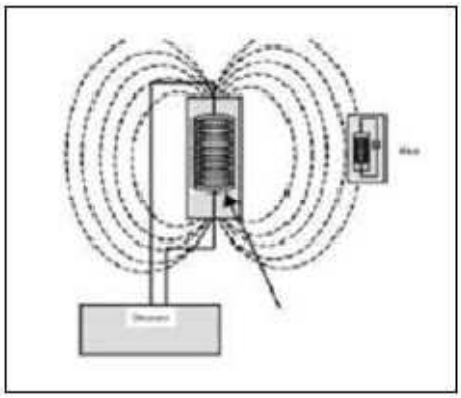
Etiketlere ulaşıp veri alışverişi sağlamak ve gelen veriyi işlemek için kullanılırlar. Bazı tipleri sadece okuma yapabilirken bazılar etiketler üzerinde yazma işlemi de gerçekleştirebilirler. RFID yazılımının bulunduğu bilgisayarlar ile iletişimi de yine okuyucular gerçekleştirir [2].

Okuyucunun görevleri:

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

2.3.4. RFID okuyucu çalışma prensibi

Okuyucu etiketle haberleşebilmek için gerekli enerjiyi, radyo frekans kimlik tanıma sisteminin çalışma frekansına bağlı olarak seçilen çalışma frekansında zamanla değişen manyetik alan yaratarak sağlamaktadır. (Şekil 2.2)



Şekil 2.2 RFID Okuyucu Çalışma Prensibi

Okuyucu ürettiği, zamanla değişen manyetik alanı genellikle çerçeve anten vasıtasıyla etikete gönderir. Okuyucunun dairesel çerçeve anteninden akım aktığında çerçeve antene dik düzlemde oluşan manyetik alan şiddeti olarak hesaplanmaktadır.

$$H = \frac{I\,NR^2}{2(R^2 + x^2)^{3/2}} \qquad (2.1)$$

Burada;

I = Çerçeve antenden akan akım

N = Çerçeve anten sarım sayısı

R = Anten yarıçapı

x = Anten düzlemine dik doğrultudaki alıcı uzaklığını tanımlar.

Bu bağıntıdan da 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. Taşıyıcı sinyal etikete enerji sağlamasının yanı sıra, etiketteki bilgilerin okuyucuya gönderilmesini ve haberleşmenin senkronizasyonunu sağlar. Etiket okuyucu tarafından gönderilen sinyali alır ve module 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.

2.3.5. Okuyucunun tasarım ve performansı

Okuyucu aynı zamanda alıcı-verici olduğundan alıcı ve verici kısımlarını içermektedir. Verici 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 [3].

Bağıntıya göre anten yarıçapı artırıldığında manyetik alan şiddeti de artmaktadır. Diğer taraftan *NI* da artırıldığında *H* değeri de 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.

2.4. RFID Çalışma Frekansları

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 [4]. RFID sistemleri kısa mesafe uygulamaları için Düşük Frekans (LF) 120-135kHz; akıllı kart ve etiket uygulamaları için Yüksek Frekans (HF) 13.56MHz; aktif düşük güçlü etiketler uygulamaları için Ultra Yüksek Frekans (UHF) 433MHz ve tedarik zinciri uygulamaları için Ultra Yüksek Frekans (UHF) 860-960 MHz ve aktif etiketlerle daha büyük haberleşme mesafeleri ve daha yüksek hızlarda veri iletimi için Süper Yüksek Frekans (SHF) 2450MHz frekans bandlarını kullanmaktadır. (Tablo 2.2)

Tablo 2.2 RFID 'de kullanılan frekanslar ve okuma mesafeleri

Frekans	Açıklama	Okuma Uzaklığı (m)	Veri Okuma Hızı
125 – 134 kHz	LF	0.45	1- 10
13.56 MHz	HF	< 1	10 – 40
868 – 870 902 – 928 MHz	UHF	2 – 5	10 – 50

Avrupa Posta ve Telekomünikasyon Birliği RFID haberleşmesi için Avrupa Standardı olarak Eylül 2004 de ETSI EN 302 208 standardının uygulanmasına karar vermiştir. ETSI EN 302 208 standardı 865–868 MHz frekans bandını kullanan 3 MHz band genişliğine sahip Söylemeden Dinle (LBT) protokolü ile 2W eşdeğer izotropik radyasyon güç seviyelerinde haberleşmeyi öngörmektedir [5]. 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;

Belirli hizmet için kesin olarak tanımlanamayan kısa mesafe erişimli telsiz cihazları Madde 6

Sayısal veya analog her türlü ses ve veri iletimini sağlayan, öncelikle uzaktan kumanda, uzaktan ölçüm, alarm, oyuncak telsiz ve araçları ile video kamera, eş

zamanlı tercüme uygulamalarından oluşan bu cihazlar, belirtilen kriterlere uygun olmak kaydıyla kullanılır [6].

2.5. RFID'nin Genel Özellikleri

RFID'nin genel özellikleri aşağıdaki şekilde sıralanabilir:

2.5.1. Okuma kapasitesi

RFID uygulamalarında barkodda olduğu gibi etiketin ancak görülebilir bir pozisyondayken okunması gerekmemektedir. Bunun nedeni radyo frekans teknolojisinde sinyallerin maddeler arasından geçebilme özelliğidir. Bu yetenek, içinde birçok kutulanmış ürün bulunan taşıyıcı paletlerin kullanıldığı depolarda gerçekleştirilecek otomasyon uygulamalarında büyük avantaj sağlamaktadır. Radyo frekans teknolojisi ile okuma yapılırken, paletlerin açılıp içindeki kutuların her birinin okutulması zorunluluğu ortadan kalkmaktadır.

Bununla birlikte nesnelerin belli bir düzen içinde dizilmediği ortamlarda yapılacak uygulamalarda da önem taşımaktadır. Havaalanı bagaj takibi, postane paket düzenleme bu uygulamalardan bazılarıdır. Birden fazla RF etiketin bulunduğu ortamlarda bir okuyucunun tüm etiketleri okuyabilmesi de çok önemli bir diğer özelliktir. Bu özelliğe ek olarak okuyucular birçok etiketin arasından yalnız belirlenmiş olan etiketi okuma yeteneğine de sahiptir. Kutuların birbirine çok yakın olarak yerleştirildiği raflardaki ürünlerin seçilebilmesinde bu yetenek büyük avantaj sağlamaktadır [7].

2.5.2. Okuma sürati

RF etiketler barkoda göre çok daha yüksek hızda okunabilmektedir. RF okuyucular saniyede 50 etiket ve daha fazlasını okuyabilecek kapasiteye sahipken barkod tarayıcılar her defasında ancak bir barkod okuyabilmektedir. RF teknolojisinin bu özelliği çok sayıda nesnenin hızlı bir şekilde takibinin gerektiği uygulamalarda çok büyük avantaj sağlamaktadır. Buna bağlı olarak bilgi toplanması sürecinde zaman

kaybı ve çalışan masrafları minimuma indirilebilmektedir. Bu durumda çalışanlar ürün takip anlamında daha efektif katma değer sağlayabilmektedir.

BÖLÜM 3. AKILLI KARTLAR

Akıllı kartlar yeni bir teknoloji değildir. 1974'de Fransız gazeteci Roland Moréno'nun akıllı kartı bulduğu kabul edilir. Bununla beraber, Almanya'dan Jargen Dethloff ve Japonya'daki Arimura Technology Institute'den Kunitaka Arimura, sırasıyla Şubat 1969 ve Mart 1970'de ilk patentleri aldılar. Moreno'nun dünya çapındaki patentleri banka tipi bir plastik kart içine bir mikrokontrolör gömme kavramını kapsıyordu. Kart endüstrisindeki firmaların onun kavramlarını desteklemeleri sürpriz olmadı. Bu durum Fransa'da hükümet, mali çevreler, toplu taşıma, tıp ve haberleşme sektörleri içinde tartışma başlattı ve böylece teknolojik deneyler başlamış oldu. Yapılan deneyler sonucunda akıllı kartların sahtekârlığı önleme potansiyeli de vardır hükmüne varıldı ve bu hüküm bu güne kadar doğrulanmıştır [8].

Akıllı kartlar, kredi kartı boyutlarında içerisinde işlemci, RAM ve ROM belleği bulunan gömülü bir mikroçipe sahip donanımlardır. Üzerinde manyetik şerit, barkod, temassız radyo frekans vericileri gibi farklı teknolojilerini bulundurabilir. Günümüzde giriş kontrolü, elektronik ticaret, kimlik doğrulama, kişisel gizlilik gerektiren bir çok uygulamada çok yaygın olarak kullanılmaya başlanmıştır. Bununla birlikte X.509 sertifikalarını ve bunlarla bağlı olan anahtarları taşımak için kullanılan en yaygın ve güvenli cihazlar akıllı kartlardır. Bu bölümde, akıllı kartların sınıflandırılması, akıllı çubuklar, akıllı kart okuyucular, donanım güvenlik modülü (HSM), açık anahtar altyapısında akıllı kartın önemi, akıllı kartlara erişim yöntemleri hakkında bilgi verilecektir.

3.1. Akıllı Kartların Sınıflandırılması

Akıllı kartlar elektronik devre yapılarına, veri aktarım tipine ve boyutlarına gore sınıflandırılabilirler. Akıllı kartlar veri tipine göre aşağıdaki gibi sınıflandırılabilirler [9].

Bellek kartları

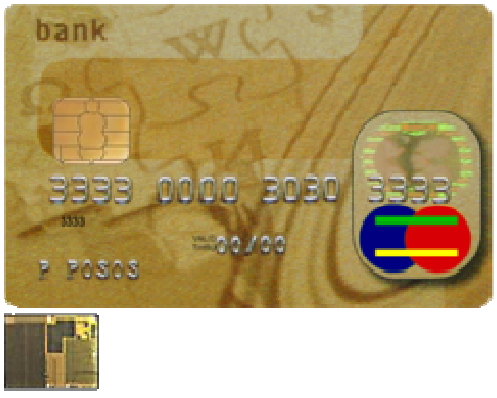
- Güvenlik donanımlı
- Güvenlik donanımı olmayan

İşlemcili Kartlar

- Kripto işlemcili
- Kripto işlemcili olmayan

Akıllı kartların genel özellileri aşağıdaki gibi sıralanabilir:

- Boyutları normal kredi kartları boyundadır. ISO 7810 standardı bu ölçüleri 85.60 mm X 53.98 mm olarak belirlemiştir. Bir diğer ölçü de SIM kart olarak bilinen 25 X 15 mm ölçüleridir.
- Kurcalamalara karşı dirençli güvenlik sistemine sahiptirler.
- Kart okuyucular ile kart içindeki veriler yönetim sistemine aktarılarak işlem yapılır.



Şekil 3.1 Bir akıllı kart uygulaması görseli ve chip görünümü

Şekil 3.1’de bir akıllı kartın ticari uygulaması görseli ve üzerindeki chipin görünümü gösterilmektedir.

Akıllı kartlar üzerinde bulunan mikroçipe gore “temaslı” ve “temassız” olmak üzere iki ana sınıfa ayrılır. Bazı kartlar temaslı ve temassız ara yüzleri üzerinde iki ayrı mikroçip olarak sunabilir. Bu tür kartlara hibrid kart adı verilir. Bu özelliğin aynı mikroçip üzerinde birleştirildiği kart tipine ise dual kart adı verilir.
Temassız kartlar RFID teknolojisi ile elektro manyetik olarak haberleşebilirler. Radyo frekansı ile haberleşmede kullanılan bağlanıtı hızı 106 kbps ila 848 kbps aralığındadır. Temassız kartlar, işlem yapabilmek için sadece bir temassız kart okuyucu antenine yaklaştırmak yeterlidir. Genellikle temassız kartlarla işlem yapmak çok hızlı veya hands-free yani sadece kartı göstermek yeterli olacak şekilde basittir. Bu yüzden özellikle toplu taşıma için uygun birer çözümdürler.

Temassız akıllı kartlar ISO 14443 ile standartlaştırılmıştır. Bu standart iki tip temassız kart tanımlamaktadır. A ve B tipi temassız kartlar. Daha önceden ISO 14443 C, D, E, F ve G tipi kartlar da tanımlamıştı. Ancak bunlar daha sonradan ISO tarafından iptal edildiler. ISO 14443 standardı haberleşmenin 10 cm’e kadar yapılmasını önermiştir. Temassız akıllı kartlar için bir diğer standart olan ISO 15963 haberleşmeyi 50 cm’e kadar mümkün kılacak şekilde belirlemiştir.

Temassız akıllı kart teknolojisi RFID teknolojisi ile yakından ilişkilidir. Elektronik ücret toplama gibi uygulamalarda bir biri yerine kullanılabilmektedirler. Ancak RFID cihazlar genellikle yazılabilir bir hafızaya sahip değilllerdir. Ayrıca temassız akıllı kartların yapabildiği şekilde işlem yapacak mikrodenetleyicilere de sahip değildirler. Akıllı kartların haberleşme protokolleri Tablo3.1’deki gibi belirlenmiştir.

Tablo 3.1 Akıllı kart haberleşme protokolleri

Protokol	**Açıklama**
T = 0	Karakter temelli haberleşme. ISO 7816 – 3 de tanımlanmıştır.
T = 1	Blok temlli haberleşme. ISO 7816 – 3’te tanımlanmıştır.
ISO/IEC 14443	Temassız ara birimden APDU gönderimi, ISO/IEC 14443’te tanımlanmıştır.

Temaslı akıllı kart kullanımı sırasında kartın kart okuyucuya takılması gerekmektedir. Böylece kart yüzeyi üzerindeki iletken bölge ile doğrudan bağlantı

kurulabilir. Temassız akıllı kartlar bir işlem gerçekleştirebilmeleri için bir anten yanından geçirilirler. Bunlarda plastik kredi kartı görünümündedirler. Onlardan tek farkı içlerinde bir mikroçip ve bir de anten gömülü olmasıdır. Bu bileşenler fiziksel bir temas gerektirmeden, kartın anten ile bağlantı elemanı arasında iletişim kurmasını sağlar. İşlemlerin çok hızlı yapılmasının gerekli olduğu toplu taşımacılıkta ve jetonla çalışan sistemlerde temassız akıllı kartların kullanımı ideal bir çözümdür. Temassız akıllı kartlarda okuyucu ve kart arasındaki mesafe ise 10 cm'yi geçmemelidir. Açık anahtar altyapısı ve e-imza sistemlerinde kullanılabilecek akıllı kartlar kripto işlemcili sınıfta yer alırlar. Bu akıllı kartlar, programlanabilir alanları olan, dayanıklı, taşınabilir bilgisayarlar olarak tanımlanabilir. Akıllı kartlar veri güvenliği, kimlik gizliliği ve mobil kullanıcı ihtiyaçlarına sahip sistemlerde faydalıdır. Bu kartların başlıca teknik özellikleri şöyle sıralanabilir [10]:

- Mikroişlemcili olarak gerçeklenmiştir. (8, 16 ve 32 bit modeller vardır)
- Bir işletim sistemine sahiptir. (AKIS, CardOS, Multos vb)
- RSA, DSA, ECDSA gibi asimetrik algoritmaları çalıştırabilen yardımcı kripto işlemcisine sahiptir.
- İşletim sistemi ve kripto kütüphanesi mikroişlemcinin ROM belleğinde saklanır.
- Kripto anahtarlarını ve sertifikaları saklamak için yeterli büyüklükte EEPROM belleğe sahiptir. (Tercihen 8Kb ve üstü)
- Özel anahtarlar kart içine yerleştirildikten sonra asla dışarı çıkarılamaz.
- Kart içindeki özel anahtarla işlem yapmak için karta PIN kodu girilmesi zorunludur.

Yukarıdaki özelliklere sahip bir akıllı kart aşağıdaki hizmetleri sunar.

- Kart üzerinde şifreleme ve şifre çözme
- Kart üzerinde imzalama ve imza onaylama
- Kart üzerinde özel ve açık anahtarların tutulması
- Kart içine bilgi yazabilme
- Kartın şifre ile korunması

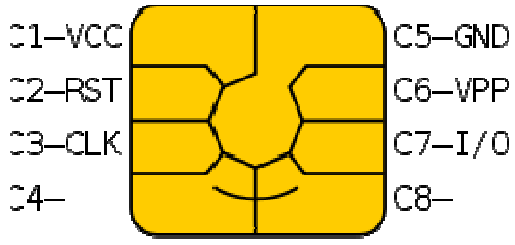
Akıllı kartların özel (private) ve açık (public) alanları vardır. Özel alanda anahtar üretimi, imzalama, şifre çözme gibi işlemler yapılır, bu alana dışarıdan erişim yasaklanmıştır. Açık alana genel bilgiler yazılır. Akıllı kart yönetim yazılımı yardımıyla buradaki bilgiler görülebilir. Akıllı kartın boyutları uluslararası ISO-7810 standardına göre belirlenir. ISO-7816 standardı ise ısı menzili, esneklik, elektriksel temasın pozisyonu ve mikroçipin dış dünya ile nasıl bağlantı kuracağı gibi özellikleri kapsayan, kartın fiziksel karakteristiğini de belirler.

Temaslı akıllı kartlar bir okuyucu için bir temas alanı sağlarlar. Bu yaklaşıl 1 cm^2 boyutlarında altın kaplı bir yüzeydir. Kart okuyucuya takıldığında okuyucunun uçları bu bölgeler ile temas ederek veri alışverişini mümkün kılar.

ISO 7816 ve ISO 7810 bu temas alanını standartlaştırmıştır. Buna gore
- Fiziksel şekli
- Elektriksel bağlantıların şekil ve yerleri
- Elektriksel karakteristikleri
- Karta gönderilen ve karttan alınan komutların haberleşme protokolleri
- Kartın dayanıklılığı
- Fonksiyonelliği

standartlarda belirlenmiştir.

Şekil 3.2'de bir akıllı kartın temas alanı görülmektedir.



Şekil 3.2 Akıllı kartın temas alanı

Elektrik sinyallerinin tanımları aşağıdaki gibidir:

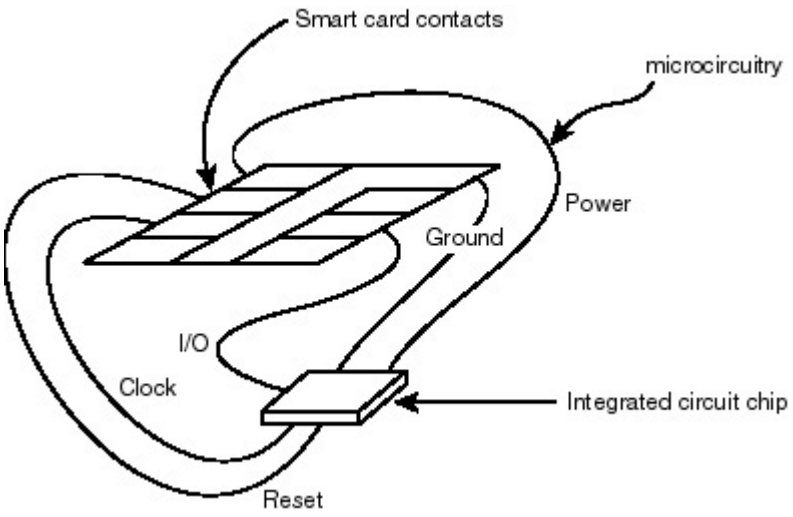
VCC: Güçsağlama girişi

RST: İşlemciyi ilklendirme komut bacağı
CLK: Zamanlama sinyal girişi
GND: Referans gerilimi
VPP: Programlama gerilim girişi
I/O: Karta gönderilen veya karttan okunan verinin seri olarak iletildiği giriş

3.2. Akıllı Kartların Yapısı

Akıllı kartlar kredi kartı büyüklüğünde ve üzerinde microchip bulunduran küçük plastik kartlardır. Manyetik kartlardan çok daha güvenli ve hatırı sayılır derecede daha fazla hafızaya sahiptir. İki temel tip akıllı kart vardır. Temaslı ve Temassız akıllı kartlar.

Temaslı kartlar üzerinde bir santimetre çapında üzeri altın plaka ile kaplı kontaklara sahiptir. Bu kontakların 8 ucu vardır. Bu plakalar alt tarafından kartın mikrochip'ine elektriksel olarak bağlıdır. (Şekil 3.3) Bu microchip bir memory chip veya bir hafıza ve CPU'ya sahip bir mikroprosesör olabilir.



Şekil 3.3 Akıllı kart bağlantısı

Hafıza kartları daha çok telefonlarda kullanıldığı gibi mikroişlemcili kartlar ise aynı kart üzerinde çeşitli uygulamalar için kullanılır. Her iki tip kartta veri saklama

alanlarına sahip olduğu gibi mikroişlemcili kartlar ilaveten sahip olduğu işlemci (CPU) ile ve ROM'unda saklı olan işletim sistemi ile işlem yapabilir.

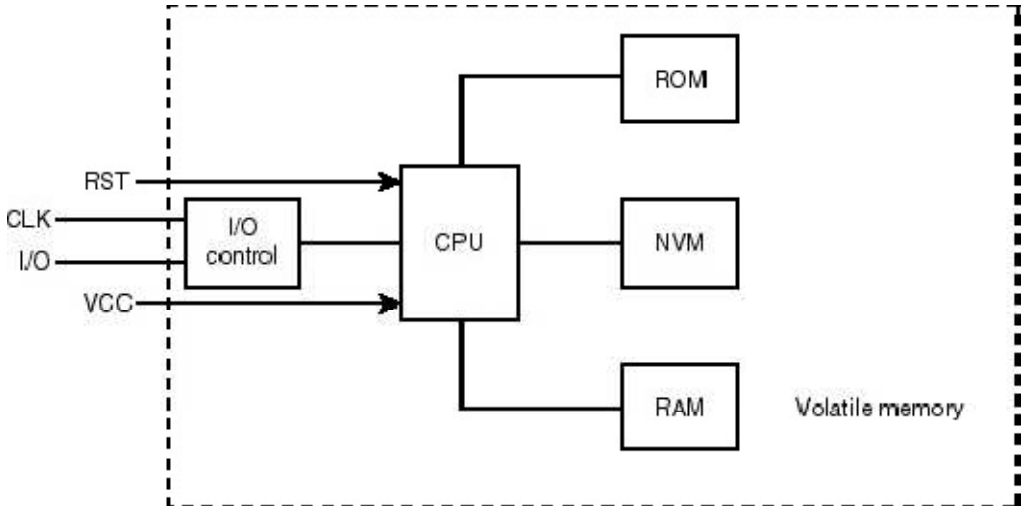
Temassız kartlar bir mikroişlemci bulundururlar. Ayrıca bir de radyo sinyallerini alabilecek bir anten tertibatına sahiptirler. Temassız akıllı kartlar sadece bir temassız kart okuyucuya yaklaştırıldığında çalışırlar. Temassız kartlar daha maliyetli olmakla beraber ulaşım ve erişim kontrolü uygulamaları için en iyi çözümdür.

Manyetik kartlar herhangi bir işlem yapabilme kabiliyetine sahip değillerdir. Ayrıca hafıza kapasiteleri de 100 byte civarındadır. Akıllı kartların sağladığı güvenlik seviyesine göre sağladıkları güvenlik seviyesi çok düşüktür. Ancak daha ucuzdurlar. Fakat manyetik kart okuyucuların üretim maliyeti akıllı kart okuyucuların üretim maliyetinin yaklaşık 10 katıdır.

Hibrid kartlar temaslı, temassız ve manyetik kartların birleşimidir. Bazı hybrid kartlar üzerinde mikroişlemci, manyetik şerit, barcode, optic kod, resim ve imza paneli bulundurular.

3.3. Akıllı Kart Donanımı

Bir akıllı kart üzerindeki bilgisayar, işlemci, hafıza, ve giriş çıkış birimleri olan tek bir yongadır. Şekil 3.4'de bir akıllı kart sisteminin genel görünüşü gösterilmektedir.



Şekil 3.4 Akıllı kart bilgisayar sistemi

3.3.1. Hafıza sistemi

Akıllı kart normal bilgisayar yazılımcılarına yabancı gelmeyen bir hafıza yapısına sahiptir. Akıllı kart üzerinde üç çeşit hafıza bulunmaktadır.

- ROM, Sadece okunabilir hafıza
- NVM, Non-Volatile, Sabit, kalıcı hafıza
- RAM, Rasgele erişimli hafıza

Akıllı kartın işletim sistemi ROM üzerinde bulunur. Bu alanda genel kullanım için çeşitli rutinler, şifreleme rutinleri ve özel amaçlı artimetik rutinler bulunur. ROM'daki kod ve veriler kartın üretimi sırasında bu alana yerleştirilirler. Bu alana yazılan kod ve veriler donanımsal olarak gerçekleştirilir. Bir daha silinip değiştirilemezler.

Kart üzerindeki bakiye, puan ve çeşitli uygulamaların kullandıkları değerli bilgiler NVM hafızasında tutulmaktadır. NVM hafıza bölgesi kart üzerindeki uygulamalar tarafından okuma ve yazma için kullanılabilir. Ancak RAM gibi kullanılmazlar. Kart üzerinde saklanması istenen bilgiler tutulurlar. RAM'den farklı olarak okuma ve yazma performansı düşüktür. Kart enerjisiz kaldığında da bu alanda tutulan veriler bozulmazlar.

Akıllı kartlar üzerinde bir miktar da RAM hafıza vardır. Programcı gözüyle çok kısıtlı bir kaynak olduğu için kart üzerindeki en değerli kaynaklardan biridir. Geliştiriciler yüksek seviyeli dil ile uygulama geliştiriyorlarsa geçici değişkenlerini kullanırken oldukça iyi optimizasyon yapmaları gerekmektedir. Ayrıca RAM hafıza bölgesi sadece programcıların geliştirdiği uygulamalar tarafından değil çağırılan tüm rutinler tarafından da kullanılmaktadır.

3.3.2. Merkezi işlem birimi, CPU

Akıllı kartlarda merkezi işlem birimi olarak kullanılan önceki 8 bitlik mikroişlemciler genellikle Motorola 6805 ve Intel 8051 işlem setlerini

kullanmaktaydılar. Bu işlem setleri hafıza ve yazmaç işlemleri, adresleme modları ve giriş çıkış işlemleri için uygundular. İşlemciler saniyede 400,000 işlem yapabilme (400 KIP) gücüne sahiptiler. Yeni üretilen akıllı kartları işlemcileri saniyede 1,000,000 işleme (1 MIP) kadar güçlenmişlerdir. Akıllı kartlarda daha kuvvetli şifreleme ihtiyacı yeni kartlar ile daha makul süreler içinde gerçekleşmesi mümkün olmaktadır. Tipik olarak bir işlemin akıllı kart üzerinde 2, 3 saniyede gerçekleştirilmesi gerekiyor. Ancak 1024 bitlik bir RSA şifreleme işleminin tipik bir akıllı kart üzerinde yapılması neredeyse 10 – 20 saniye almaktadır. Bu yüzden akıllı kartlar için zorlayıcı şifreleme işlemlerini yapacak yardımcı işlemciler geliştirilmiştir.

20 yıldan beri süren geliştirmelerle akıllı kart teknolojisi hızla gelişmiştir. Örneğin hafıza kapasiteleri artarken işlemci mimarileri de 8 bitten 16 bit ve 32 bite evrilmiştir.

3.3.3. Akıllı kart giriş çıkış birimi

Bir akıllı kart üzerindeki giriş çıkış birimi tek yönlü bir seri haberleşme kanalıdır. Akıllı kart donanımı 115200 bps hızındaki haberleşmeyi destekleyebilir. Ancak çoğu akıllı kart okuyucuları tipik olarak bu hızdan daha düşük hızlarda akıllı kartlar ile haberleşirler.

Akıllı kart okuyucusu ile akıllı kart arasındaki haberleşme tipi master-slave tipindedir. Host karta bir komut gönderir ve cevabını bekler. Akıllı kart hostun gönderdiği bir sorguya cevap haricinde hosta hiç bir veri göndermez. Tüm haberleşme soru – cevap şeklinde gerçekleşir.

3.4. Akıllı Kart Yazılımı

Temel olarak iki tip akıllı kart yazılımı vardır. Biri, bir PC üzerinde çalışan ve akıllı kart ile okuyucu vasıtası ile haberleşen host uygulamasıdır. Host yazılımına ayrıca okuyucu-taraflı yazılım denmektetir. Diğeri kart yazılımıdır. Bu yazılım kart üzerinde koşar. Bu yazılıma da kart-tarafı yazılım ismi verilmektedir.

Akıllı kart yazılımlarının çoğu okuyucu-tarafı yazılımlarıdır. PC'ler gömülü sistemler için geliştirilen okuyucu-tarafı yazılımlar akıllı kartlar ile sistemleri birleştirirler. Okuyucu-tarafı yazılımlar genelde son kullanıcı yazılımlarıdır. Sistem seviyesinde kart yazılımına erişimleri sağlayarak kartların kullanılmasını sağlarlar.

Okuyucu tarafı yazılımlar C, C++, Java, C# gibi yüksek seviyeli diller kullanılarak yazılırlar.

Kart tarafı yazılımlar genelde işletim sistemi, utilty ve uygulama yazılımı olarak sınıflandırılır. Kart uygulamaları genellikle mevcut kartların özelleştirilerek diğer büyük sistemlere servis sağlaması ve entegre olması için geliştirilir. Kart sistem yazılımları düşük seviye diller kullanılarak geliştirilirler.

Okuyucu tarafı ve kart tarafı yazılımların temel olarak farklı hedef ve görevleri vardır. Kart yazılımları kartın içeriğine odaklanmıştır. Kart yazılımları kart içeriğine erişmek isteyen uygulamalar için işlemsel hizmet veridikleri gibi üzerinde bulundurdukları değerli verilerin yetkisiz uygulamalar tarafından erişilmesini engellecek işlemler yaparlar. Diğer taraftan okuyucu tarafı yazılımlar birden fazla çeşit kart ile çalışabilirler.

Kart yazılımları kart üzerindeki güvenlik işlemlerini yerine getirir. Örneğin bir kart yazılımı kartın üzerinde tutulan hesap numarası bilgisini, doğru kullanıcının PIN kodunu girmeden dışarı vermesini engeller. Veya bir kart yazılımı kendi üzerindeki Private Key'i kullanarak bir dijital imzanın üretilmesi işlemleri yapar ve bu Private Key kesinlikle kart dışına çıkartılamaz. Kart üzerinde çalışan uygulama kartın özel verilerine erişimi denetler.

3.5. Akıllı Kart Standartları

Temel temaslı akıllı kart standartları ISO 7816 1 – 10 ile belirlenmiştir. Temassız akıllı kartların standardı ise ISO 14443'tür. Bu standartlar kart standartların tanımlanması, fiziksel detayları, elektriksel ve mekanik özellikleri ve uygulama

programlama arayüzü gibi özellikleri tanımlar. Aşağıdaki listede temaslı akıllı kartların standartları gösterilmiştir.

- ISO 7816 – 1 (1987) : Fiziksel karakteristikler
- ISO 7816 – 2 (1988) : Kontakların boyutları ve konumları
- ISO 7816 – 3 (1989) : Elektronik sinyaller ve iletişim protokolleri
- ISO 7816 – 4 (1995) : Komutlar ve cevaplar
- ISO 7816 – 5 (1994) : Uygulama belirteçleri
- ISO 7816 – 6 (1995) : Veri elemanları
- ISO 7816 – 7 (1998) : Smart Card Query Language komutları
- DIS 7816 – 8: Güvenlik komutları
- CD 7816 – 9 : Genişletilmiş komutlar
- ISO 7816 –10 (1999) : Senkron kartlar

3.6. Akıllı Kart İşletim Sistemi

Akıllı kartların genellikle COS – Card Operating System – veya Mask olarak isimlendirilen Chip İşletim Sistemi kartın ROM hafızasına kalıcı olarak yazılmış olan bir dizi komut setidir. PC'lerdeki DOS veya Windows işletim sistemlerine benzer olarak akıllı kart işletim sistemi de herhangi bir uygulamanın bir parçası veya ona bağımlı değildir. Ancak diğer uygulamalar kart işletim sistemini kullanırlar.

Akıllı kart işletim sistemleri iki sınıfa ayrılırlar:

- Genel amaçlı akıllı kart işletim sistemi. Bir çok uygulama için genel özelliklerde hizmetler sağlar
- Özel amaçlı akıllı kart işletim sistemleri. Özel işlemler için özel hizmetleri ve uygulamaları bulunan kapalı işletim sistemleridir. Örneğin elektronik cüzdan uygulamaları için geliştirilmiş kartlar gibi.

Tüm akıllı kartlarda işletim sistemlerinde bulunan temel fonksiyonlar şunlardır:

- Kart ve dış dünya arasındaki haberleşmeyi yönetmek
- Kart hafızasında tutulan dosya ve verilerin yönetilmesi
- Verilere erişim haklarının denetlenmesi

- Kart güvenliği ve şifreleme algoritmalarının çalıştırılması
- Hata denetimleri
- Veri güvenliği ve doğruluğunun sağlanması
- Kart yaşam döngüsündeki safhaların yönetimi. Üretim, kişiselleştirme, aktif hayat ve kart sonlandırma gibi.

Kart okuyucu terminal ile akıllı kart arasındaki haberleşme biçimi master – slave biçimindedir. Terminal akıllı karta bir komut gönderir. Akıllı kart komutu çözer, ve işletir. Eğer bir geri dönüş bilgisi varsa bunu terminale geri bildirir. Kart terminalden gelecek yeni komutları bekler.

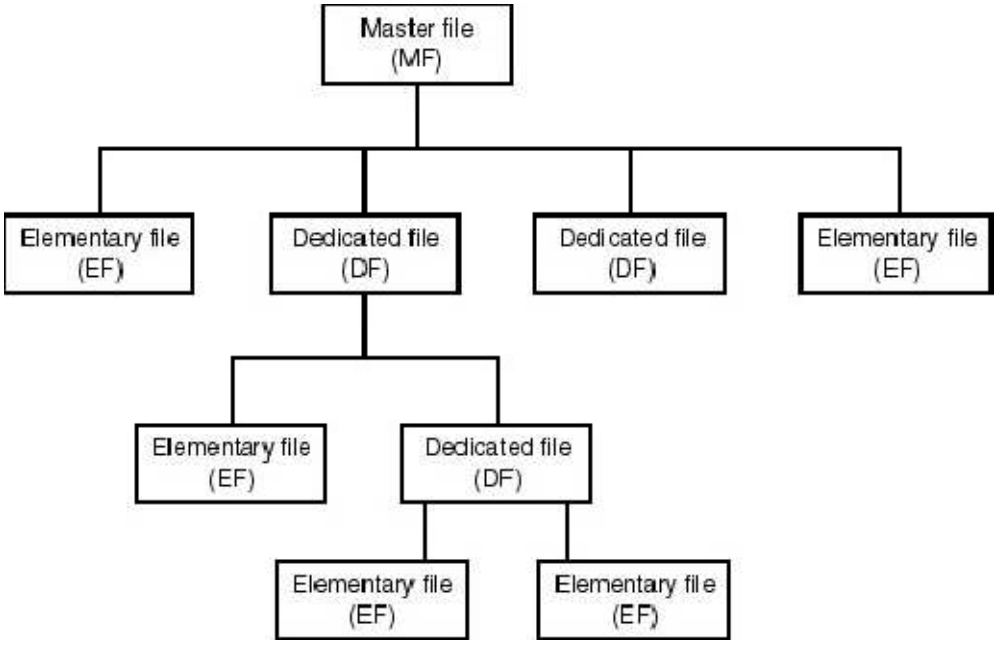
Akıllı karta gönderilecek ve akıllı kart işletim sisteminde yorumlanabilecek komutlar ISO 7816'da belirtilmiştir. Bunlara ilave olarak kart üreticileri kendi özel komut setlerini de ilave etmişlerdir.

Akıllı kart işletim sisteminin ilk zamanlarında kart sahibi olan kurumlar uygulamalarını işletim sistmini özelleştirerek yapıyorlardı. Müşteriye sunmak istedikleri her bir uygulama için yeni tasarımlar ve çalışmalar yapılmak zorunda idi. Bu da akıllı kartların geliştirme açısından esnek olamamasına sebep oluyordu.

Ancak bugün akıllı kart uygulamaları açık işletim sistemi ve çoklu uygulama deskteleme özelliğinden dolayı kolaylıkla geliştirlebilmektedir. Akıllı kart işletim sistemi olarak çoklu uygulama destekli JavaCard OS, Multos gibi kart işletim sistemleri geliştirilmiştir.

3.7. Akıllı Kart Dosya Sistemleri

Bir çok akıllı kart işletim sistemi ISO 7816 standartlarında belirtildiği gibi tutarlı bir dosya sistemi sağlarlar. Akıllı kart dosya sistemleri çok iddialı olayan dosya sistemleridir. Çünkü akıllı kartlar her hangi bir çevre birime sahip değildir. Dosya sistemi sadece akıllı kartın hafızasındaki bir bloktur. Bir akıllı kart dosya sistemi tekil olarak bir köke bağlı klasör yapısında hiyerarşik bir yapıdır.



Şekil 3.5 Bir akıllı kartın dosya sistemi

Şekil 3.5'de bir akıllı kart işletim sistemi dosya yapısı gösterilmektedir. Akıllı kart işletim sistemi dosya oluşturma, okuma, yazma ve silme gibi temel dosya erişim hizmetlerini sağlar. İlaveten işlemler belli çeşit dosya tipleri için yapılabilir. Lineer dosyalar, örneğin sabit uzunlukta kayıtlara sahip olan lineer dosyalara erişim kayıt numarası verilerek veya bir önceki kayıt, bir sonraki kayıt şeklinde erişim yapılabilir. Bazı akıllı kart işletim sistemleri lineer dosyalar üzerinde kısıtlı erişim ve arama işlemleri sağlarlar. Döngüsel dosyalar da aslında birer doğrusal dosyadır. Tek farkı son kayıttan sonra bir sonra erişilen kayıt, dosyanın ilk kaydıdır. Purse dosyalar ise bazı akıllı kart işlerim sistemleri tarafından kullanılan uygulamalara özel dosya türleridir. Bu dosyalar her bir kaydında elektronik cüzdan işlemlerinin tutulduğu bir döngüsel dosyadır. Son olarak da akıllı kart uygulaması tarafından istenildiği gibi kullanılabilen, bir hazfıa bloğu şeklinde olan transparent dosyalardır.

Her bir dosyaya erişim akıllı kart işletim sistemi tarafından bir yetki listesi ile kontrol edilmektedir. Bu erişim listesi ile kart üzerindeki her bir oturum ayrı ayrı denetlenebilir. Örneğin A kişisi bir dosyaya sadece erişip okuyabilirken, B kişisi dosyaya erişip, okuyup yazabilir. Hatta erişim listesindeki yetkileri de değiştirebilir.

3.8 Application Protocol Data Unit (APDU)

Akıllı kart ile haberleşmede kullanılan en küçük komut parçasına APDU denir. APDU komutu uygulama seviyesinde hazırlanıp karta gönderilir. Aynı şekilde karttan alınan cevap da uygulama seviyesinde yorumlanır. Bir APDU, karta gönderilen bir komut ve kartın bu komuta verdiği cevap olarak tanımlanabilir.

ISO – 7816 standartdı iki tip APDU tanımlar. Birincisi Command APDU, kart üzerindeki uygulamaya gönderilen komuttur. Diğeri Response APDU; alınan komuta göre kart uygulamasının cevap olarak gönderdiği komuttur.

Bir APDU şu alanlara sahiptir:
- CLA
- INS
- P1
- P2
- Lc
- Data
- Le

Örnek bir komut Komut APDU'su aşağıdaki gibidir.

CLA	INS	P1	P2	Lc	Data	Le

CLA komutun sınıfını bildirir. Örneğin komut ISO uyumlu mu yoksa komut şifreli haberleşme ile mi yapılıyor gibi nitelikleri gösterir.

INS, kart uygulamasının sağladığı metodu ifade eden belirteçtir.

P1 ve *P2* değerleri parametre değerleridir. INS ile belirtilen metodun istediği parametreler bunlarla gönderilirler.

Lc Komut uzunluğunu ifade eder. Eğer metoda bir veri bloğu gonderilecekse bu verinin uzunluğu Le ile belirtilir.

Data, metoda gönderilecek veri bloğudur. Her zaman gerekli değildir. İsteğe bağlı olarak kullanılır.

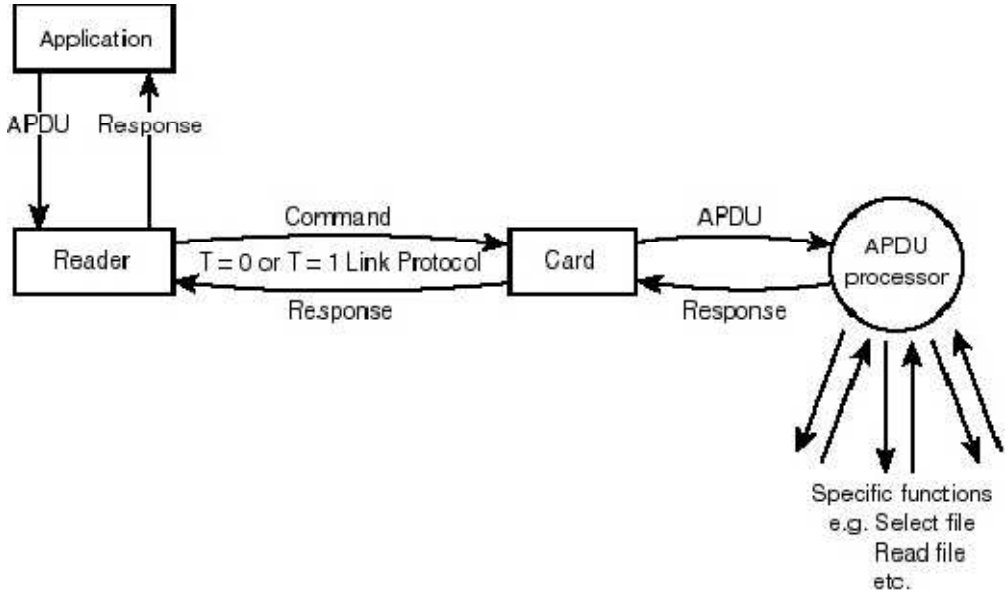
Le, Beklenen veri uzunluğu bilgisidir. Gönderilken APDU'ya karşılık olarak gelecek cevabın uzunluğu belli ise Le ile belirtilebilir. Ancak 0x00 değeri verilerek karttan gelecek tün cevap verisinin alınması da sağlanabilmektedir.

Örnek bir cevap APDU'su aşağıdaki gibidir.

Data	SW1	SW2

Her cevap APDU'sunda;
Kart gönderiyorsa bir Data bloğu vardır.
İki byte uzunluğunda cevap durum değerleri *SW1* ve *SW2* vardır. SW1 ve SW2'nin alabileceği değerler ISO 7816'da tanımlanmıştır.

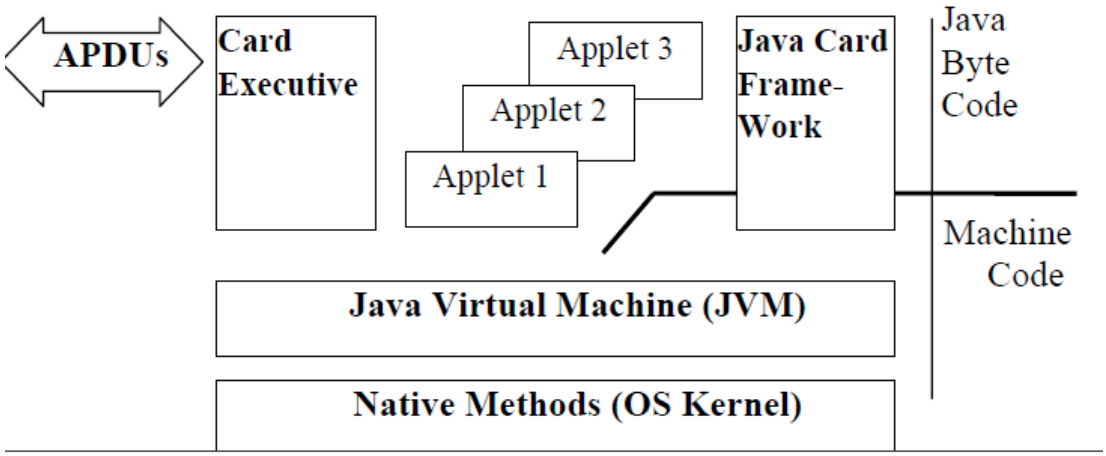
Uygulama yazılımı bu protokolü kullanarak okuyucu üzerinden akıllı kart ile haberleşmektedir. Haberleşmede kullanılan her bir APDU paketi T=0 ve T=1 link protokolü ile karta gönderilmektedir. T=0 ve T=1 link protokolü kart ile haberleşmede gönderilen verilerin byte bazında mı yoksa paket bazında mı gönderildiğini ifade eder. Şekil 3.6'da bir uygulama yazılımının kart okuyucuyu kullanarak bir akıllı kart ile haberleşmesinin aşamaları gösterilmektedir.



Şekil 3.6 Akıllı kart haberleşme mimarisi

3.9. Java Kartlar

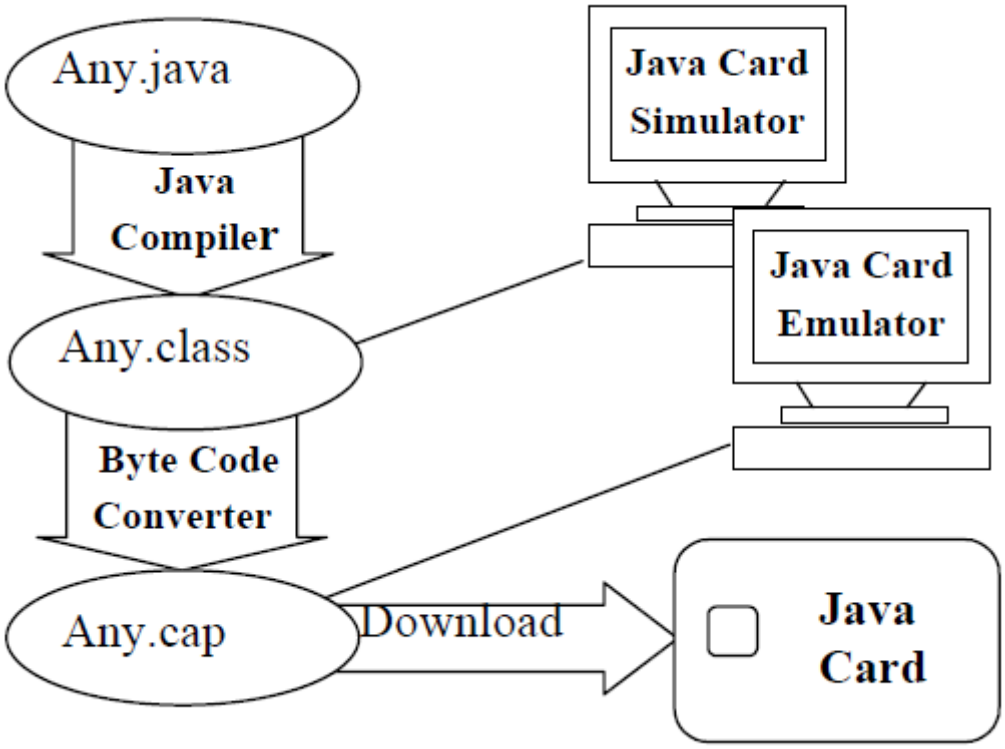
Java kartlar ilk olarak Schulumberger tarafından üretilmişler ve Javasoft tarafından standart hale getirilmişlerdir. Java kartlar üzerlerinde bir Java sanal makinesine sahiptirler. Bununla kart işlemcisinden bağımsız olarak Java appletlerinin çalıştırılması mümkündür. Java kart işletim sistemi akıllı kart üzerinde çalışacak uygulamaların Java dili ile yazılmasını mümkün kılmıştır.



Şekil 3.7 JavaCard işletim sistemi genel mimarisi

Şekil 3.7'de JavaCard işletim sisteminin kart üzerindeki genel mimarisi gösterilmektedir. Java kart işletim sistemi her biri kart üreticisine çok sıkı bağlı ve karttan karta değişen işletim sistemlerinden bağımsız olarak yazılım geliştirilmesi imkanını sağlar. Şekil 3.7'de bir Javacard işletim sisteminin genel görünümü gösterilmiştir. Bunlara ilaveten JavaCard işletim sistemi bir kart üzerinde bir birinden bağımsız birden fazla uygulamayı çalıştırıbilir. Kart üzerindeki her bir derlenmiş Java byte kodlarına Java Applet denir. Java Appletleri çalışma zamanında Java sanal makinesi tarafından yorumlanırlar. Java sanal makinesi çalışma zamanında çalışan tüm appletlerin birbirinden bağımsız olmalarını ve birbirlerini etkilememelerini garanti eder.

JavaCard işletim sistemi için bir uygulama geliştirme süreci Şekil 3.8'deki gibi adımlardan oluşur.



Şekil 3.8 Kart uygulaması geliştirme adımları

Java kaynak kodları öncelikle standart Java derleyicisi ile java byte code'lara çevrilir. JavaCard Framework derleme aşamasında dahil edilir. Derleme ile üretilen

“*.class*” dosyaları Java Card Simulatörleri ile test edilebilir. Byte kod çeviriciler derlenmiş olan “*.class*” dosyalarını akıllı kartların kısıtlı kaynakları için optimize ederek “*.cap*” dosyalarına çevirirler. Bu “.cap” dosyaları JavaCard Emulatörleri ile test edilebilir veya Java kartlara yüklenebilirler.

3.10. MULTOS

MULTOS, Mondex International tarafından geliştirilmiş çok uygulamalı, yüksek güvenlikli, açık bir akıllı kart işletim sistemidir. Multos işletim sistemi akıllı kart üzerinde birden fazla uygulamanın aynı anda kullanılabilmesine imkan sağlar. JavaCard işletim sistemi gibi kart üzerindeki tüm uygulamalar birbirinden bağımsızdır. Mondex International geliştiricilerin kullanımı için akıllı kartlara özel optimize edilmiş MEL (Multos Enabling Languge) ve Multos-API spesifikasyonları geliştirmiştir. Multos spesifikasyonları açık lisanslıdır ve uluslararası bir kuruluş olan MAOSCO tarafından yönetilirler.

Multos işletim sisteminin en önemli özelliği dil bağımsız olmasıdır. Multos akıllı kart işletim sistemi uygulamaları için kullanılabilecek programlama dilleri şunlardır.

Assembly

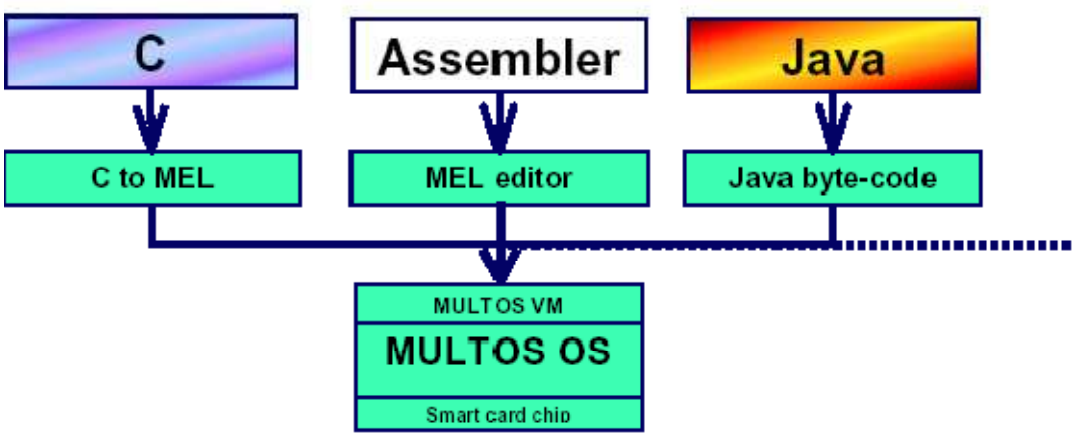
Multos, Assembly dilinin kullanılabildiği tek akıllı kart platformudur. Multos akıllı kart uygulamaları temel olarak tipik assembly komutları ve bunlara ilaveten akıllı kart için geliştirilmiş basit metodları içeren MEL dili ile geliştirilirler.

C

Multos, günümüzde C derleyicisine sahip olan tek akıllı kart platformudur. C dili en yaygın olarak kullanılan gömülü sistem programlama dilidir. SwiftCard tarafından üretilen SwiftC derleyicisi ile ANSI standartlarına uygun C kodları kolayca Multos platformu için derlenebilirler.

Java

Multos ve Javacard işletim sistemleri Java ile geliştirilmiş uygulamaların çalıştırılmasını desteklerler. Her iki platform içinde java derleyicileri kaynak kodları java sınıflarına çevirirler. JavaCard işletim sistemi için sınıflar Java byte kodlarına çevrilirler. Multos için SwiftJ derleyicisi java sınıflarını MEL kodlarına çevirir. Şekil 3.9'de Multos işletim sisteminin desteklediği geliştirme ortamları gösterilmektedir.



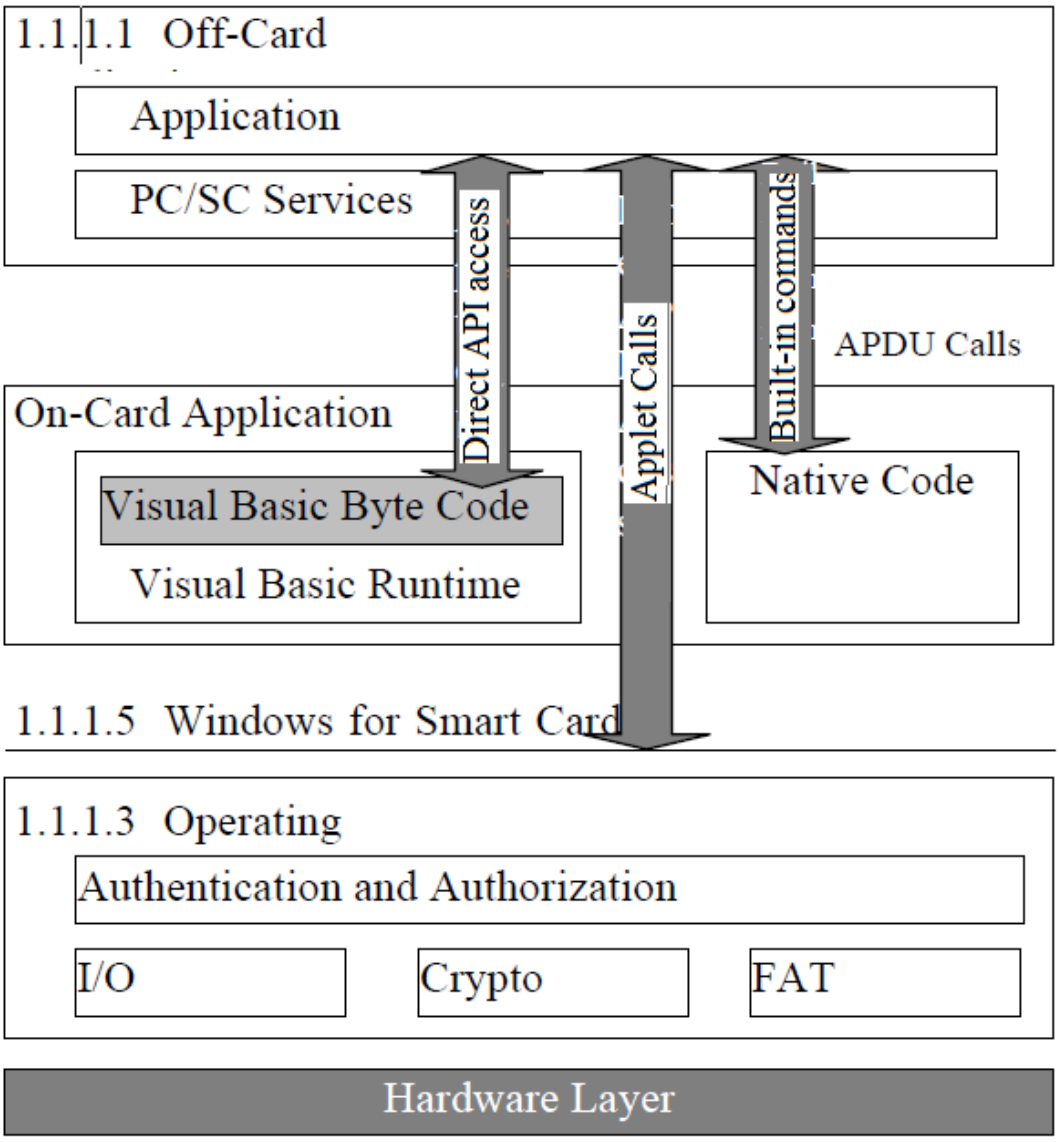
Şekil 3.9 Multos çoklu uygulama yapısı

3.11. Windows Card

1999 yılında Microsoft yazılım firması Windows for Smart Cards isimli işletim sistemi ile akıllı kart dünyasına giriş yaptı. Microsoft işletim sistemleri ailesinin en genç üyelerinden biri olan yeni Windows for smart Cards işletim sistemi bilinen Windows ortamının akıllı kartlar segmentine bir genişlemesiydi.

Microsoft Windows for Smart Cards işletim sistemi 8K ROM hafızasına sahip ve 8 bitlik işlemcileri olan kartlar için geliştirildi. İşletim sisteminde Visual Basic kullanılarak kolay şekilde programlanabilecek düşük maliyettli bir tasarım yapıldı. Hedeflenen bir diğer önemli özellik de PC ortamının akıllı kart üzerinde kullanılabilmesiydi.

Microsoft Windows for Smart Cards işletim sisteminin genel mimarisi Şekil 3.10'daki gibidir.



Şekil 3.10 Microsoft Windows for Smart Cards işletim sisteminin genel mimarisi

JavaCard işletim sistemine benzer olarak akıllı kart uygulamaları yüksek seviye diller ile yazılabilmektedir. JavaCard'ın aksine Microsoft yine kendi ürünü olan Visual Basic dilini tercih etmiştir. Bu dille yazılmış olan kodların çalıştırılması için akıllı kart işletim sistemine Visual Basic Runtime ortamını kurmuştur. Kart uygulaması dışarıdaki uygulamalar ile standart APDU komutlarını kullanarak haberleşir. İşletim sistemi akıllı kartın içeriği üzerinde işlemler yapmaya imkan

sağlayan API'leri kullanıma sunmuştur. Bu API'ler Visual Basic ile geliştirilen appletler veya diğer appletler tarafından çağırılabilirler. Bu API'ler aşağıdaki gibi sınıflandırılmış işlemleri yaparlar:

- Dosya işlemleri
- Kimlik doğrulama ve oturum açma işlemleri
- Güvenlik ve kriptografi işlemleri
- Bazı utilityler

BÖLÜM 4. MOBİL CİHAZLARDA YAKIN ALAN HABERLEŞMESİ

Yakın Alan Habeleşme teknolojisi kısa mesafeli bir temassız haberleşme sağlar. Hayatın bir çok alanında Yakın Alan Haberleşmesi uygulamaları hızla artmaktadır. Özellikle mobil cihazlarda bu gelişme daha belirgindir. Cep telefonlarının kullanım yaygınlığı ve sağladığı imkanlar Yakın Alan Haberleşmesi uygulamalarının yayılmasını ve gelişmesine imkan sağlamaktadır. Mobil alanda yapılan bu çalışmalar genelde aşağıdaki gibi sınıflandırılabilir:

Ödeme ve Bilet uygulamaları:
NFC teknolojisi kullanıcılarına hızlı ve güvenli elektronik ödeme alt yapısını sağlamaktadır. Elektronik para, sinema, uçak, konser ve etkinlik biletlerinin elektronik olarak kullanımını sağlar.

Elektronik Anahtar:
NFC teknolojili elektronik anahtarlar, ev, araç ve ofis anahtarları şeklinde kullanılabilir.

Kimlik dokümanları:
NFC teknolojisi bir cep telefonunun bir kimlik kartı şeklinde kullanımını sağlayabilir. Örneğin Japonya'da ünversitede öğrenciler telefonlarını öğrenci kimlik kartı gibi kullanabilmektedirler. NFC destekli bu telefonlarla okul ve sınıf girişlerini, kütüphane işlemlerini, kantin ve kafeterya harcamalarını, üniversite etkinliklerini kullanabilmektedirler.

Çevrim içi haberleşme:
NFC, Bluetooth ve WiFi gibi bağlantı için karmaşık konfigurasyonlar gerektiren kablosuz bağlantı türlerine alternatif olarak bir bağlantı hizmeti sunar. Bu

bağlantıların kurulumları için gerekli olan konfigurasyon işlemlerini çok hızlı şeklide yapar.

Şekil 4.1 NFC Teknolojisinin kullanım alanları

Şekil 4.1'de NFC teknolojisinin genel kullanım alanları gösterilmektedir. Bunlarla beraber yeni bir teknoloji olmasından dolayı kullanım alanları ve sağladığı çözümlerde artmaktadır.

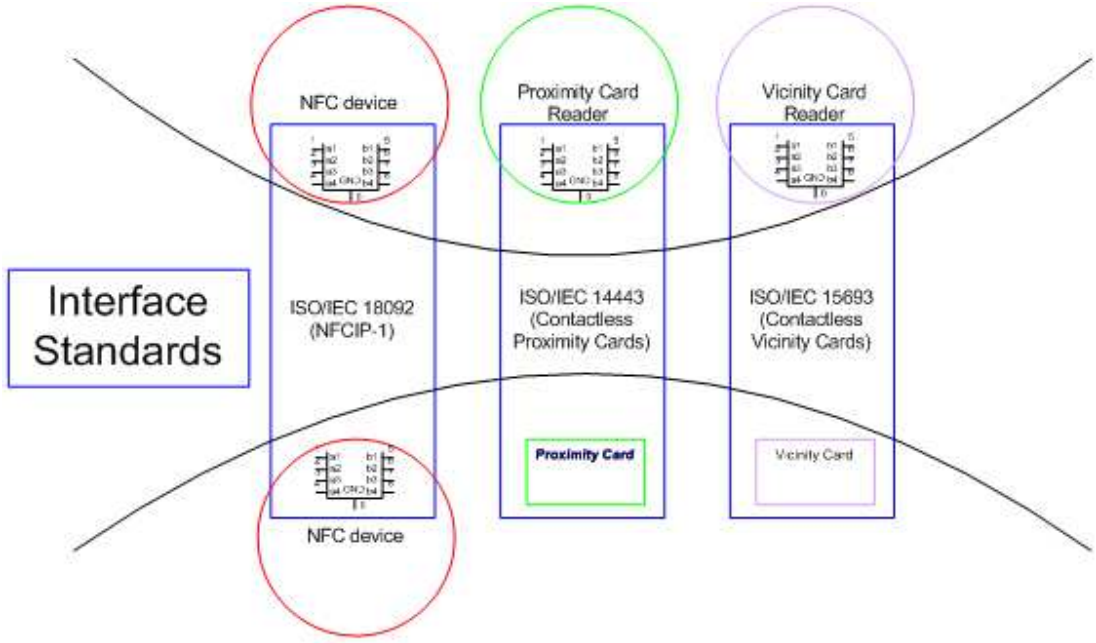
Bugüne kadar NFC genellikle, özellikle başta Japonya ve Güney Kore olmak üzere Asya'da sıklıkla kullanımaktadır. NFC'nin yaygın şekilde kullanılabilmesi için bu bölgelerde sunulan SIM kartlar NFC destekli olarak dağıtılmaktadır. Eylül 2006'da ABI Araştırma şirketinin yaptığı bir istatisiksel araştırmaya göre 2011 yılına kadar dünyadaki cep telefonu kullanıcılarının %30'u (yaklaşık 450 milyon kişi) NFC uyumlu cep telefonları kullanacaklardır. Ayrıca 2011 yılındaki NFC teknolojisi kullanılarak yapılacak ödemelerin yaklaşık 36 milyar dolara erişeceği tahmin ediliyor.

4.1. Standartlar ve Uyumluluk

NFC Philips (NXP Technologies) ve Sony'in geliştridiği bir açık platform teknolojisidir. NFC, NFCIP-1 (Near Field Communication Interface and Protocol 1) şeklinde isimlendirilir. ISO 18092, ECMA 340, ETSI TS 102 190 olarak standartlandırılmıştır.

Bu standartlar temel yetenekleri, transfer hızlarını, bit kodlama şemalarını, modülasyonu, çerçevelemeyi ve iletişim protokolünü konu edinirler. Ayrıca bunlara ilaveten aktif ve pasif NFC modlarını, haberleşme sırasında uçların durumlarını ve haberleşme kurulumundaki çakışma tespitini de konu edinirler.

Günümüzdeki NFC cihazları sadece NFCIP-1'i uygulamazlar. Ayrıca NFCIP-2'yi de uygulamaktadırlar. NFCIP-2, ISO 21481, ECMA 352, ETSI TS 102 312'de standartlaştırılmıştır. Şekil 4.2'de NFC standartları ve ilişkileri gösterilmektedir.



Şekil 4.2 NFC Standartları

NFCIP-2 ayrıca şu çalışma modlarının seçimini de sağlamaktadır:

- NFC veri transferi (NFCIP-1)
- Yaklaşım Cihaz Bağlantısı (Proximity Coupling Device) PCD
- Komşu Cihaz Bağlatısı (Vicinity Coupling Device) VCD

NFC cihazlar bu üç çalışma modunu temel uluslararası akıllı kart çalışma prensiplerini sağlamak için desteklemek zorundadır. Temassız akıllı kartların uluslararası temel standartları ISO14443 (Philips Mifare ve Proximity kartlar) ISO 15693 ve Sony'nin FeliCa temassız akıllı kart sistemleridir.

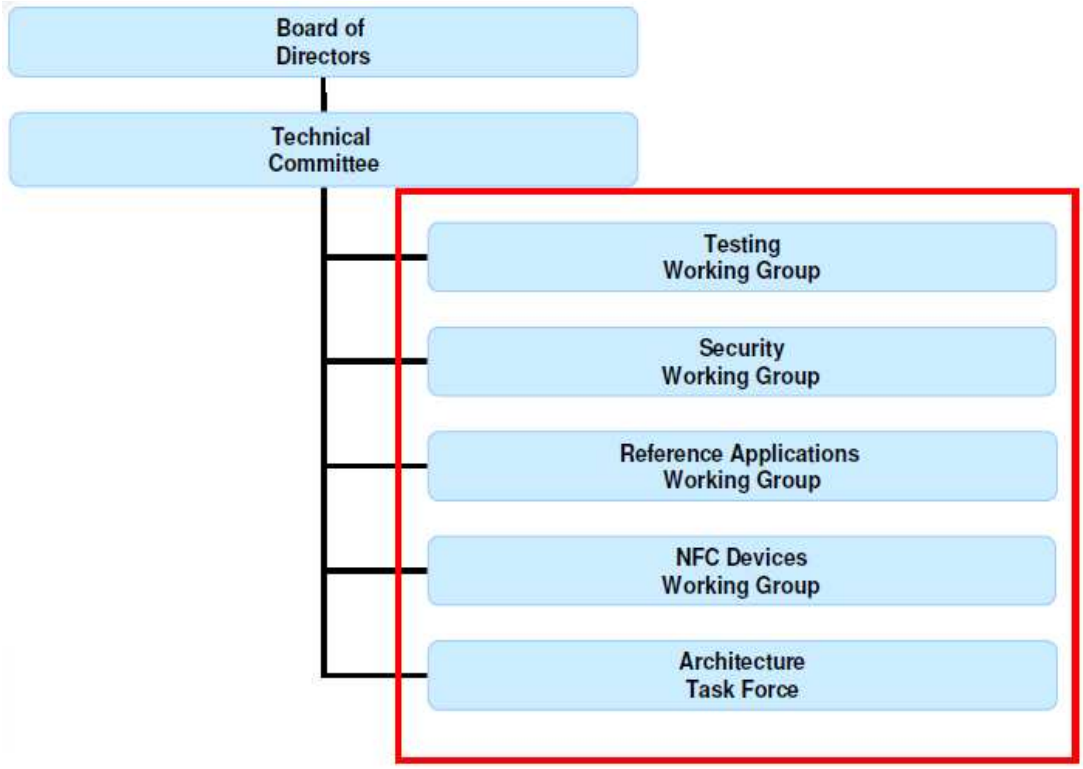
Akıllı kartlar ve temassız kartların bu birleşiminden dolayı NFC günümüz saha uygulamalarında kullanılan RFID teknolojisi ile de uyumludur.

4.2. NFC Forum

NFC Forum 18 Mart 2004'te NXP Semiconductors, Sony ve Nokia'nın katılımı ile kurulan kar amacı gütmeyen bir organizasyondur.

NFC teknolojisinin gelişimini ve standartlarını NFC Forum düzenler ve yönetir. Halen NFC Forum'un 140'a yakın üyesi bulunmaktadır. Bu üyeler üreticiler, uygulama geliştiricileri, finansal servis kurucuları gibi alanlarda faaliyet gösteren firmalardır.

NFC Forum'un teknik çalışma komiteleri Şekil 4.3'deki gibi organize edilmiştir.



Şekil 4.3 NFC Forum teknik komitesi

NFC Forum teknik komitesi beş başlık altında toplanmaktadır.

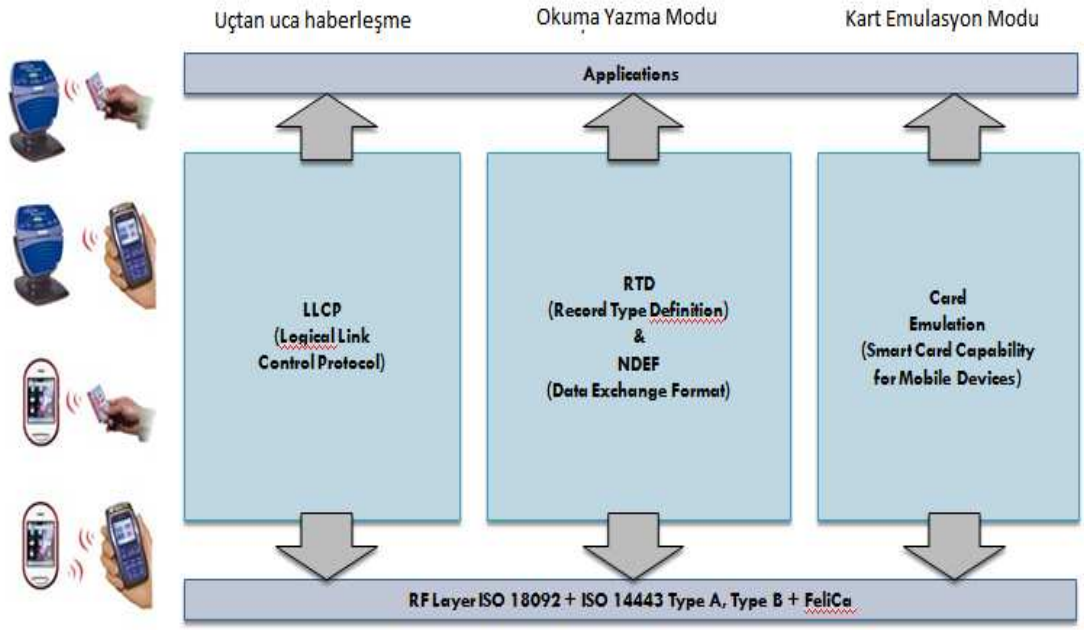
- Test çalışma grubu
- Güvenlik çalışma grubu
- Referans uygulamalar çalışma grubu
- NFC cihazlar donanım grubu
- Mimari grubu

NFC Forum'un hedefleri şunlardır

- NFC cihazların ve protokollerin standartlarını belirlemek,
- NFC Forum standartlarını kullanan ürünlerin geliştirilmesini teşvik etmek
- NFC konusunda eğitimler vermek

Kuruluşundan sadece 16 ay sonra Haziran 2006'da NFC Forum NFC'nin resmi mimarisini yayınlamıştır. Ekim 2009'a gelindiğinde NFC Forum 12 spesifikasyon, 2 aday spesifikasyon yayınlamıştır.

NFC Forum spesifikasyonları Şekil 4.4'te görüldüğü gibi sınıflandırlabilir.



Şekil 4.4 NFC Forum Spesifikasyonları

Bir örnek olarak Smart Poster RTD spesifikasyonunda Tablo 4.1'deki şu tanımlamalar olur.

Tablo 4.1 SmartPoster NDEF kayıt bilgileri

Değer	Aksiyon
0	Aksiyonu işlet. (SMS gönder, Browser'i başlat, telefon araması yap gibi)
1	Daha sonra işletmek üzere kaydet. Örneğin SMS'i Inbox'a kaydet, URI'yi Bookmark'a kaydet, Telefon numarasını Telefon defterine kaydet gibi.
2	Değiştirmek için Aç. SMS'i SMS editöründe aç, URI'yi URI editöründe aç, Telefon numarasını değiştirmek üzere aç gibi.

Örneğin bir Smart Poster kaydı bir URI ve bu URI'yi tanımlayan Metadata içerir. Şekil 4.5'te bir URI bağlantısı içeren bir SmartPoster NDEF kaydının very yapısını gösterilmektedir.

NDEF Message				
Sp (Smart Poster)				application/vcard
URI	Text	Action	Configuration	vCard data

Şekil 4.5 URI içeren SmartPoster NDEF yapısı

NFC Forum NDEF'ler için gerekli olan spesifikasyonları yayınlamaktadır. Smart Posterler'de kullanılan NDEF, NFC cihazlarla uyumlu olarak çalışabilmesi için RFID'lerin NFC veri iletişim formatı altında biçimlendirilmesi gereklidir. NDEF'in açılımı NFC Data Exchane Format şeklindedir.

NFC Forum'un tanımladığı tag tipleri şunlardır:

- Type 1: ISO14443A temel alınmıştır. Tagler okuma ve yazma uyumludur. Kullanıcılar tagleri sadece okunabilir olarak konfigure edebilirler. Hafıza kapasiteleri 96 bytetır. 2 kbyte'a kadar yükseltilebilir. Haberleşme hızı 106 Kbit/s'dir.
- Type 2: Type 1 tagler ile aynı özelliklere sahiptir. Sadece hafıza kapasitesi 48 bytetır. 2 kbyte'a kadar yükseltilebilir.
- Type 3: FeliCa temel alınmıştır. Tagler üretim aşamasında okunabilir ve yazılabilir veya sadece okunabilir olarak konfigure edilirler. Hafıza limitleri her bir servis için 1 Mbyte'tır. Haberleşme hızı 212 Kbit/s veya 424 Kbit/sdir.
- Type 4: ISO14443A ve ISO14443B standartları ile tam uyumludur. Taglar üretim aşamasında ön konfigurasyonludur. Hafıza limitleri her bir servis için 32 KBytetır. Haberleşme hızları 424Kbit/s'dir.

Bu tag tiplerinin tabloda gösterimi Tablo 4.2'deki gibidir.

Tablo 4.2 NFC Forum'un tanımladığı Tag Tipleri

	Type 1	Type 2	Type 3	Type 4
RF Interface	ISO 14443 A-2	ISO 14443 A-2	FeliCa (ISO 18092, passive communication mode at 212 kbits/sec)	ISO 14443-2
Initialization	ISO 14443 A-3	ISO 14443 A-3	FeliCa (ISO 18092, passive communication mode at 212 kbits/sec)	ISO 14443-3
Speed	106 kbits/sec	106 kbits/sec	212 kbits/sec	106-424 kbits/sec
Protocol	Specific Command set	Specific Command Set	FeliCa protocol	ISO 14443-4 ISO 7816-4 commands
Memory Size	Up to 1 KB	Up to 2 KB	Up to 1 MB	Up to 64KB
Cost (memory dependent)	Low	Low	Moderate	Moderate
Use cases	Tags with small memory for single application		Flexible tags with larger memory offering multi-application capabilities	

4.3. Teknolojiye Genel Bakış

NFC, tüm dünyada kullanılabilen 13,56 Mhz frekans bandında çalışmaktadır. Mümkün olan veri transferleri 106 kbps, 212 kbps ve 424 kbps hızlarındadır. (Şekil 4.6). Ancak daha hızlı iletişim oranlarını uygulamak da mümkündür. NFC teknolojisi, haberleşmenin 20 cm'ye kadar bir mesafeden yapılabilmesini sağlayacak şekilde tasarlanmıştır. Ancak uygulamalar 10 cm'e kadar bir mesafeden haberleşmeyi gerçekleştirmektedir. Standartlara rağmen daha kısa mesafede haberleşme yapmak maliyetlerden kaçınmaktan kaynaklanmaktadır. Daha kısa mesafeden haberleşen cihazların üretim maliyeti daha uzun mesafeden haberleşen cihazların üretim maliyetine nazaran daha azdır. Ancak mesafenin kısa olması bir dezavantaj değil aksine avantajdır. Veri güvenliği açısından daha kısa mesafeli haberleşmeler daha güvenlidirler. Kalabalık ortamlarda temassız haberleşmenin daha dar alanlarda gerçekleşmesi istenmeyen kulak misafirlerini önleyecektir.

Şekil 4.6 NFC bağlantısı

Yakın alan haberleşmesinde kullanılan radyo dalgaları frenkansları şunlardır:

125-135 KHz:
- Radyasyon problemi yoktur.
- Yansıma problemi yoktur.
- Daha ucuz elektronik bileşenlerle imal edilir.

13.56 MHz
- En fazla 1 metre haberleşme mesafesi,
- Metaller ve akışkanlar içinde çalışmazlar.

UHF
- Uzun mesafe haberleşme imkanı; herhangi bir güç kaynağı olmaksızın 10 metreye kadar haberleşebilme.

GHz
- Uzun mesafe haberleşme,
- Yüksek veri transfer hızı,

4.4. Haberleşmede Yakın Alan

RFID antenleri ortamdaki elektromanyetik alanı, radyo dalgalarını absorbe ederler. Eğer bir RFID tag, okuyucunun ortama yaydığı elektro manyetik dalgaların tam

dalga boyunun mesafesi içinde ise buna “Yakın Alan” denir. Eğer RFID tag okuyucunun yaydığı elektro manyetik dalgaların tam dalga boyundan daha uzak mesafede ise buna “Uzak Alan” denmektedir.

Yakın alan sinyalleri anten ile olan mesafenin küpü ile doğru oranltılı olarak azalmaktadır. Bununla beraber Uzak alan sinyalleri anten ile olan mesafenin karesi ile doğru orantılı olarak azalmaktadır.

Bu yüzden Yakın Alan Haberleşmesi ile çalışan Pasif RFID sistemleri diğer Uzak Alan Haberleşmesi ile çalışan sistemlerden daha kısa mesafeli okuma mesafesine sahiptir .

4.5. Haberleşme Modları

Bir NFC cihazı iki modda çalışabilir. Bu modlar Aktif mod ve Pasif mod olarak isimlendirilir.

Aktif modda çalışan bir NFC cihazı haberleşmek için kendi elektro manyetik alanını kendisi oluşturur. Bunun için bir enerji kaynağına sahiptir. Ancak pasif modda çalışan bir NFC cihazı haberleşmek için bir elektro manyetik alan oluşturmaz. Bağlı olduğu, haberleştiği cihazın elektro manyetik alanını kullanırlar. Pil ile beslenen cep telefonu gibi cihazlarda pasif modu kullanmak daha avantajlıdır. Pasif modda haberleşen NFC uyumlu bir cep telefonu Aktif modda çalışmanın tersine haberleşme için üzerindeki pili kullanmayacaktır. Pasif modda çalışma durumunda NFC cihazı veri transferi için aktif olan diğer NFC cihazının elektro manyetik alanını kullanacaktır. Bu sayede cihazın kart emulasyonu modunda çalışması mümkündür. Örneğin bilet uygulamalarında cep telefonları kapalı olsa bile üzerindeki NFC cihazlar çalıştırılabilir.

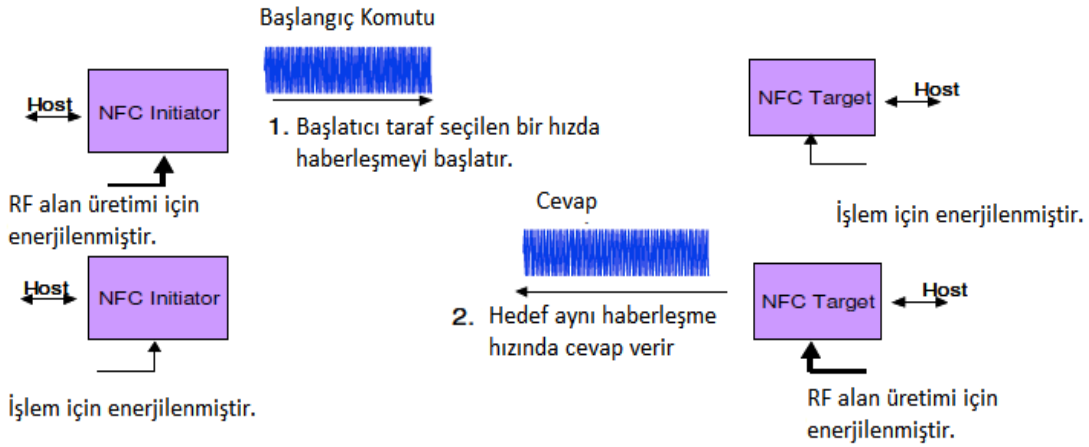
4.5.1 Aktif modda haberleşme

İki aktif NFC cihaz arasındaki haberleşme Aktif Haberleşme modu diye isimlendirilir. Bir Aktif ve bir Pasif NFC cihaz arasındaki haberleşme moduna da Pasif Haberleşme modu adı verilir. Bu iki mod aşağıdaki tabloda gösterilmiştir.

Tablo 4.3 NFC haberleşme modları

Haberleşme Modu	Açıklama
Aktif Mod	İki aktif NFC cihazının birbiri ile haberleşmesidir. Her bir cihaz veri göndermek istediğinde kendi elektro manyetik alanlarını kendileri oluştururlar.
Pasif Mod	Bu haberleşme modu, bir uçta aktif modda çalışan NFC cihaz ile diğer uçta pasif modda çalışan NFC cihaz arasında gerçekleşir. Pasif modda çalışan NFC cihazı kendi enerjisini aktif tarafın ürettiği elektro manyetik alandan üretir.

Şekil 4.7'de aktif modda gerçekleşen bir haberleşme gösterilmektedir. Şekle gore sol taraftaki cihaz haberleşmeyi başlatan (Initiator) sağ taraftaki cihaz ise hedef (Target) cihazdır.



Şekil 4.7 Aktif modda haberleşme

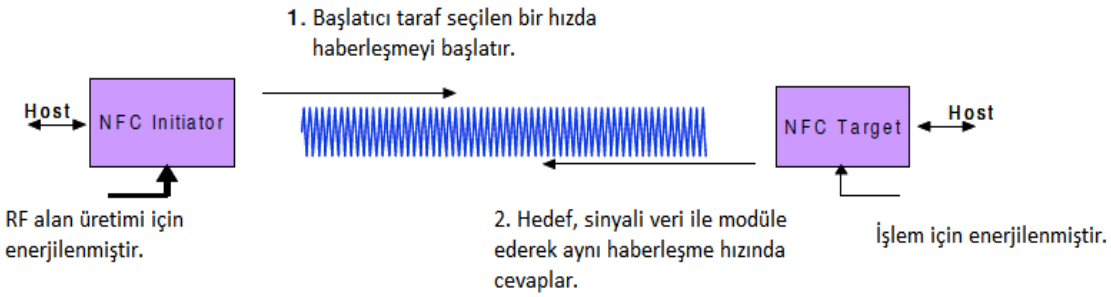
Aktif modda haberleşmede haberleşmeyi başlatan taraf (Initiator) kendi elektro manyetik alanını oluşturur. Göndermek istediği mesajı oluşturarak seçilen bir hızda

mesajını gönderir. Bu sırada hedef (Target) cihaz dinlemededir. Hedef cihaz mesajı alıp işldikten sonra cevap mesajını oluşturur. Hedef cihaz kendi oluşturduğu elektro manyetik alanı ile mesajını haberleşmeyi başlatan tarafa iletir. Bu sırada haberleşmeyi başlatan taraf elektro manyetik alan üretmemekte gelen cevabı dinlemektedir. Hedef cihaz, aldığı mesaj ile aynı hızda cevabını karşı tarafa iletir.

4.5.2. Pasif modda haberleşme

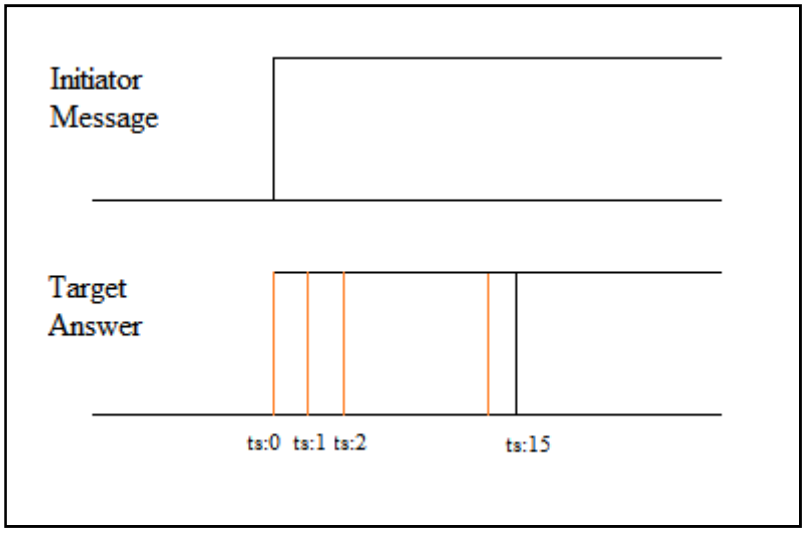
Pasif modda haberleşmede haberleşmeyi başlatan taraf –Şekil 4.8'e gore soldaki taraf- mesajını oluşturur ve kendi elektro manyetik alanını üreterek mesajı seçilen belli bir hızda hedef cihaza gönderir. Bu sırada hedef cihaz dinlemededir. Hedef cihaz diğer işlemleri için enerjilendirilmiş olabileceği gibi, tamamen enerjisiz de olabilir. Tamamen enerjisiz durumda haberleşmeyi başlatan tarafın ürettiği eletro manyetik alan değişiminin içinde bulunduğu anda işlem yapabilecek kadar enerjiyi gelen mesajı taşıyan elektro manyetik alandan üretebilir. Böylece herhangi bir enerji kaynağına ihtiyaç duymaksızın gelen mesajı işleyebilir. Hedef cihaz gelen mesajı module ederek aynı hızda cevaplar.

Şekil 4.8'de de pasif modda haberleşen iki cihaz gösterilmektedir.



Şekil 4.8 Pasif modda haberleşme

Genelde her iki cihaz aynı anda bir biri ile haberleşirler. Ancak pasif modda birden fazla hedef ile haberleşebilir. Bu işlem Single Device Detection (SDD)'inin uyarlanmasında kullanılan time slot metodu ile gerçekleştirilir. Maksimum time slot 16 ile sınırlandırılmıştır. (Şekil 4.9)



Şekil 4.9 Pasif mod haberleşmede time slot

Hedef cihaz haberleşmeyi başlatan cihaza rasgele seçilmiş bir time slot içinde cevap verir. Böylece diğer hedef cihazların aynı anda çalışmasında çakışmalar bir miktar önlenir. Çakışmayı önlemek için kullanılan bir diğer metod da haberleşmeyi başlatan tarafın sorgulama isteklerini hedef cihazın görmezden gelmesidir. Eğer haberleşmeyi başlatan cihaz sorgulama isteğine herhangi bir cevap alamıyorsa sorgulama isteğini tekrarlar.

4.6. Kodlama ve Modülasyon

Bir NFC cihazının aktif veya pasif modda olmasının durumu haberleşmenin nasıl yapıldığını belirlemektedir. Pasif modda çalışan cihazlar her zaman Manchester kodlama ve %10 ASK kullanırlar. Bunun yerine aktif modda çalışan cihazlar iki kodlama türünden birini seçerler. Eğer veri transfer hızı 106 kbps ise %100 modülasyonlu Miller kodlamasını seçerler. Eğer veri transfer hızı 106 kbps üzeride gerçekleşiyorsa cihazlar %10 modüasyon oranını kullanan Manchester kodlamasını kullanırlar. Tablo 4.4'te seçilen veri hızına gore aktif ve pasif cihazların kullandıkları modülasyonlar gösterilektedir.

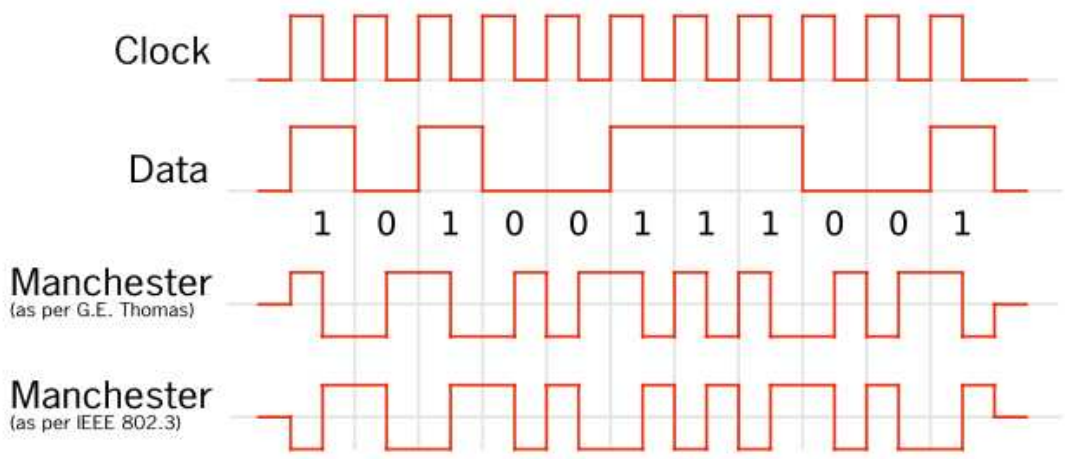
Tablo 4.4 Kullanılan modülasyonlar

Veri trasnfer hızı	Aktif Cihaz	Pasif Cihaz
106 kbps	Modifiye edilmiş Miller, %100 ASK	Manchester, %10 ASK
212 kbps	Manchester, %10 ASK	Manchester, %10 ASK
424 kbps	Manchester, %10 ASK	Manchester, %10 ASK

4.6.1. Manchester kodlama

Manchester kodlama bir periodun ortasında iki durum arasında geçişlerin durumuna dayanır. Düşük durumdan yüksek duruma geçişler Manchester kodlamada 0 olarak ifade edilir. Aynı şekilde yüksek durumdan düşük duruma geçişler de 1 olarak tanımlanırlar. Manchester kodlamada her bit bir geçişi ifade eder. Periodun başındaki durum dikkate alınmamaktadır.

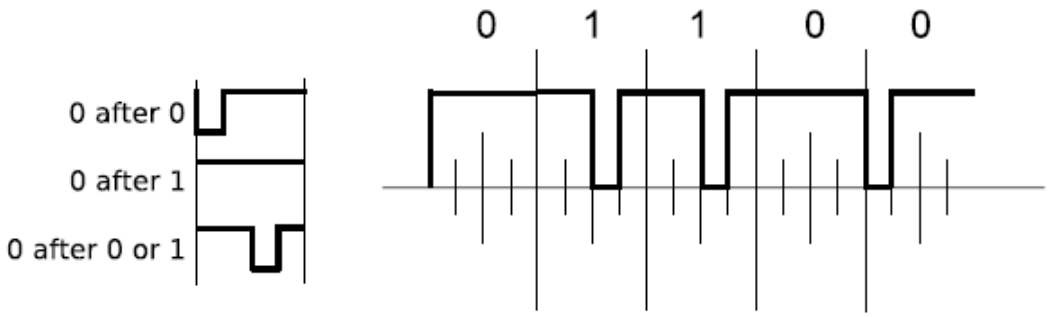
ASK (Amplitude Shift Keying) için taşıyıcı işaretinin farklı genliği kullanılmaktadır. İkili ASK (Binary Amplitude Shift Keying, BASK) için taşıyıcı 0 ve 1 bitleri için taşıyıcının iki farklı genliği (A0 ve A1) kullanılır. Bu modülasyon türünde taşıyıcının frekans ve fazı sabittir. Genel olarak faz sıfır olarak alınır. Şekil 4.10'da bir Manchester kodlama örneği gösterilmektedir



Şekil 4.10 Manchester kodlama

4.6.2. Modified Miller kodlama

Bu tür kodlama taşıyıcının bir periodun farklı pozisyonlarında duraklaması ile yapılır. Haberleşmede gönderilen veriye bağlı olarak bitler farklı şekillerde kodlanır. Modified Miller kodlamada 1 değerli bitler her zaman aynı şekilde kodlanırken sıfır değerli bitlerin kodlanması kendinden once gelen bitin değerine gore değişir. Şekil 4.11'de örnek bir sıfır dizisinin Modified Miller ile nasıl kodlandığı gösterilmektedir.



Şekil 4.11 Modified Miller kodlama

4.7. Başlatıcı (Initiator) ve Hedef (Target) Uçlar

Başlatıcı (Initiator) ve Hedef (Target) taglerin aldıkları rolleri gözlemek de ayrıca önemlidir. Başlatıcı haberleşmeyi isteyen ve haberleşme işlemini başlatan taraftır. Hedef ise başlatıcı tarafın gönderdiği haberleşme sinyallerini alan ve onlara cevap veren taraftır. Bu kavram hedefin herhangi bir haberleşme verisi almaksızın veri göndermesini engeller. Pasif haberleşme moduna göre ise, pasif cihazlar sürekli olarak bir NFC hedef cihaz gibi davranırlar. Aktif cihazlar haberleşmeyi başlatıcıdır. Sonuç olarak başlatıcı taraf haberleşmek için elektro manyetik alanlarını oluştururlar. Elektro manyetik alanın üretilmesindeki aktif olan konfigurasyonun durumuna gore başlatıcı ve hedefin haberleşmedeki roller kimin haberleşmeyi başlattığı ile yakından ilgilidir. Default olarak tüm cihazlar NFC hedef cihazlardır. Ancak bir uygulama tarafından kullanıdığı zaman NFC başlatıcı cihaz olarak çalışırlar.

Her iki taraftaki, başlatıcı ve hedef cihazın pasif olduğu durumda haberleşme gerçekleşemez. Tablo 4.5'de mümkün olan aktif, pasif ve başlatıcı, hedef kombinasyonları gösterilmiştir.

Tablo 4.5 Mümkün olan kombinasyonlar

	Başlatıcı	Hedef
Aktif	Mümkün	Mümkün
Pasif	Mümkün Değil	Mümkün

4.8. Çakışma Önleme

Genellikle cihazların doğrudan yaklaştırıldığı durumlarda yanlış haberleşmeler oldukça nadir gerçekleşir. Haberleşme protokolünün temel prensibi şudur: Konuşmadan önce dinle.

Eğer bir başlatıcı haberleşmek istiyorsa, öncelikle başka bir harici elektro manyetik alan olmadığından emin olmalıdır. Ortamda başka bir başlatıcının ürettiği bir elektro manyetik alan varsa yeni bir haberleşme başlatmak için beklenir. Başlatıcı var olan bir NFC haberleşmesini kesmemelidir. Başlatıcı haberleşmeye başlamadan önce sessizce bir başka elektro manyetik alan olup olmadığını anlamak için ortamı dinler. Bu bekleme süresine Guard-Time denir. Eğer birden fazla hedef cihaz aynı anda cevap veriyorsa bu çakışma başlatıcı tarafından tespit edilir.

4.9. Genel NFC Protokol Akışı

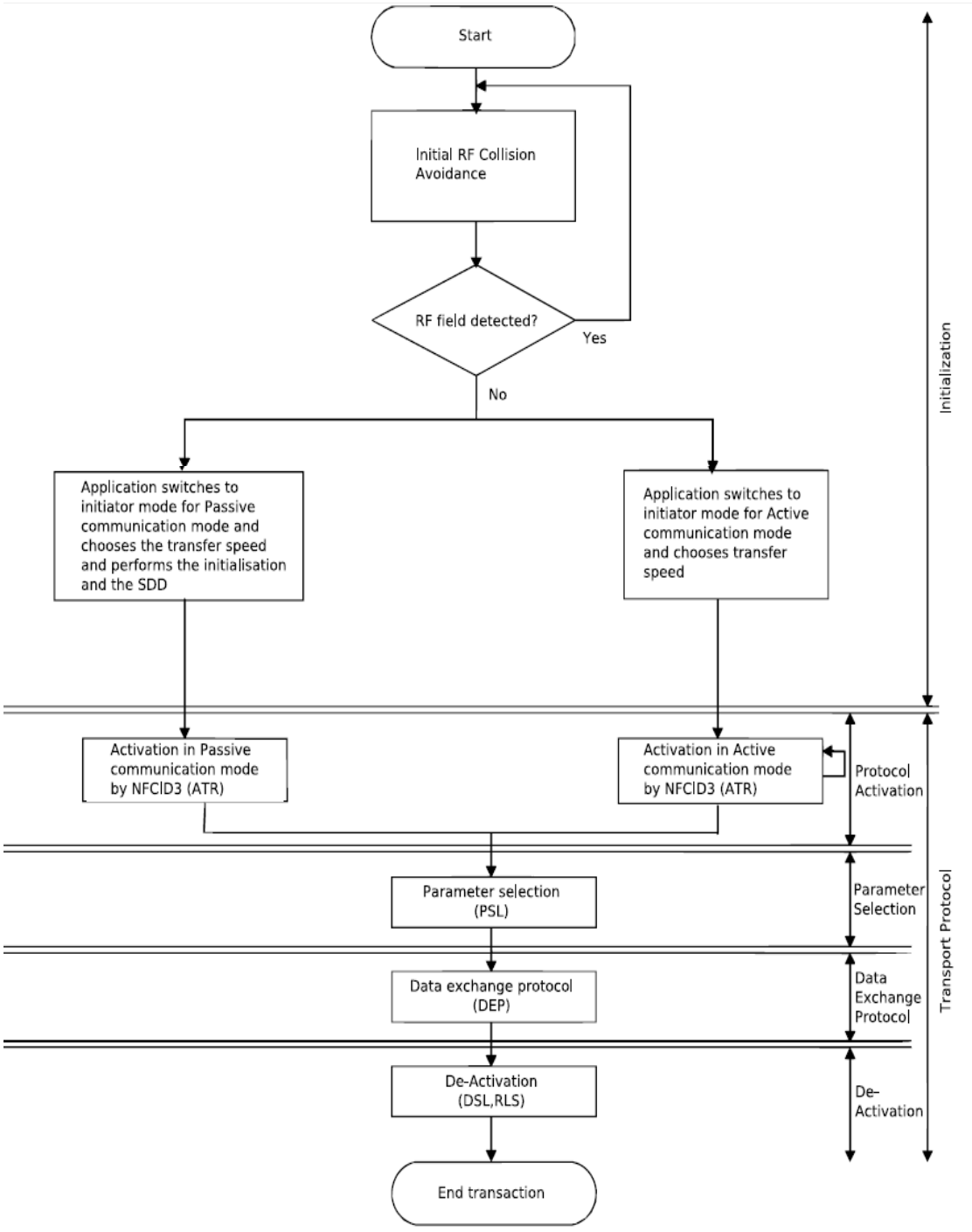
Şekil 4.12'de de görüldüğü gibi genel protokol akışı kurulum ve transport protokolü olmak üzere ikiye ayrılır. Kurulum safhası çakışma önlemeyi ve hedeflerin seçimini içerir. Başlatıcı kurulum safhasında ayrıca aktif veya pasif haberleşme modunu ve haberleşme hızını seçer.

Transport protokolü üç kısma ayrılmıştır.

- Protokolün başlatılması: Niteliklerin talep edilmesi (Request for Attributes) ve parametre seçimi (Parameter Selection) içerir.

- Veri değişim protokolü
- Protokolün bitirilmesi, Seçimlerin bırakılması (Deselection) ve kaynakları serbest bırakılması (Release)

Bir haberleşme işlemi sırasında aktif ve pasif olma durumu ve başlatıcı veya hedef olma rolü haberleşme tamamlanmaksızın değişmez. Haberleşmenin başlamasındna once bu durumlar belli olur ve bitene kadar devam eder. Buna rağmen veri transfer hızı parametre değiştirme prosedürleri ile değiştirilebilir. Parametre değiştirme prosedürleri standartlarda detaylı olarak belirtilmiştir.



Şekil 1.12 Genel ilklendirme ve veri taşıma protokolü

4.10. NFC ve Diğer Haberleşme Teknolojileri

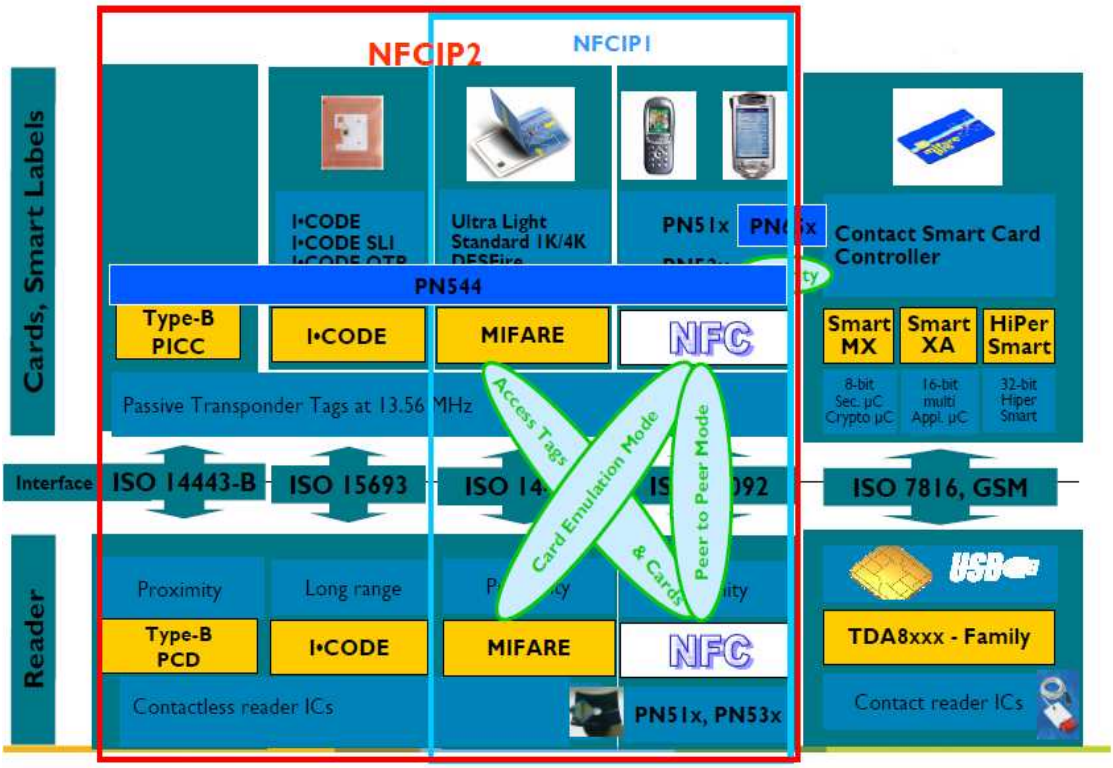
NFC'nin diğer bağlantı teknolojileri ile çeşitli konularda kıyaslanması Tablo 4.6'da gösterilmiştir.

Tablo 4.6 NFC ve diğer bağlantı türleri karşılaştırması

	NFC	**RFID**	**IrDA**	**Bluetooth**
Kurulum Süresi	< 0.1 ms	< 0.1 ms	~0.5 s	~6.0 s
Mesafe	10 cm	3m	5m	30m
Kullanım hedefleri	Son kullanıcıya yönelik	Nesne izleme	Veri transferi	Veri transferi
Kullanım alanları	Ödeme, Erişim, Paylaşım, Servis başlatma, Kolay kurulum	Nesne izleme	Kontrol ve Veri transferi	Veri transferi için network ve headset kullanımı
Bağlantıda seçicilik	Yüksek, Güvenli, Belirli/görünür	Kısmen belirli/görünür	Görüş alanında olmalı	Kimsin? Modunda seçimli
Son Kullanıcı deneyimi	Dokunma, gösterme/sallama, Kolay bağlantı	Bilgi alma	Kolay	Konfigurasyon gerekiyor

4.10.1. NFC ve RFID

Temel olarak RFID ve NFC teknolojileri aynı standartlar üzerine kurulmuştur. Ancak RFID teknolojisine en büyük eklenti haberleşmenin iki aktif cihaz arasında yapılabilmesi imkanıdır. Temassız akıllı kartların haberleşmesinde bir taraf aktif diğer taraf pasif olan bir haberleşme modu vardır. Ancak NFC iki aktif cihazın uçtan uca haberleşmesini de sağlamaktadır. Bu yüzden NFC hem RFID taglerin okunup yazılması hemde iki elektronik cihazın veri paylaşımını da sağlar.



Şekil 4.13 Temassız kart ve okuyucu ilişkileri

Şekil 4.13'de NFC ve RFID teknolojilerinin bir biri ile etkileşmi gösterilmektedir. Mavi ile işaretlenen kısım NFCIPI standardında desteklenen teknolojileri göstermektedir. Kırmızı ile işaretlenen kısımda ise NFCIP2 standardı ile desteklenen teknolojileri gösterir.

Yerleşik RFID teknolojilerinin desteği ile birlikte NFC standarlarının ilişkili olduğu standartlar aşağıda listelenmiştir.

- ISO 14443 A/B Reader / Writer
- ISO 15693 Reader / Writer
- ISO 7816 – 4 (T = 0, T = 1)

4.10.2. NFC ve kızılötesi bağlantı

Diğer bir yakın haberleşme teknolojisi olan Kızılötesi bağlantı IrDA, 1993'te keşfedilmiş ve kullanılmaya başlanmıştır. Eski bir kablosuz haberleşme teknolojisi

olan Kızılötesi haberleşmenin en büyük dezavantajı haberleşecek olan her iki cihazın da bir birini direk olarak görmesi gerektiğidir.

4.10.3. NFC ve bluetooth bağlantısı

NFC ile Bluetooth bağlantıları birbirlerine oldukça benzer iki bağlantı türüdür. Her ikiside mobil telefonlara entegre edilmiş kısa mesafeli haberleşme teknolojileridir. NFC'nin Bluetooth'a gore en büyük avantajı çok kısa sürede bağlantı kurulabiliyor olmasıdır. Bluetooth kullanan cihazlarda bağlatı kurulabilmesi için once elle konfigurasyon yapılması gerekmektedir. Bu işlem oldukça uzun süre almaktadır. Yaklaşık bağlantı kurulum süresi 6 saniye kadardır. Bununla beraber NFC kullanan cihazlarda bağlantı kurulma süresi saniyenin onda biri kadar bir sürede yapılabilmektedir. Karmaşık kurulum işlemlerinden kaçınmak için NFC temassız iletişimin kurulması için oldukça kullanışlıdır.

NFC'nin maksimum veri transfer hızı 424 Kbit/s'dir. Bu Bluetooth'un 2.1MBit/s'lik hızına göre oldukça yavaştır.

NFC'nin veri iletişim mesafesi de 20 cm'nin altındadır. Bu mesafe Bluetooth'un mesafesinin altındadır. Ancak mesafenin kısa olması güvenliği arttırmaktadır. Kalabalık ortamlarda üçüncü şahısların haberleşmeyi dinleme imkanları daha azdır.

NFC teknolojisi tamamen RFID teknolojisi üzerine kurulmuştur. NFC mobil cihazlar mevcut RFID sistemlerle geriye uyumlu olarak çalışabilirler.

NFC cihazlar Bluetooth cihazlara göre daha az enerji tüketirler. Bluetooth haberleşmesi yapılırken her iki cihazın da enerjili olması gerekmektedir. Ancak NFC cihazlarda haberleşme sırasında sadece bir tarafın enerjili olması yeterlidir. Örneğin NFC uyumlu bir telefon kapalı iken bile üzerindeki temassız akıllı kart çalışabilir. Veya akıllı posterler hiç bir enerji kaynağı olmadan NFC mobil cihazlar tarafından okunabilirler. Tablo 4.7'de NFC ile Bluetooth bağlantılar karşılaştırılmıştır.

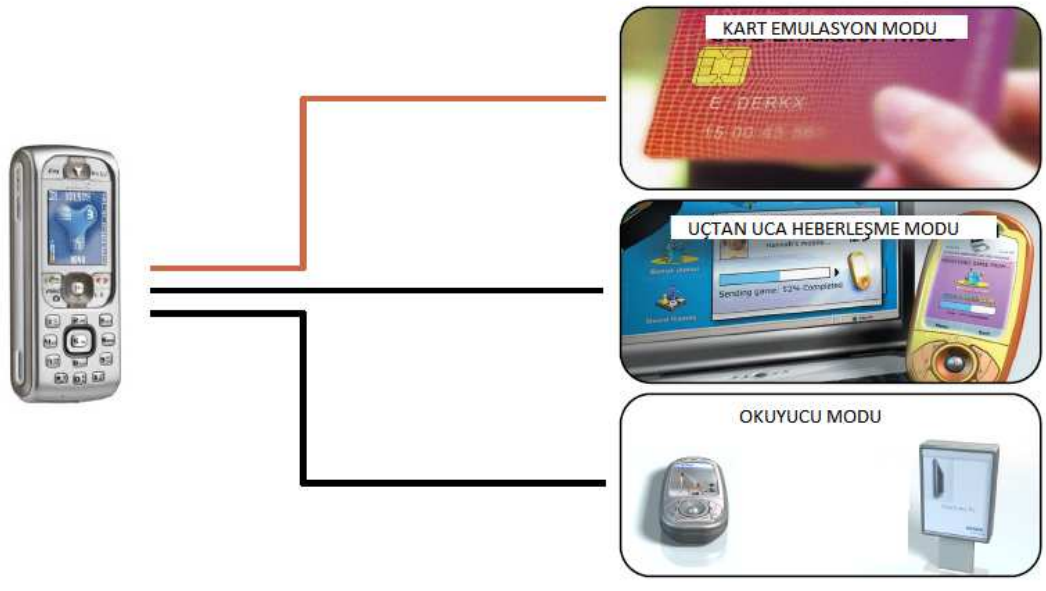
Tablo 4.7 NFC ve Bluetooth bağlantıların karşılaştırılması

	NFC	Bluetooth
Network tipi	Point-to-Point	Point-to-MultiPoint
Mesafe	<10 cm	10 m
Frekans	13.56 MHz	2.4 – 2.5 GHz
Bit Rate	424 Kbit/s	2.1 MBit/s
Kurulum süresi	<0.1 s	6 s
RFID uyumluluk	Evet	Hayır

4.11. NFC Cihazların Çalışma Modları

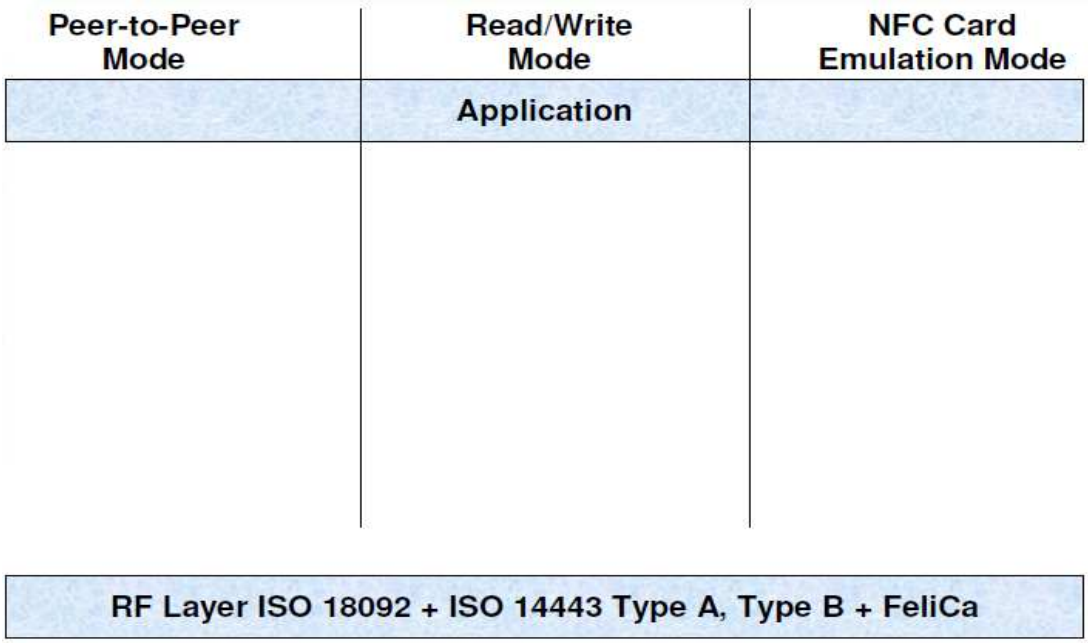
NFC uyumlu cihazlar farklı hedeflerle farklı şekillerde haberleşebilirler. Diğer temassız haberleşme teknolojilerine göre daha çeşitli haberleşme tipleri oluşturabilirler. Bu haberleşme türlerinde NFC cihazlar hem aktif hem de pasif olarak rol alabilirler.

NFC uyumlu cihazların üç temel çalışma biçimi vardır. Bunlar:
- Okuyucu mod haberleşme. Reader Mode
- Kart Emülasyonu, Card Emulation Mode
- Uçtan uca haberleşme. Peer-to-Peer Mode



Şekil 4.14 NFC çalışma modları

Şekil 4.15'de NFC cihazların çalışma modlarına göre belirlendikleri standartlar gösterilmiştir.



Şekil 4.15 NFC çalışma modları ve standartlar

NFC standartları, bir NFC cihazın en temelde bazı özellikleri destrekliyor olmasını şart koşar. Bunlar ISO 14443 Type A ve ISO 14443 Type B Tag standartları ile Sony'nin FeliCa standardıdır. (Şekil 4.15)

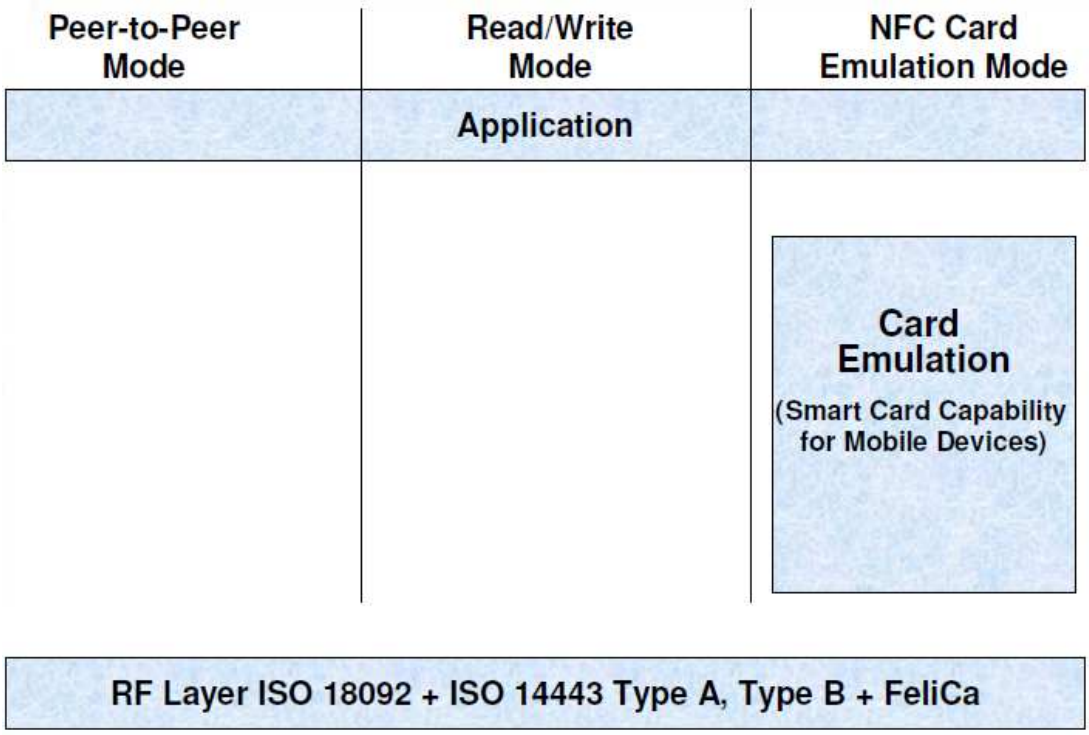
ISO 14443 dört alt bölümde 13,56 MHz hızında temassız olarak bir okuyucu antenle haberleşen akıllı kartları standardize eder.

- Type 1: ISO14443A temel alınmıştır. Tagler okuma ve yazma uyumludur. Kullanıcılar tagleri sadece okunabilir olarak konfigure edebilirler. Hafıza kapasiteleri 96 bytetır. 2 kbyte'a kadar yükseltilebilir. Haberleşme hızı 106 Kbit/s'dir.
- Type 2: Type 1 tagler ile aynı özelliklere sahiptir. Sadece hafıza kapasitesi 48 bytetır. 2 kbytea kadar yükseltilebilirler.
- Type 3: FeliCa temel alınmıştır. Tagler üretim aşamasında okunabilir ve yazılabilir veya sadece okunabilir olarak konfigure edilirler. Hafıza limitleri her bir servis için 1 Mbytetır. Haberleşme hızı 212 Kbit/s veya 424 Kbit/sdir.

- Type 4: ISO14443A ve B standartları ile tam uyumludur. Taglar üretim aşamasında ön konfigurasyonludur. Hafıza limitleri her bir servis için 32 KBytetır. Haberleşme hızları 424Kbit/s'dir.

4.11.1. Kart emulasyon modu – NFC card emulation mode

Kart emülasyon modunda NFC cihaz bir temassız akıllı kart ile aynı şekilde çalışmaktadır. Okuyucunun elektro manyetik alanında bulunan kart, okuyucudan aldığı komutları çalıştırır. Kart emulasyon modunda çalışan NFC cihaz işlemlerini yapabilmek için enerjisini okuyucunun üretmiş olduğu ve içinde bulunduğu elektro manyetik alan değişiminden üretir. Bu modda NFC cihaz pasif durumda çalışmaktadır. Bu işlemde NFC cihaz bir temassız akıllı karttan farklı değildir.



Şekil 4.16 Kart emulasyonu modu

NFC cihazı barındıran mobil cihaz enerjili olmasada NFC cihaz bu modda çalışabilmektedir. Enerjisini okuyucunun elektro manyetik alan değişiminden üretmektedir.

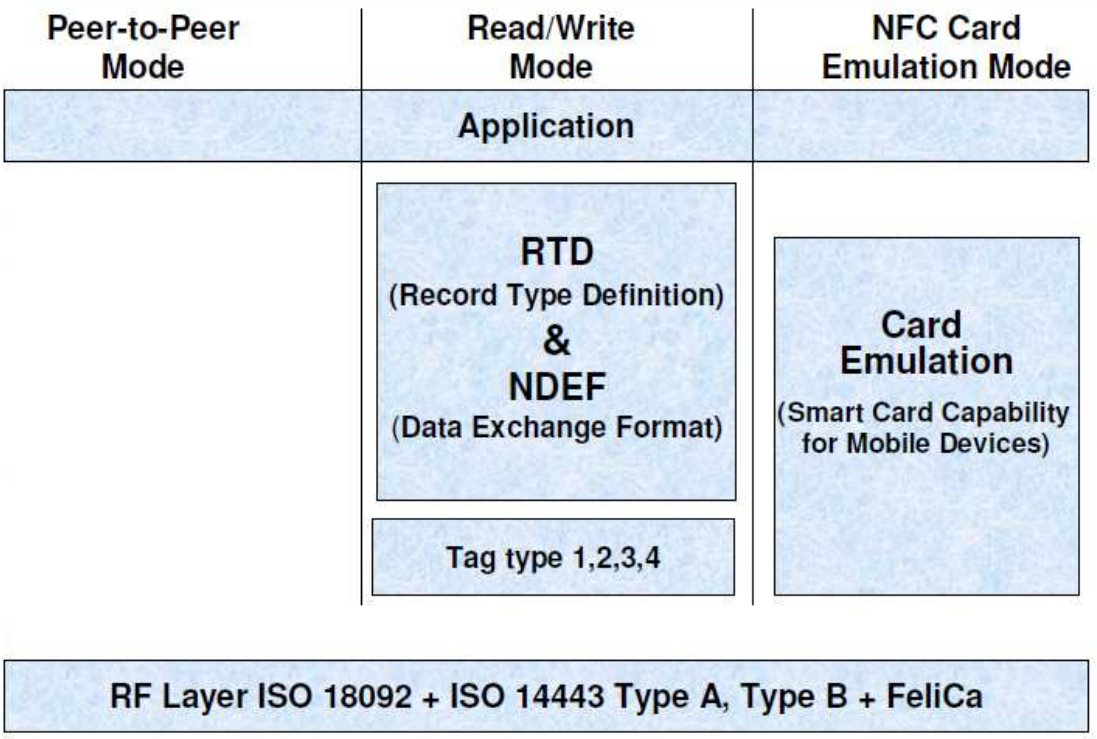
NFC'nin kart emulasyonu yeteneği sayesinde temassız ödeme teknolojilerinde hiç bir değişiklik yapmaksızın bu yeni teknolojiyi kullanabilme imkanı doğmaktadır. NFC temassız ödeme teknolojisinde geriye uyumlu olarak çalışmaktadır.

Şekil 4.16'da Kart Emulasyon modunda çalışan NFC cihazın standartlara göre durumu gösterilmiştir.

4.11.2. Okuyucu mod, read/write mode

Okuyucu modunda çalışan bir NFC cihazı, NFC Forum'un standartlarında tanımladığı türden tag tiplerini okuyup yazabilmektedir. Okuyucu modda çalışan bir NFC cihaz temassız kart okuyucu gibi çalışmaktadır. NFC cihaz diğer tagleri ve temassız akıllı kartları okuyabilmektedir.

Okuyucu modda çalışan bir NFC cihaz tag ve temassız akıllı kartları okuyabilmek için kendi elektro manyetik alanını üretir. Bu modda çalışan NFC cihaz aktif modda haberleşmektedir.



Şekil 4.17 Okuyucu modu

NFC Forum okuyucu modunda çalışan cihazlar için bazı standartlar belirlemiştir. Bunlar NDEF (NFC Data Exchange Format) ve RTD (Record Type Definition) olarak isimlendirilmişlerdir. (Şekil 4.17)

NDEF spesifikasyonu bir NFC cihaz ile diğer NFC cihaz veya uyumlu tag arasında veri haberleşmesindeki mesaj formatlamasını belirler.

NDEF, uygulama tarafından istenen bir veya daha çok herhangi bir bilginin kolay bir şekilde tek bir mesaj yapısı içinde tanımlanmasına olanak sağlayan binary mesaj formatıdır. Her bir bilgi tip, uzunluk ve seçimlik bir özellik ile ifade edilir. Bu özellikler URI, MIME veya NFC'ye özgü bir özellik olabilir.

NFC RTD (Record Type Definition) bir NFC cihaz ile diğer NFC cihaz veya taglerin arasında kullanılan mesajların standart kayıt tiplerini tanımlar. Ayrıca standart internet medya tiplerini de tanımlarlar. Bazı özel tanımlı RTD'ler şunlardır:

- Akıllı Poster RTD
Yazı, ses, video veya diğer veri türleri içeren poster tagları için kullanılır.
- Text RTD
Salt metin içeren taglerin kayıt tanımları için kullanılır.
- Uniform Resource Identifier (URI) RTD
Herhangi bir internet kaynağını işaret eden kayıt tanımları için kullanılır.

4.11.3. Uçtan uca haberleşme, peer-to-peer mode

Uçtan uca haberleşme modunda çalışan bir NFC cihazı, diğer bir NFC cihazı ile haberleşme yapmaktadır. Bu haberleşme modunda her iki uçtaki NFC cihazı aktif modda haberleşmektedir. Bir Bluetooth bağlantısı gibi iki NFC cihaz arasında aktif bir bağlantı kuruşarak veri alışverişi yapılmaktadır. (Şekil 4.18)

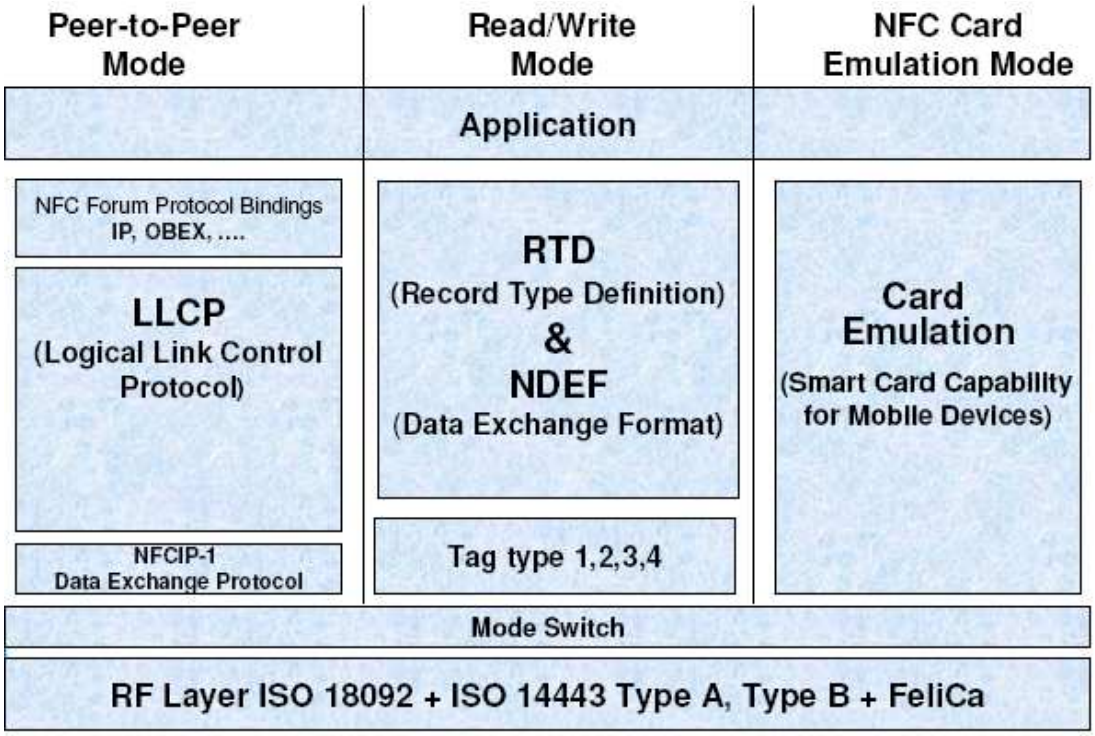
Şekil 4.18 Uçtan uca haberleşme

Diğer bağlantı türlerine gore NFC bağlantısı bazı yönlerden daha avantajlıdır. Örneğin bir Bluetooth bağlantısının kurulabilmesi için önce kullanıcıların kurulum yapması ve karşıdaki cihazı tanıtarak yetkilendirmesi gerekmektedir. Pairing denen bu işlem kullanıcı tarafından elle yapılır. Bir Bluetooth bağlantısının kurulması yaklaşık 6 saniye sürmektedir. Bunun yanında bir NFC bağlantısının kurulması 0.1 saniye civarında sürer.

Bluetooth cihazları yaklaşık 10 metre mesafeden bağlanabildiği halde NFC cihazlar 20 ila 10 cm mesafeden bağlanabilirler. Bu düşük mesafe dezavantaj gibi görülse de güvenlik açısından avantajdır. Özellikle ödeme işlemlerinde kullanıldığında, temassız bağlantının üçüncü şahıslar tarafından dinlenememesi oldukça önemlidir. Kısa mesafeli haberleşme ile üçüncü şahısların haberleşmeyi izleme imkanı azaltılarak güvenlik daha da arttıtılır.

Uçtan uca haberleşmede her iki NFC cihazı da aktif modda haberleşmektedir. Uçlardan biri Başlatıcı –Initiator- diğeri de Hedef –Target- olarak isimlendirilir.

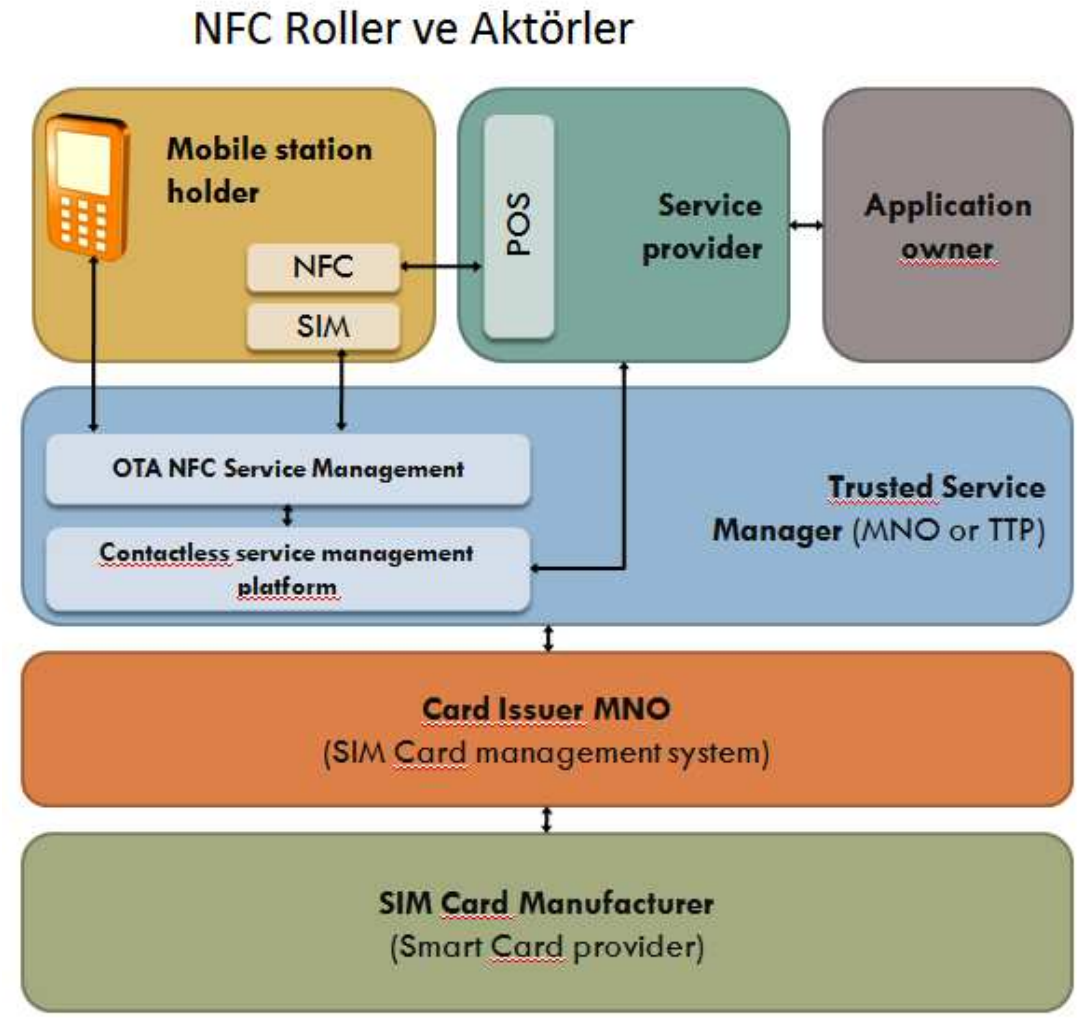
Uçtan uca haberleşme modu için NFC Forum ISO 18092 / NFCIP-1 isimli spesifikasyonu yayınlamıştır. Bu spesifikasyon NFC cihazlar arasındaki lojik linki yöneten protokolü tanımlamaktadır. (Şekil 4.19)



Şekil 4.19 Uçtan uca haberleşme modu protokolleri

4.12. NFC Sistemindeki Roller

Bir NFC tabanlı mobil ödeme sisteminin çeşitli tabakalarda çeşitli sorumlulukları ve bunların sahipleri vardır. Her bir sorumluluk ve aksiyon bu tabakalar arasında belirlidir. Şekil 4.20'de de görüldüğü gibi temel olarak NFC tabanlı bir ödeme sisteminin beş ayrı sorumluluk ve aksiyon alanı mevcuttur.



Şekil 4.20 NFC'de roller ve aktörler

Şekil 4.20'de görüldüğü gibi NFC özellikli bir mobil cihazın Servis Sağlayıcı (Trusted Service Manager) ve POS ile ilişkisi vardır. Mobil cihaz NFC arayüzünü kullanarak POS üzerindeki uygulama ile haberleşmektedir. Mobil cihaz yerleşik mobil haberleşme altyapısını kullanarak Servis Sağlayıcı ile haberleşmektedir. Mobil cihaz üzerindeki ve/veya Mobil cihaz üzerinde bulunan SE (Secure Element, Güvenli Eleman) üzerindeki uygulamalar Servis Sağlayıcının hizmete sunduğu OTA (Over-The-Air) servisleri ile dağıtılmaktadır. Mobil Servis Sağlayıcının OTA ile dağıttığı uygulamalar Kart Sahibi Kurum - Card Issuer - tarafından verilmektedir. Mobil ödeme uygulamasının kullandığı hesaplar ve güvenlik anahtarları Card Issuer tarafından yönetilirler. Kart Sahibi Kurumun kullandığı kartlar SIM kart üreticisi tarafından verilir. Yükleme ve en üst düzeyde yönetici anahtarları SIM Kart Üreticisi tarafıdan yönetilir.

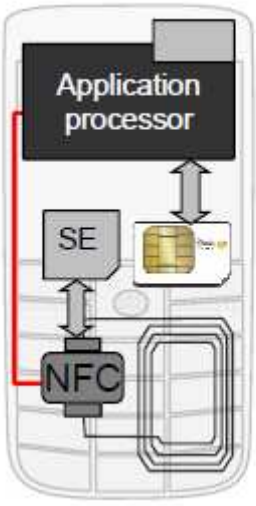
4.13. Bir Mobil Cihazda NFC Kullanım Mimarisi

Yeni nesil mobil cihazlarda kamera, GPRS, 3G, Wireless, Bluetooth, TV gibi donanım ve özelliklerle beraber artık temassız haberleşmeyi sağlayan NFC donanımı da bulunmaktadır. Piyasa araştırmaları ve üretici firmaların tahminlerine göre önümüzdeki yıllarda NFC destekli mobil cihazların pazardaki payı hızla artacaktır. Bu artışla beraber Yakın Alan Haberleşme uygulamaları da yaygınlaşacak ve çeşitlenecektir.

Üç yıl önce ABI Araştırma Şirketi 2009'a kadar dünyadaki mobil telefonların yarısının NFC uyumlu olacağını tahmin etmişti. Her ne kadar bu rakamlara ulaşılamadıysa da rakamlar hızla yaklaşmaktadır. Jupiter Araştırma Şirketi NFC destekli mobil cihazlarla yapılan ödemelerin 2012 yılında 30 milyar doları aşacağını tahmin etmektedir.

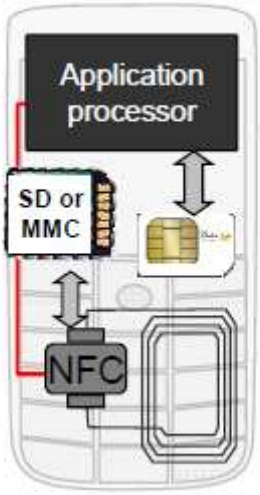
Bir mobil cihaz üzeride NFC/Güvenli Eleman mimarisi üç şekilde kurulmaktadır.

- Güvenli elemanın mobil cihaz üzerinde yerleşik olduğu mimari
- Güvenli elemanın SD veya MMC kart üzerinde sunulduğu mimari
- Güvenli elemanın SIM kart üzerinde sunulduğu mimari



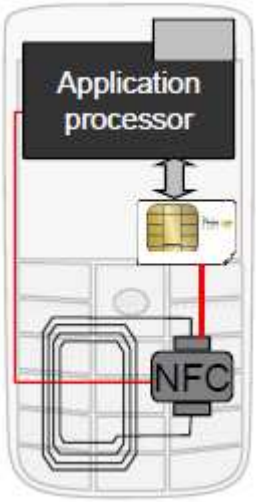
Şekil 4.21 SE mobil cihaz üzerinde

Şekil 4.21’de güvenli elemanın mobil cihaz üzeriden sunulduğu mimari görülmektedir. NFC işlemcisi mobil cihaz üzerindeki güvenli eleman ile haberleşmektedir.



Şekil 4.22 SE MCC kart üzerinde

Şekil 4.22’deki mimaride Güvenli Eleman bir SD veya MMC kart üzeriden sağlanmaktadır.



Şekil 4.23 SE SIM üzerinde

Bu mimaride de Güvenli Eleman mobil servis sağlayıcının verdiği SIM kart üzeriden sağlanmaktadır. (Şekil 4.23)

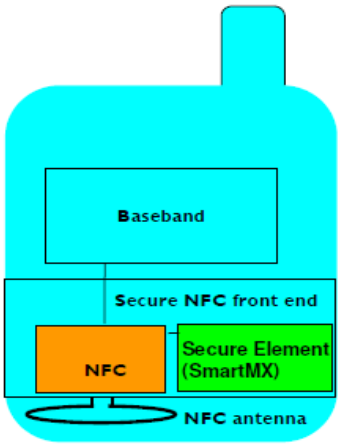
Bu mimarilerde NFC donanım mobil cihaz üzeride gömülü olarak bulunmaktadır. Mimarilerde değişen Güvenli Elemanın mobil yapı içerisinde aldığı konumdur. Güvenli eleman farklı şekillerde sağlanabilmektedir.

Bununla beraber mobil sistemdeki NFC donanım da farklı mimarilerde tasarlanabilmektedir. NFC donanım mobil sistem üzerinde gömülü olarak bulunmayabilir.

4.13.1. NFC-WI mimari

Mobil sistemde NFC donanımı ve Güvenli elemanın mobil cihaza gömülü olduğu mimariye NFC-WI ismi verilir. WI, Wired Interface veya S2C olarak da ifade edilir. NFC bileşeni hem haberleşme işlemcisini hemde çoklu uygulamalı SmartMX işlemcisini içerir. Ödeme, ulaşım gibi uygulamalar SmartMX işletim sistemi üzerinde bulunmaktadır. SmartMX işletim sistemi JCOP, Multos veya diğer çoklu uygulama işletim sistemleri olabilir. SmartMX güvenli elemanı mobil servis sağlayıcının sağladığı SIM karttan farklı bir donanımdır. Örneğin CDMA telefonlar gibi SIM kart bulundurmayan mobil sistemlerde güvenli eleman da ayrı bir donanım olmak zorundadır.

SmartMX güvenli elemanının kişiselleştirilmesi Mobil Servis Sağlayıcının hizmete sunduğu OTA servisleri ile 3G, GPRS veya EDGE bağlantılar üzerinden yapılamaktadır.

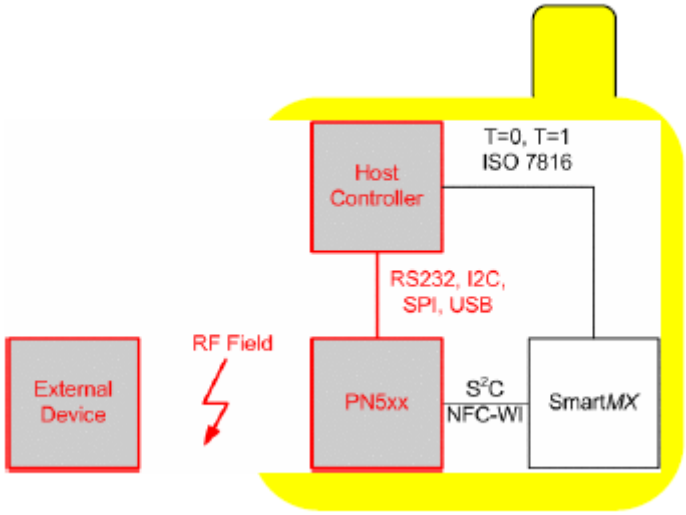


Şekil 4.24 NFC-WI mimarisi

Şekil 4.24'te bir NFC-WI mimarisi görülmektedir.

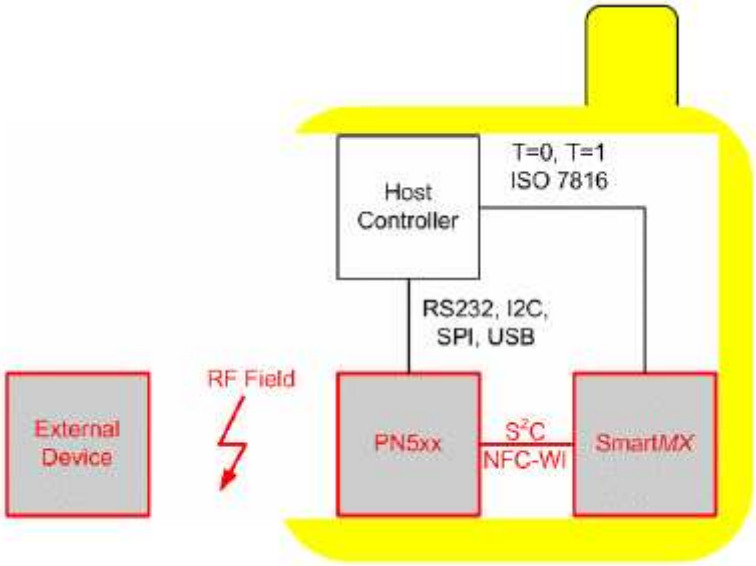
Bir NFC-WI mimarisinin mümkün olan çalışma şekilleri aşağıda gösterilmiştir.

Mod 1. Easy Connect mod. Bu mod daha once bahsedilen Peer-To-Peer modda çalışma şekli gibidir. Mobil cihaz NFC donanım üzerinden diğer NFC uyumlu cihaz ile haberleşmektedir. Mobil cihaz işlemcisi NFC işlemcisi ile RS232, I2C, SPI veya USB bağlantılardan biri ile bağlanmaktadır. (Şekil 4.25)



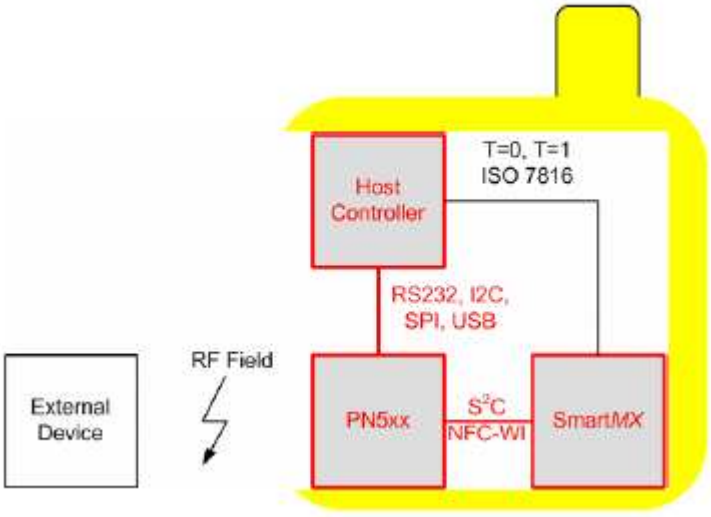
Şekil 4.25 NFC-WI mimari mod 1 çalışma tipi, Easy Connect

Mod 2. Kart Emulasyon modu. Mobil cihazın herhangi bir kontrolü olmaksızın harici NFC cihaz tarafından güvenli elemana erişim sağlanır. NFC işlemci Güvenli Elemana S2C bağlantı ile bağlanmaktadır. (Şekil 4.26)



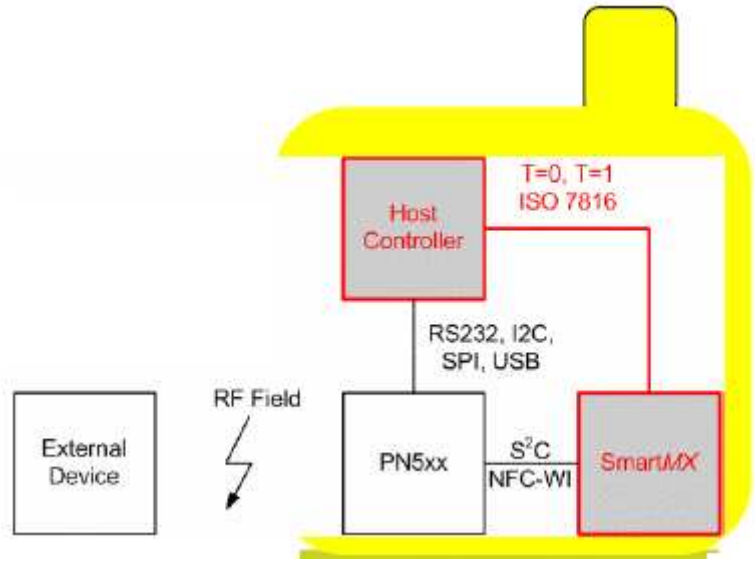
Şekil 4.26 NFC-WI mimarisi kart emulasyonu modu çalışma tipi

Mod 3.Dual mod bağlantı. Bu çalışma türünde mobil cihaz işlemcisi NFC işlemcisi ve Güvenli Eleman ile bağlantı kurmaktadır. Güvenli Eleman ile bağlantı doğrudan kurulmamakta, çalışma sırasında NFC işlemci bağlantıyı kurmaktadır. Bu bağlantıda da mobil işlemci ile NFC işlemci arasındaki bağlantı RS232, I2C, SPI veya USB olabilmekte, NFC işlemci ile Güvenli Eleman arasındaki bağlantı da S2C olmaktadır. (Şekil 4.27)



Şekil 4.27 NFC-WI mimari Dual mod çalışma tipi

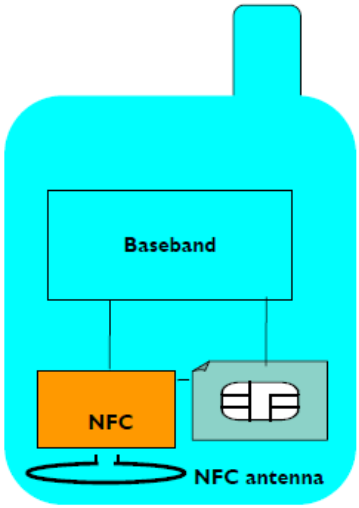
Mod 4. Wired Mod. Mobil işlemci ile Güvemli Elemanın direk bağlantıda olması. Bu çalışma şeklinde mobil işlemci Güvenli Eleman ile doğrudan bağlantı halindedir. Mobil işlemci Güvenli Eleman ile ISO 7816 protokolü ile haberleşmektedir. Bu çalışma modunda herhangi bir NFC işlemi yapılmamaktadır. (Şekil 4.28)



Şekil 4.28 NFC-WI mimari Wired mod çalışma tipi

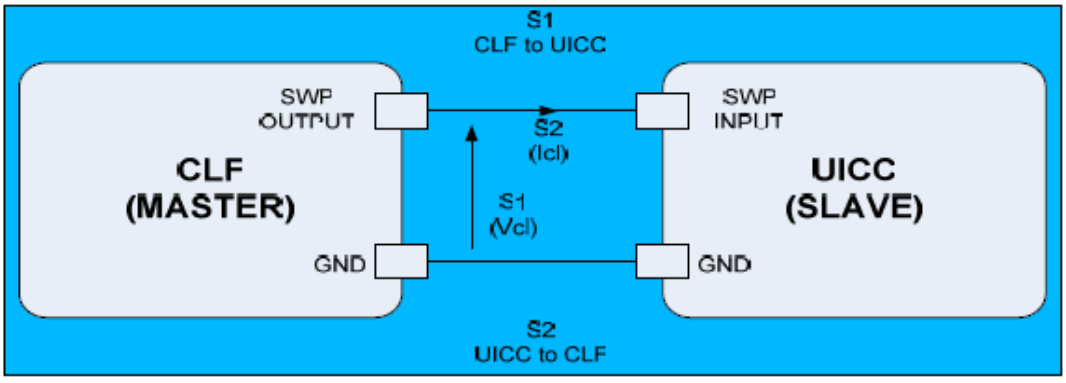
4.13.2. NFC-SWP mimari

NFC-WI mimariden farklı olarak Güvenli Eleman mobil cihaz üzerine gömülü olarak tasarlanmamıştır. NFC-SWP mimarisinde NFC işlemci ve anten donanımı mobil cihaz üzerinde gömülüdür. Ancak Güvenli Eleman SIM üzerinde bulunmaktadır. NFC işlemci ile SIM üzerindeki Güvenli Eleman Single Wire Protocol ile haberleşmektedir. NFC Single Wire Protocol 2006 Q4 standartlaştırma aktivitelerinde ele alınmıştır. Bu mimaride NFC donanımı SIM kart üzerinde bulunan çoklu işlemli JavaCard güvenli ortamından izole edilmiştir. Ödeme, ulaşım gibi uygulamalar SIM kart işletim sistemi üzerinde bulunmaktadır. Güvenli uygulamalar SIM kart sağlayıcısı tarafından yönetilmektedir. Erişim ve şifreleme anahtarları SIM kart üzeride bulunmaktadır. Güvenli Uygulamaların kişiselleştirilmeleri mobil servis sağlayıcının hizmete sunduğu OTA ile 3G, GRPS veya EDGE bağlantı üzerinden yapılmaktadır.



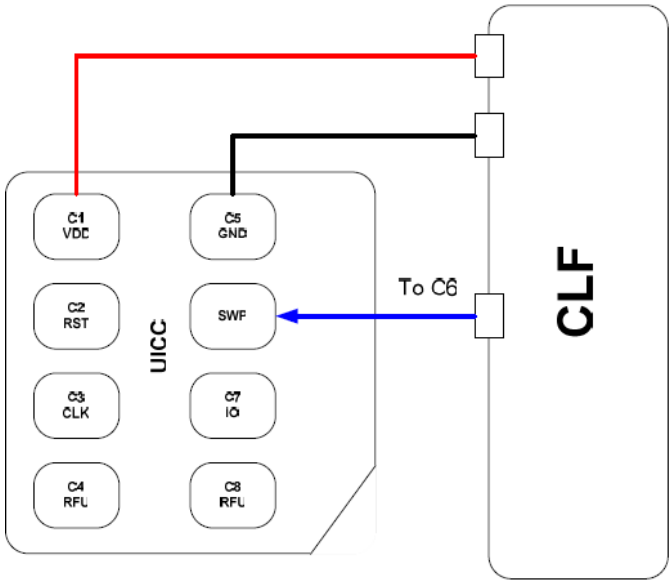
Şekil 4.29 NFC-SWP mimari

Şekil 4.29'da bir NFC-SWP mimari görülmektedir. Şekil 4.30 ve Şekil 4.31'deki UICC kısatlması SIM kart anlamına gelmektedir. Şekilde görüldüğü gibi mobil cihazın işlemcisi SIM karta tek hat üzeriden bağlanmaktadır.



Şekil 4.30 SIM kart ve mobil cihaz bağlantısı

Şekil 4.30 ve Şekil 4.31'daki CLF mobil cihazın işlemcisini ifade etmektedir.



Şekil 4.31 SIM ve mobil işlemci bağlantısı

4.14. Dünyada NFC Denemeleri

Dünyada yapılan çeşitli NFC uygulama deneyimlerinden bazıları aşağıda listelenmiştir. Halen bir çok farklı uygulama geliştirilmekte ve denenmektedir.

- Hanau (Frankfurt) – Almanya:
Toplu taşımada bilet operasyonu
2005
- Limburg (Roda Stadyumu) – Hollanda:
Bilet operasyonu
Ödeme
2005 – 2006
- Caen – Fransa:
Ödeme
Park
Turistik bilgilendirme
Toplu taşıma bilgilendirme
Akıllı poster
2005- 2006
- Atlanta – Amerika Birleşik Devletleri:

Ödeme

Akıllı poster

2005 – 2006

- Paris Metro Sistemi – Fransa:

“Navigo” seyahat kartları

2005 – 2006

- Singapur – Malezya:

Mobil Visa Ödeme, Mobile Visa Wave payment

Visa International & May Bank

2006

- Seul – Güney Kore:

Bilet uygulaması

Akıllı poster

Erişim kontrolü

2006

- Xiamen – Çin:

Bilet uygulaması

Ödeme

2006

- Manchester – İngiltere:

Manchester Şehir Stadyumu bilet uygulaması

Ödeme

2006

- Amsterdam – Hollanda:

Ödeme

Bilet uygulaması

2006

- Şangay – Çin:

Sadakat uygulama yükleme

OTA

Kullanıcılar mobil networkten sadakat uygulamalarını telefonlarının güvenli elemanına yükleyebiliyorlar.

2006

- New York – Amerika Birleşik Devletleri:

Master Card'ın OTA dağıtımı, m-Payments

Mobil telefon bazlı ödeme sistemlerinin ödeme uygulamasının güvenli kişiselleştirmesi

2003

- Strasbourg – Fransa:

NFC ödeme denemesi

2006

- Paris – Fransa:

Paris metro işletmesi RATP ve Bouygues mobile Telco arasında SWP protokolü ile bilet uygulaması denemesi

2006

- Sylt:

Turstik bilgilendirme

- Tayvan:

Toplu taşıma

- Seattle – Amerika Birleşik Devletleri:

Philadelphia & Detroit stadyumu bilet uygulaması

- Hagenberg – Avusturya:

Kampüs erişim uygulaması

- New York – Amerika Birleşik Devletleri:

NewYork metrosunda "TAP&GO" uygulaması

BÖLÜM 5. NFC‘DE GÜVENLİK

Bu bölümde NFC’nin güvenlik konuları incelenmektedir. Bu konuda çok önemli iki yayın yayınlanmıştır. Ernst Haselsteiner ve Klemens Breitfuβ, Security in Near Field Communication (NFC) isimli yayınlarında bazı durumları ve bunlar için NFC’nin güvenlik çözümlerini irdelemişlerdir. Ayrıca “Security Aspects and Prospective Applications of RFID Systems” isimli yayınlarında da bazı önemli, kullanışlı bilgiler verilmiştir.

Her şeyden önce şu iyi bilinmelidir ki yakın alan haberleşmesi birkaç santimetrelik kısa mesafeden ve kullanıcının bilinçli olarak uygulamayı kullanmasına rağmen gerçek bir güvenli haberleşmeyi garanti etmez.

Yakın alan haberleşme teknolojisine birden fazla şekilde saldırı yapılabilir. Öncelikle NFC cihazlar, tag’ler fiziksel olarak değiştirilebilir. Üzerinde RFID tag bulunan herhangi bir nesneden veya Smart Poster’den tag sökülebilir. Veya üzerine RF sinyalleri engelleyecek bir ekranlama yapılabilir. Böylece RFID tagi okuyacak NFC cihaz orjinal RFID tag’e erişemez, değiştirilmiş orjinal olmayan sahte tag ile haberleşir. Bir diğer durum da özel bilgilere erişim problemidir. Eğer kişisel, özel bir bilgi bir RFID tag içine yazılmışsa, bu bilgilerin yetkisinin okuma ve yazmalara karşı korunması gerekmektedir. Yetkisiz yazma işlemlerine karşı sadece okunabilir tag’ler güvenliği sağlayabilemektedir. Tekrar yazılabilir taglerin kullanıldığı ve saldırganın mobil okuyucuya sahip olduğu ve uygun yazılımların yüklendiği ve okuma mesafesine uygun konuşlandığı durumlarda yeniden yazılabilir tag’lere yetkiyi aşarak okuma ve yazma yapması mümkündür.

Yakın alan haberleşmesinde hataların tespiti için Cyclic Redundancy Check (CRC) kullanılır. Bu metod ile cihaza ulaşan veri paketinin bozulup bozulmadığını tespit etmek mümkündür.

Aşağıda Yakın alan haberleşmesine yapılacak çeşitli saldırılar incelenmiştir. Bir çok saldırı tipi için geliştirilmiş karşı önlemler mevcuttur.

5.1. NFC Haberleşme Güvenliği

Yakın alan haberleşmesinde ortamın yetkisiz kişilerce dinlenmesi ile gerçekleştirilebilecek saldırılar mevcuttur. Bunlar Kulak misafiri olma, taşınan veriyi bozma, taşınan veriyi değiştirme, veri enjeksiyonu ve MIM (Man-in-the-Middle) saldırılarıdır.

5.1.1. Kulak misafiri saldırısı

Yakın alan haberleşme teknolojisi kulak misafirliği için herhangi bir koruma mekanizması önermez. Temassız haberleşmede verileri taşıyan radyo dalgaları bir anten aracılığı ile saldırgan tarafından tespit edilerek taşınan veri görülebilir. Pratikte kötü niyetli bir kişi farkedilmemek için mesafesini korumalıdır. Ancak önemli olan başarılı bir şekilde kullanılabilecek olan radyo frekanslarını hangi mesafeden alınabileceği sorusuna cevap verebilmektir. Ancak bu da aşağıdaki kriterlerin durumuna göre belli olabilecek bir çözümdür. Aşağıda sağlıklı bir şekilde ortamdaki radyo dalgalarını izleyebilmek için gerekli olan bazı unsurlar zikredilmiştir.

- Sinyal gönderen cihazın radyo frekanslarının alanın karakteristiği. Anten geometrisi, PCB, ortam özellikleri gibi.
- Saldırganın kullandığı antenin karakteristikleri. Anten geometrisi, her üç yöne göre aldığı pozisyon gibi.
- Saldırganın kullandığı alıcının kalitesi ve verimliliği.

- Saldırganın kullandığı radyo frekansı sinyal çözücüsünün kalitesi ve verimliliği.
- Saldırganın işlem sırasında bulunduğu konum. Duvar gibi bir bariyerin arkasında bulunması, ortamdaki metal eşyaların pozisyonları.
- Hedefteki NFC cihazın harcadığı güç.

Bunlarla beraber kulak misafirliği tekniği en çok haberleşme modundan etkilenir. Haberleşme modunda, aktif veya pasif haberleşmeye göre taşınan veriler farklı şekilde kodlanır ve modüle edilir. Eğer gönderilen veri güçlü bir şekilde modüle edilmişse daha kolay saldırılabilir. Bu yüzden kendi elektro manyetik alanını üretmeyen pasif cihazlara saldırmak, kendi elekro manyetik alanını üreten aktif cihazlara nazaran çok daha zordur. Kabaca saldırı için verilen mesafeler için şu ifade kullanılmıştır. “Eğer bir cihaz aktif modda veri gönderiyorsa, kulak misafirliği saldırısı yaklaşık 10 metreden gerçekleştirilebilir. Eğer veri gönderen cihaz pasif modda haberleşiyorsa mesafe kayda değer şekilde düşerek kulak misafirliği saldırısı 1 metre civarında gerçekleştirilebilir.”

Bir saldırının gerçekleştirilebilmesi için gerekli olan tüm donanım herkes tarafından erişilebilirdir. Gerekli olan anten tertibatı ve uygun yazılımlarla mücehhez kötü niyetli bir kişi ortamdaki radyo frekanslarını dinleyerek içerisindeki veriye ulaşabilir. Bu tür bir çalışma yapılabilmesi için gerekli bilgi kaynağı da açık ve erişilebilirdir. Bu yüzden NFC’nin güvenliği garanti edilmez. Korunması gereken değerli verilerin taşınması için güvenli kanalın (Secure Channel) kullanılması tek çözüm yoludur.

5.1.2. Veri bozma

Bu tür saldırıda saldırganın hedefi haberleşmedeki verilerin bozularak haberleşmenin kesilmesidir. Bunun sonucu verilen hizmetin kesilmesidir. RFID tag veya Smart Poster veya herhangi bir NFC cihaz artık hizmet veremez duruma gelir. Bu saldırı çeşidinde saldırgan her hangi bir geçerli, uygun mesaj oluşturmaz. Kulak misafirliği saldırısına nazaran Veri Bozma saldırısı pasif bir saldırı değildir. Geçerli bir paket

oluşturma zorunluluğu olmadığı için bu tür bir saldırıyı gerçekleştirmek diğerlerine nazaran daha kolaydır. Yakın alan haberleşmesinde kullanılan sinyalleri bozmanın bir yolu RFID Sinyal Karıştırıcı (RFID Jammer) kullanmaktır.

Bu tarz bir saldıyı önlemenin herhangi bir yöntemi yoktur. Fakat bu tarz bir saldırı tespit edilebilir. NFC cihazlar aynı anda hem veri gönderebilir hemde veri alabilir. Bu da NFC cihazların elektro manyetik alan kontrol ederek çakışmayı tespit etmesine imkan sağlar. NFC cihaz haberleşme sırasında ortamdaki radyo sinyallerini dinleyerek başka bir vericinin olup olmadığını anlayabilir.

5.1.3 Veri değiştirme

Yakın alan haberleşmesinde taşınan verinin her hangi bir yetki olmaksızın okunup değiştirilerek geçerli bir mesaj halinde gönderilmesi şeklinde yapılan bu saldırı çok daha fazla karmaşıktır ve tüm protokol ve haberleşme tekniğinin çok iyi bilinmesine ihtiyaç duyar. Taşınan veriyi değiştirmeyi hedefleyen saldırgan radyo frekansı sinyalindeki bitlerin her biri ile ilgilenmek zorundadır. Haberleşmede gönderilen veri farklı yollardan gönderilmektedir. Bu tür saldırının verimliliği yani bir bitin sıfırdan bire veya birden sıfıra çekilmesi, yapılan modülasyonun gücü ile ilgilidir.

Eğer %100 modülasyon kullanılmışsa, bir radyo frekansı sinyalinin durdurulmasını bertaraf etmek mümkünken herhangi bir duraklama yoksa onu üretmek mümkün değildir. Bu da alıcının anteni üzerinde orjinal sinyal ile saldırganın gönderdiği sinyalin, mümkün olamayan, tam olarak çakışmasını gerektirir. Yinede Yakın alan haberleşmesi teknolojisi Modified Miller kodlamayı %100 modülasyon ile kullanır. Modified Miller kodlamanın Şekil 5.1'de görüldüğü gibi mümkün olan 4 durumu vardır. Sadece 1 değerli bir bitten sonra tekrar 1 değerli bir bit geliyorsa saldırgan bu bitin değerini değiştirebilir. Radyo frekansı sinyalindeki iki yarım bitin arasına boşluk bırakılırsa mesajı alan taraf bu biti üçüncü durumdaki gibi algılayacaktır. Bir

önceki bitin değerini alıcı taraf kabul ettiğinden dolayı bu da onaylanacaktır. Diğer üç durum bir saldırı için uygun değildir.

Bit x-1	Bit x	Bit-x'in değişimi	Saldırıya uygun
0	0	1	Hayır
0	1	0	Hayır
1	0	1	Hayır
1	1	0	Evet

Şekil 5.1 Modified Miller Code bit modifikasyonu

NFC'de %10 modülasyon her zaman Manchester kodlama ile birlikte kullanılır. %100 modülasyonun aksine bir duraklama aralığında alıcıya gerçekten hiç bir sinyal gönderilmez. Radyo frekansı sinyalindeki bu duraklamalar ile tam sinyal seviyesinde %82 olur. Bir saldırganın tüm haberleşme oturumu boyunca, alıcının hiç farketmeden, varolan radyo frekansı sinyalini %18 arttırdığını kabul edelim. Daha sonra saldırgan RF sinyali arttırarak bit biti sıfırdan bire , sinyali keserek de birden sıfıra set edebilir.

Özetle; bir durum hariç NFC veri transferinde daima %10 ASK Manhester kodlama kullanılır. Bu da saldırının yapılabilmesi için en iyi imkanı oluşturur. Bu tarz haberleşme tüm bitlerin değiştirilebilmesine olanak sağlar. Tek istisnası aktif cihazların 106 kbps'de haberleşmesidir. Bu durumda %100 modülasyonlu Modified

Miller kodlama kullanılması sadece belli bitlerin değiştirilmesi şeklinde saldırıyı kısıtlar.

Güvenlik için aktif cihazların 106 kbps haberleşmeyi kullanmaları saldırıya karşı savunmayı arttırır. Bu gönderilen verinin değiştirilmeriskini tamamen ortadan kaldırmasa da saldırı riskini azaltacaktır. Daha savunma için cihazların ortamdaki radyo frekansı sinyallerini dinlemesi tercih edilmelidir. En iyi çözüm ise Güvenli Kanal, Secure Channel kullanılmasıdır. Bu yöntem veri güvenliğini ve doğruluğunu sağlayacaktır.

5.1.4. Veri enjeksiyonu

Bu tür saldırı sadece gerçek cihazın kendi mesajını göndermeye başlamadan önce yeterli bir süre varsa gerçekleştirilebilir. Eğer bir çakışma gerçekleşirse veri transferi bir defa için kesilir. Bu tür bir saldırıyı önlemek için NFC cihaz her hangi bir gecikme olmaksızın cevap vermeye çalışmalıdır. Ayrıca radyo frakensı alanının tekrar kontrolü veya güvenli kanal (Secure Channel) kullanımı da bu saldırıyı önlemek için kullanılabilir.

5.1.5. Man-in-the-Middle saldırısı

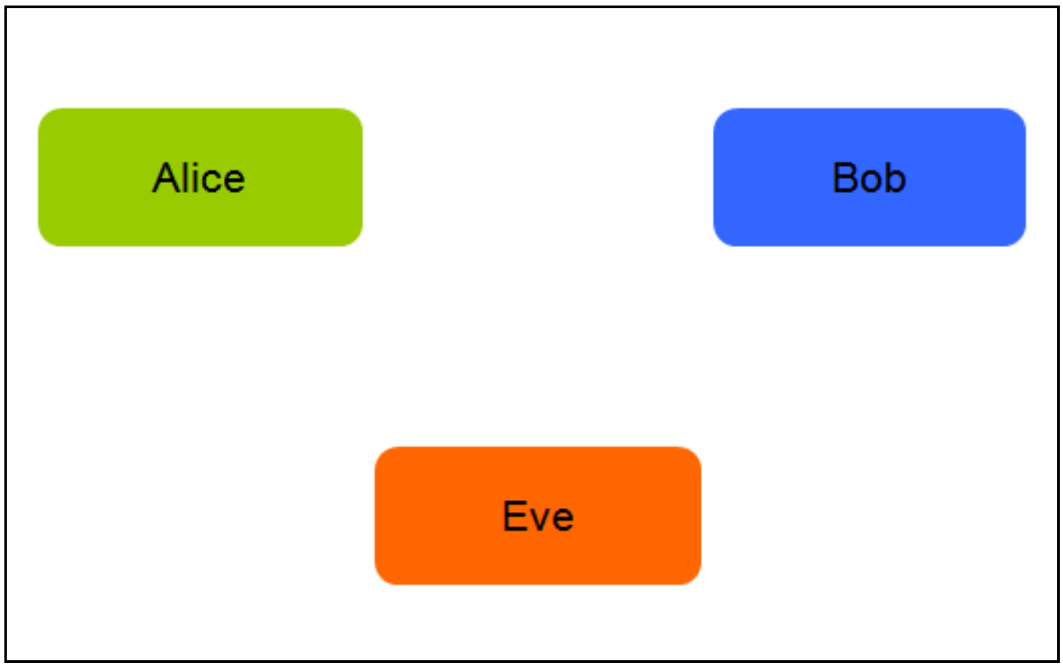
Yakın alan haberleşmesinin Man-in-the-Middle saldırısına karşı güveli olduğunu göstermek için hem aktif haberleşme modunu hem de pasif haberleşme modunu inclemek gerekmektedir. Aşağıda A ve B birbirleri ile yakın alan haberleşmesi ile veri gönderip almak isteyen iki ayrı cihazdır.

Pasif modda, aktif olan A cihazı pasif olan B cihazına veri göndermek için kendi elektro manyetik alanını oluşturur. Bu haberleşmede davetsiz misafir olan

saldırganın hedefi bu mesajı yakalamak ve B'nin mesajı almasını önlemektir. Bir sonraki adım bu orjinal mesajın yerine değiştirilmiş başka bir mesajı göndermektir. Birinci adımı gerçekleştirmek mümkündür. Fakat eğer A cihazı mesaj göndeririken ortamdaki radyo frekansını dinliyorsa bu saldırı tespit edilebilir. Ancak ikinci adım pratikte mümkün değildir. B cihazına bir mesaj gönderebilmek için saldırgan kendi elektro manyetik alanını üretmek zorundadır.

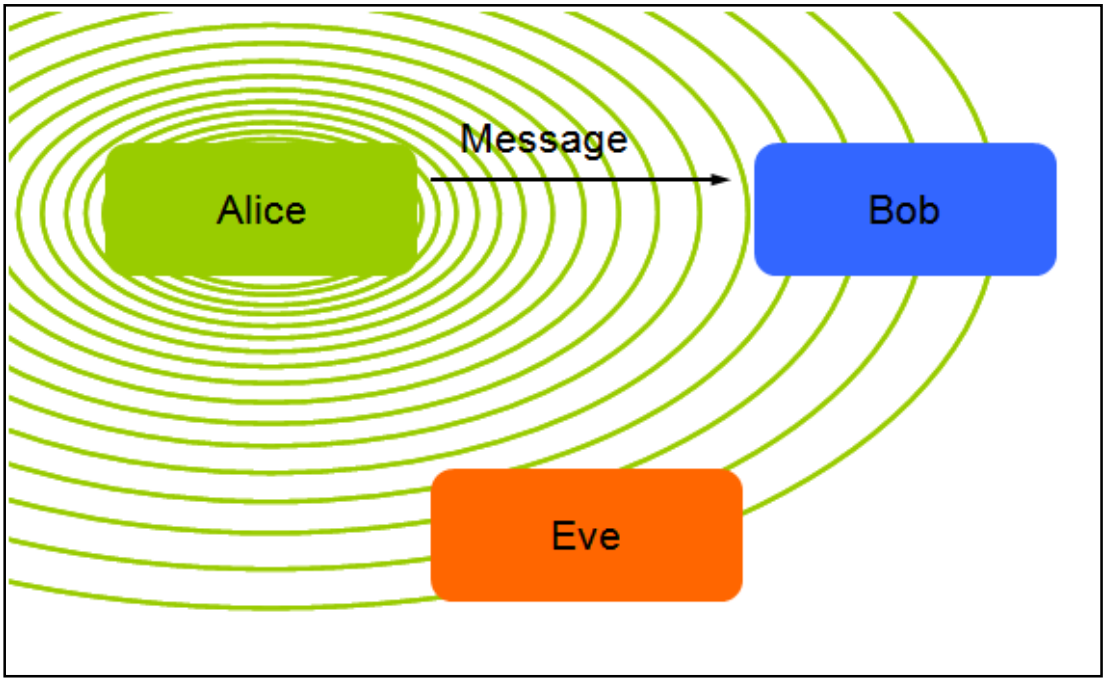
Pasif modda haberleşmenin aksine, aktif moddaki A cihazı mesajını gönderdikten sonra elektro manyetik alanını kapatır. Bu durumda artık saldırgan başka bir problemle yüzyüzedir. Saldırgan mesajını göndermek için kendi elektro manyetik alanını üretebildiği halde B cihazına herhangi bir mesaj gönderemez. Çünkü A cihazı mesajını gönderdikten sonra B cihazından cevap beklemektedir. Bu yüzden A cihazı gelen mesajın gerçekten B'den geldiğini doğrulayacak bir görevi yapmaktadır.

Bir Man-in-the-Middle saldırısı ve sonuçları aşağıdaki şekillerde gösterilmiştir. Yayınlardaki isimlendirmelere benzer olarak haberleşmeyi yapan taraflar Alice ve Bob olarak, davetsiz misafir olan saldırgan ise Eve olarak isimlendirilmiştir. Şekil 5.2'de haberleşme ve saldırıın tarfları gösterilmektedir.



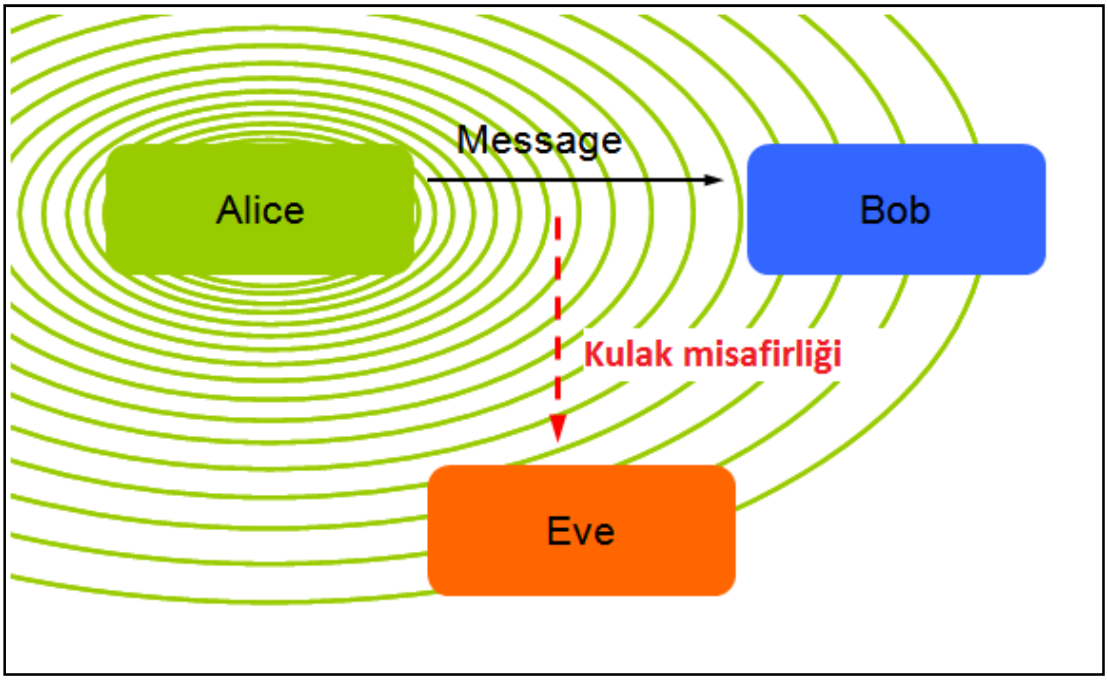
Şekil 5.2 MIM saldırısında taraflar

Alice kendi elektro manyetik alanını oluşturarak mesajını Bob'a gönderir. Şekil 5.3'de bu işlem gösterilmektedir.



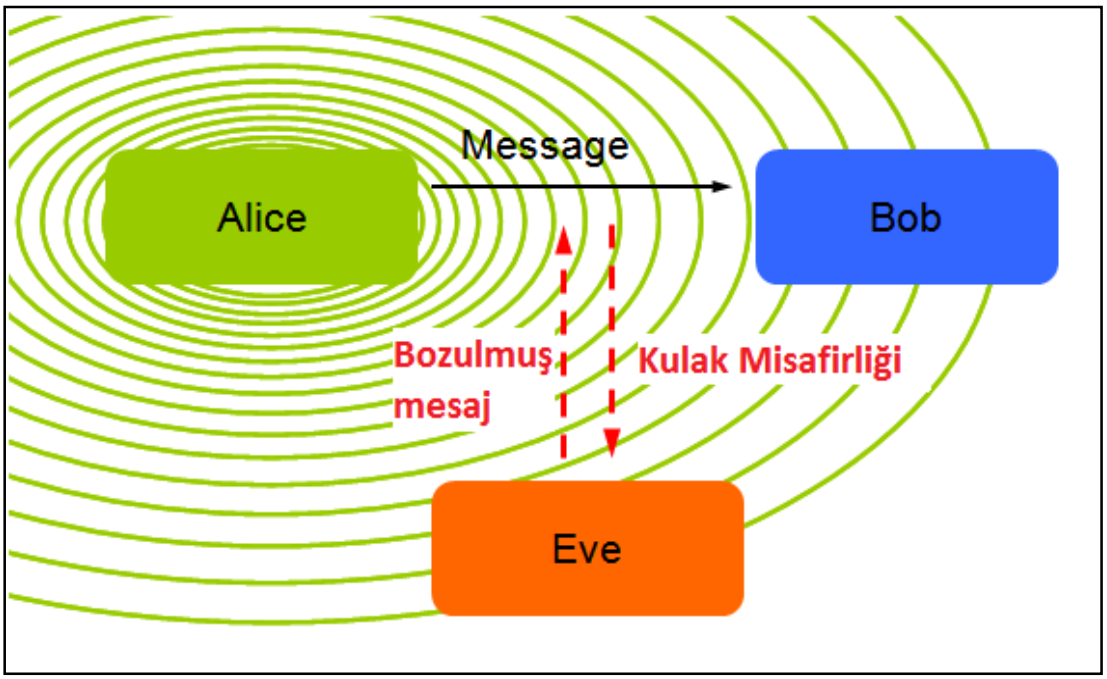
Şekil 5.3 Alice Bob'a mesaj gönderir

Şekil 5.4'de gösterildiği gibi Eve ortamı dinleyerek Alice'in Bob'a gönderdiği mesajı yakalar.



Şekil 5.4 Eve mesajı yakalar

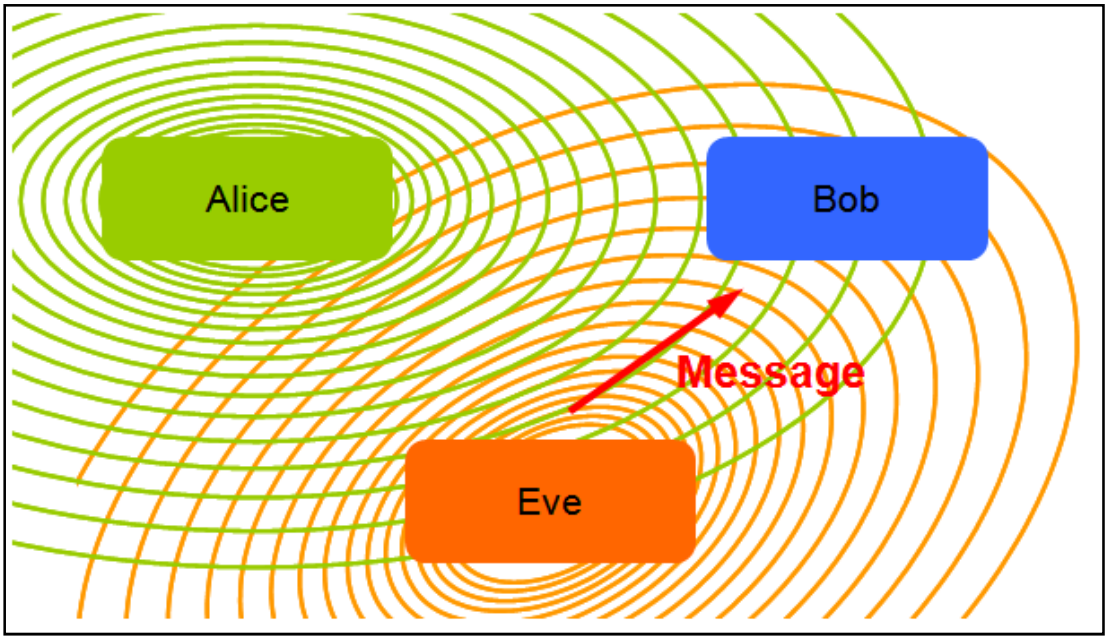
Eve kendi mesajını oluşturur. (Şekil 5.5)



Şekil 5.5 Eve mesajı bozar

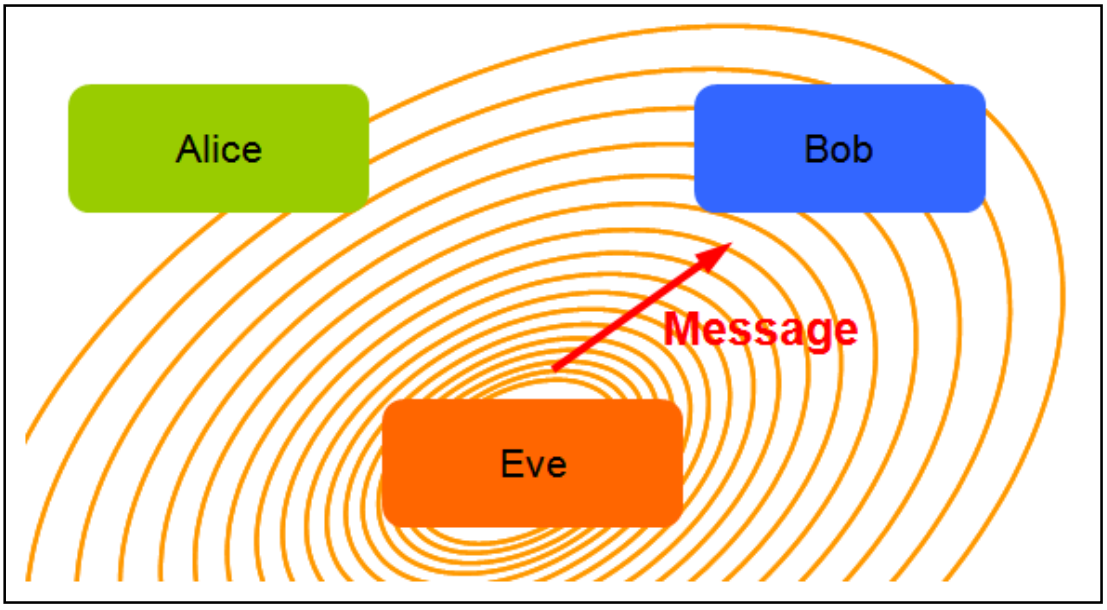
Bu aşamada Alice mesajdaki bozukluğu farkeder ve protokolü durdurur. Bu karışıklık izleme protokol seviyesinde gerçekleştirilmektedir.

Eve kendi elektromanyetik alanını oluşturarak mesajını Bob'a göndermeye çalışır. (Şekil 5.6)



Şekil 5.6 Eve mesajı Bob'a gönderir

Ancak Alice'in elektro manyetik alanı aktifken Eve Bob'a mesaj gönderemez. Alice elektro manyetik alanını kapatsa da Eve'nin göndermiş olduğu mesajı alabilir. (Şekil 5.7)



Şekil 5.7 Alice Eve'nin mesajı alabilir

Alice aldığı mesajı doğrulayarak bunun bir saldırı olup olmadığını tespit edebilir.

Man-in-the-Middle saldırılarına karşı Alice'in yapması gerekenler:
- 106 kBaud haberleşme hızını seçmelidir.
- Alice aktif, Bob pasif modda haberleşmelidir.
- Alice mesaj karışıklığını kontrol etmelidir.
- Alice, Bob'dan gelen şüpheli mesajları kontrol etmelidir.

Sonuç olarak NFC, kulak misafirliği saldırısına ve veri bozma saldırısına karşı bir güvenlik garantisi vermez. Bu saldırılara karşı Secure Channel kullanılmalıdır. Ancak kulak misafirliği gibi ortam dinleyerek yapılacak saldırılar, yakın alan haberleşmesinin kısa mesafeden yapılıyor olmasından dolayı büyük ölçüde elenirler. Man-in-the-Middle türünden bir saldırı da NFC'nin fiziksel özelliklerinden dolayı gerçekleştirilemez.

5.2. Mobil Uygulamaların Güvenliği

NFC'de bir diğer güvenli konusu da mobil NFC uygulamalarının güvenliğidir. Akıllı kart dünyası güvenlik ile tamamen içi içe gelişmiştir. Ödeme sistemlerinde veya güvenlik gerektirecek diğer işlemlerde akıllı kartlar işlemi yavaşlatacak ve ayrıca daha çok maliyete sebep olacak çevrim içi bağlantılara ihtiyaç duymadan güvenlik konusunda gerekli olan ihtiyacı sağlamak üzere geliştirilmiştir. Akıllı kartlar işlemlerin yapıldığı anda çevrim içi bağlantı olmaksızın gerekli denetimleri yaparak güvenliği sağlayabilirler. Akıllı kart üreticileri bu tüm güvenlik ihtiyacını sağlayacak olan akıllı kart işletim sistemini (COS, Card Operating System) geliştirmiş ve ürettikleri geliştirme araçları ile uygulama geliştiricilerin hizmetine sunmuşlardır. Akıllı Java kartların ortaya çıkması, güvenli akıllı kart uygulamalarının geliştirilmesi sorumluluğunu Akıllı Kart İşletim Sistemi geliştirenlerden alıp akıllı kart uygulaması üreten geliştiricilere yüklemiştir. Günümüzde NFC mobil cihazların ortaya çıkması ile "süper akıllı kart" haline gelen ve hem bir akıllı kart hem de bir terminal olarak kullanılabilen mobil telefonlar daha önemli hale gelmeye başlamıştır. Bu yönelimle beraber bir çok uygulama geliştiricisi akıllı kart teknolojileri ve güvenlik konularını bilmese de NFC mobil cihazları programlamayı hedeflemektedir. Akıllı kartların

güvenliğini ve akıllı kart uygulamalarının güvenliğini çok iyi bilmeden yapılacak uygulama geliştirmeleri bir çok güvenlik açığı ve tuzaklara sebep olacaktır.

Güvenlik genellikle çok az geliştiricinin bildiği ve güvenlik açığı ortaya çıkmadan önce pek de düşünülmeyen bir konudur. Güvenlik sorunlarını çözmek oldukça maliyetli ve zaman alıcı konulardır.

Aşağıda Akıllı Kart İşletim sisteminde kullanılan güvenlik prensipleri ve kavramlar ile daha güvenli bir NFC mobil uygulaması yazılması için önerilen yöntemler sıralanmıştır.

5.2.1. Internal authentication

Bir akıllı kart uygulaması aynı zamanda bir akıllı kart kimlik doğrulaması anlamına da gelir. Bir mobil NFC uygulamasında, üzerinde çalıştığı mobil cihazın kimliği doğrulanmış, onaylanmış bir cihaz olduğu denetlenir. Bu işlem genel olarak şöyle yapılır: Doğrulayacak olan harici ortam rasgele bir sayı üreterek gönderir. Rasgele sayıyı alan hedef bu sayıyı kendi üzerindeki anahtarlar ile şifreleyerek geri gönderir. Bu şifrelemede kullanılan anahtarlar internal authentication key olarak isimlendirilir. Şifrelenmiş rasgele sayıyı alan harici taraf aldığı veriyi kendi anahtarları ile açarak ilk gönderdiği rasgele sayı ile karşılaştırır. Eğer ilk gönderdiği rasgele sayı ile karşı taraftan aldığı şifrelenmiş mesajdan çıkartılan rasgele sayı aynı ise karşı tarafın kimliği doğrulanır.

5.2.2. External authentication

Bu tip kimlik doğrulamada, kimliği doğrulayacak taraf belli bir karakter dizisi bekler. Kullanıcıdan alınan bu bilgi external authentication key'ler kullanılarak şifrelenir. Akıllı kart şifreyi açtıktan sonra gelen mesajı karşılaştırarak onayını verir. Bu işlem belli sayaçlar ile belli sayıda yapılır. Akıllı kartlarda kullanılan PIN kodu buna bir örnektir. PIN girişi genellikle 3 deneme ile sınırlandırılmıştır. 3 başarısız external authentication denemesinden sonra akıllı kart bloke olur.

5.2.3. Güvenli kanal için oturum anahtarı

Başarılı Internal authentication ve External Authantication işlemlerinden sonra iki uç arasında güvenli kanal (Secure Channel) kurulur. NFC mobil cihaz ile harici cihaz arasında bağlantıda güvenli oturum kurulurken oturum rasgele sayısı kullanılmasıyla oturum anahtarı ile veri güvenliği (şifreleme) ve veri doğruluğu (MAC) sağlanır. Oturum anahtarı (Session Key) NFC mobil cihaz ile harici cihazın ürettikleri bir rasgele sayı kombinasyonudur. Bu oturum anahtarı üretilirken NFC cihaz ve harici cihaz, ürettikleri rasgele sayıları paylaşırken mesajları açık olarak göndermezler. Mesajı açık olarak göndermek önemli bir güvenlik açığı olurdu. Bu rasgele sayılar Internal ve External authantication key'ler kullanılarak şifrelenir ve gönderilir.

Güvenlik anahtarı kullanımı – Non replay-able data integrity

Oturum anahtarı, Session Key, haberleşme sırasında gerçekleşebilecek olan verinin bozulması veya karıştırılmasına karşı veri bütünlüğünü sağlamak üzere mesajda kullanlır. Buna MAC ismi de verilir, Message Authentication Cryptogram. MAC kullanılırken her bir mesajda yeni bir MAC hesaplanarak gönderilir. Böylece MAC'in tekrar kullanımı önlenmiş olur. Tekara kullanılan MAC kriptogramı güvenlik açığına sebep olur.

Güvenlik anahtarı kullanımı – Non replay-able data confidentiality

Eğer veri gizliliği gerekli ise oturum anahtarı, Session Key, verinin şifrelenmesinde de kullanılabilir. Karşı tarafa gönderilecek olan mesajlar oturum anahtarı ile şifrelenir. Mesajı alan taraf da aynı oturum anahtarına sahip olduğundan gelen mesajı açabilir.

5.2.4. Her işlem için ayrı anahtar

Güvenlik prensiplerinden biri de bir güvenlik anahtarının sadece ve sadece belli bir işlem için kullanılıyor olmasıdır. Aslında aynı prensip günlük hayatta da kullanılmaktadır. Ev anahtarları, dolap anahtarları, araba ve garaj anahtarları hepsi

birer güvenlik anahtarıdır ve hepsi birbirinden farklıdır. Her birinin sadece bir amacı vardır. Eğer bir anahtar birden fazla güvenlik ihtiyacı için kullanılırsa bu bir güvenlik açığı oluşturur. Bu yüzden sistemde internal authenticatin key, external authentication key ve session key gibi haberleşme güvenliği ve credit key, debit key, device transaction signature key gibi veri doğruluğu anahtarları gibi bir çok güvenlik anahtarları vardır. Bunların her birinin kullanım alanları ve hedefleri birbirinden farklıdır. Bir anahtarın sadece bir görevi vardır.

5.2.5. Anahtar türetimi

Tüm sistem içinde bir çok çeşitli, farklı cihaz vardır. Anahtar türetimi mümkün olduğu müddetçe her bir cihaz için üretilen anahtarlar sayesinde her bir cihaz tekil olur. Her bir cihaz için tekil anahtar türetimi master key ve cihaz tekil ID'si (device unique ID) kullanılarak gerçekleştirilir.

5.2.6. Değerli verilerin güvenliği

Değerli verilerin güvenliği NFC uygulamalarında çok önemlidir. Bu yüzden bu verilerin güvenliğini sağlama tekniklerini bilmek de çok önemlidir. Ödeme sistemlerinde bir çok değerli veri vardır. Örneğin mobil cüzdan sahibinin adı, bağlı olduğu bankanın bilgileri gibi. İşlemler sırasında üretilen kriptogramlar ile bu değerli vreilerin güvenliği sağlanmalıdır.

5.2.7. Debit ve credit erişim hakları

Credit ve Debit için erişim metodu aynen bir veri dosyasına yazma ve dosyadan okuma erişim hakkı gibidir. Bir Debit işlemi sadece saklı olan bakiye tutarından belli bir miktarı düşürür. Credit işlemi ise Debit işleminin tersine saklı olan bakiye tutarına ilave yapar. Debit işlemi basit bir satış işlemi gibidir. İşlem yapıldıkça bakiyeden düşülür. Credit işlemi ise yine basit bir kredi yükleme, bakiye yükleme işlemi gibidir. Bu işlem de yapıldıkça tutulan bakiye miktarı artar. Debit ve Credit işlemlerini yapma hakkı alabilmek için öncelikle sisteme kimlik doğrulama yapılmalıdır. Debit ve Credit işlemleri ancak bundan sonra yapılır.

5.2.8. Kara liste yönetimi

Bir ödeme sistemi mutlaka bir kara liste takibi yapmalıdır. Bu kara listede daha önceden herhangi bir kuşkulu ödeme işlemi yapan veya sahtecilik teşebbüsü bulunan kartların bilgileri tutulur. Bu karaliste ödeme terminali kullanıma geçmeden önce mutlaka güncellenmelidir. Karalisteye dahil olan elektronik cüzdan veya akıllı kartın işlem yapması engellenmelidir.

5.2.9. Terminal işlem imzası

Ödeme sistemine sahip olan banka veya kurum ödeme terminallerini üyesi olan işyerlerine sağlar ve ödeme işlemlerini üye işyerinin adına takip eder. Banka veya kurum, ödeme terminaliden gelen işlemin bozulmadığından veya daha önce tekrar gönderilmediğinden emin olmalıdır. Bu yüzden terminal işlem imzası ödeme terminali tarafından üretilerek ödeme işlem kaydındaki tüm detay bilgilerin güvenliğini sağlar.

5.2.10. Debit imzası

Debit imzası, ödeme terminali tarafından elektronik cüzdandan doğru miktarda debit işlemi yapıldığını gösteren, onaylayan bir kriptogramdır. Teknik olarak, debit imzası işlem tutarı ve terminal işlem imzasının elektronik cüzdan içinde debit signature key kullanılarak şifrelenmesi ile üretilir. Bakiye değeri eş zamanlı olarak debit imzası üretilirken düşürülür. Bu iki işlem atomik olmak zorundadır.

5.2.11. Debit imzasının doğrulanması

Ödeme terminali herhangi bir sahtekarlığı önlemek için bu debit imzasını doğrulamalıdır.

5.2.12. Credit sertifikası

Harcama yapıldıkça bakiye toplamı düşer. Bazı zamanlarda bakiye toplamı belli bir eşik seviyesinin altına düşer ve bakiye yüklenmesi ihtiyacı doğar. NFC mobil cihazlar bakiye yükleme işlemi için iyi ve etkili bir ağ erişim imkanı sunar. Bakiye yükleme işlemi için güvenlik mekanizması, hesapları takip eden arka ofis uygulamasının oluşturduğu ve sadece bir defa kullanılabilecek olan bir sertifikaya ihtiyaç duyar. Sertifikanın kullanımı ardından uygun yükleme değeri hesabından düşülür.

5.2.13. İşlemler sonrası denetim ve inceleme

Akıllı kartlar ve NFC mobil cihazların sağladığı güvenlik sayesinde ödeme terminallerinde yapılan işlemler işlem gerçekleştikten sonra, hesapları takip eden sisteme çevrim dışı olarak gönderilebilirler. Tüm işlemlerin gönderimi ve gün sonu yapıldıktan sonra arka ofis uygulması tüm işlem hareketlerini kontrol eder. Eğer işlemlerde bir şüphe veya sahtekarlık varsa elektronik cüzdan uygulaması kara listeye alınır.

Sonuç olarak, NFC mobil uygulamalarında değerli verilen işletilmesi gittikçe popülerleşmektedir. Bu yüzden güvenliği de önemli olmaktadır. NFC ürün geliştiriciler güvenlik sistemini doğru şekilde nasıl kullanacaklarını bilmek zorundadırlar. Özellikle yapılan işlemler çevrim dışı, offline gerçekleşiyorsa. Uygulama geliştiriciler hem internal authentication'ın hem de external authentication'ın NFC mobil cihaz ile Akıllı kartın baerleşmesi sırasında veri güvenliğini nasıl sağladığını iyi bilmeliler.

BÖLÜM 6. NFC UYGULAMA GELİŞTİRME ORTAMLARI

NFC uygulamalarının geliştirilmesi için çeşitli ürünler geliştirilmiştir. NFC uyumlu cihazlar genellikle mobil cihazlardır. Mobil cihazlar platformları, işletim sistemleri ve mimarileri açısından çok çeşitlilik gösterirler. Farklı üreticiler mobil cihazlarda Linux, Microsoft Windows Mobile, Android ve Symbian gibi çeşitli işletim sistemleri kullanmaktadırlar. NFC cihazlar için C gibi dillerle native kodlar geliştirilse de farklı platformlarda uygulamanın çalışması için Java tercih edilmektedir.

Giderek hayatımızda daha çok yer almaya başlayan cep telefonu, kişisel cep bilgisayarları, POS cihazları, televizyon yayın kutuları gibi çeşitli kategorilerden cihazların temelde benzer noktaları olmalarına rağmen yaptıkları işler nedeniyle kendilerine özgü nitelikleri vardır. Bu cihazlar bildiğimiz bilgisayarlardan farklı olarak teknik özellikleri (hafıza, işlem gücü, ekran çözünürlüğü vb.) daha az güçlü ve daha özel konuları hedeflemektedirler.

Bu tip cihazların sayıları hızla artmaktadır ve bu cihazlar devamlı olarak bir networke bağlı olarak hedefledikleri alanlardaki gerekli bilgiye ulaşabilmektedirler. Böylece görünüş ve fonksiyon olarak farklı olan cihazlar temelde birbirlerine bağlı olabilmektedirler.

Çok çeşitli sayıda cihaz için bir ortak uygulama çalıştırma ortamı sağlamak ancak tüm yapıların ortak olarak kabul ettikleri standartlar üzerine kurulabilir. Bu tip cihazların bir ağ içerisinde olmalarının en önemli getirilerinden birisi de kişiselleştirmeyi kolaylaştırmasıdır. Şu an en çok cep telefonlarında öne çıkan bu

özellik ile cep telefonu sahipleri telefonlarına oyunlar, çeşitli uygulamalar yükleyerek telefonlarını kişiselleştirebilmektedirler.

Çok çeşitli cihazlar üzerinde aynı uygulamanın çalışabileceği bir ortamı oluşturabilmek için cihazlar üzerinde bir uygulama çalıştırma ortamı oluşturmak gerekmektedir. Geniş kullanım alanları, ve genişletilebilirlik özellikleri ön plana çıkan Java bu amacı oluşturmak için en iyi ortam olarak görülmektedir.

Sun Microsystems firması hızla gelişen bu alandaki ihtiyacı karşılamak için Java teknolojisinin kapsamını genişletti ve J2ME'yi oluşturdu.

J2ME, cep telefonları, kişisel asistanlar (PDA), TV kutuları, telematik sistemler gibi görüntü, hafıza ve işlemci gücü olarak kısıtlı olan bütünleşik cihazlar (embedded devices) için geliştirilmiş olan bir Java ortamıdır. Aynı J2EE (Java Enterprise versiyonu), J2SE (Java Desktop versiyonu) ve SmartCard / JavaCard gibi J2ME'nin API ve bileşenlerinin (MIDP, CLDC gibi) standartları da bir çok cihaz üreticisi, yazılım geliştirici ve servis sağlayıcının üyesi olduğu JCP tarafından belirlenen JSR'larda tarif edilmiştir.

J2ME'nin sağladığı ortak uygulama çalıştırma ortamı, J2ME sınıfları kullanılarak geliştririlmiş olan uygulamaları cihaz üzerinde çalıştırma işlevini yerine getirir. Tabii ki her Java ortamının ortak bileşeni olan Java Sanal Makinesi de J2ME'nin temel bileşenidir.

J2ME; hafıza, işlemci ve görüntü özellikleri açısından kısıtlı olan cihazlar için geliştirilmiş olduğu bir Java platformu olduğundan hedeflediği cihazlar üzerinde çalışmak için J2SE'nin Sanal Makinasında ve diğer fonksiyonlarında kısıtlamaya gidilmiş ve hedef kitlesi olan cihazlar üzerinde çalışabilir hale getirilmiştir. Java'nın mobil cihazlar dünyasında uygulama geliştirmek için seçilmesinin önemli nedenleri vardır.

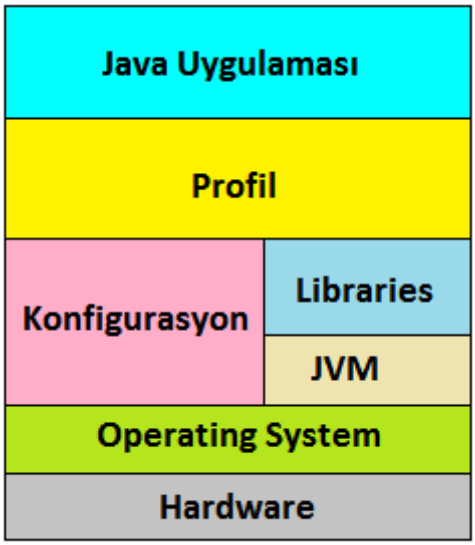
Java ortamı güvenlidir. Java byte kodları sadece Sanal Makina üzerinde çalışırlar ve en kötü ihtimalle sadece Sanal Makinenin çökmesine neden olabilirler. Mobil cihaz üzerindeki uygulama herhangi bir nedenden dolayı çökerse sadece Java Sanal Makina etkileneceğinden mobil cihazın diğer fonksiyonalarını etkilemeyecektir.

Ayrıca Java'nın sağladığı artık toplama (Garbage Collector) ve hata yakalama (Error handling) mekanizmaları hızlı ve güvenli kod geliştirilmesini de sağlar.

Java taşınabilirdir. MIDP standartlarına uygun olarak geliştirilen bir mobil uygulama MIDP standartlarını destekleyen tüm mobil cihazlarda sorunsuzca çalışabilmektedir. OTA (Over-The-Air) uygulama yükleme için Java byte kodları daha güvenli bir ortam sunar.

6.1. Profil (MIDP) ve Konfigurasyon (CLDC)

J2ME platformunun Sanal Makinası temel olarak diğer Java versiyonları gibi çalıştığı cihazın işletim sistemi üzerinde çalışır. Konfigurasyon ve Profil, J2ME ortamının temelini oluşturan diğer bileşenlerdir. Böylece üç katmanlı modüler bir yapı (Sanal Makina, Konfigurasyon ve Profil) ile farklı özelliklerdeki mobil cihazlarda uygulama geliştirme ve çalıştırma imkanını sağlanmış olmaktadır. Şekil 6.1'de Konfigurasyon ve Profil bileşenlerinin bir cihazda nasıl yer aldıkları gösterilmektedir. Konfigurasyon bir cihazın işletim sistemi üzerinde, Java Sanal Makinasını tamamlayıcı özelliklere sahiptir. Profil ise daha üst seviyede işlemlerin yapılmasını sağlar. J2ME uygulamaları genel olarak Profil sınıfları kullanılarak geliştirilir.



Şekil 6.1 Konfigurasyon ve Profil bileşenleri

6.1.1. Konfigurasyon

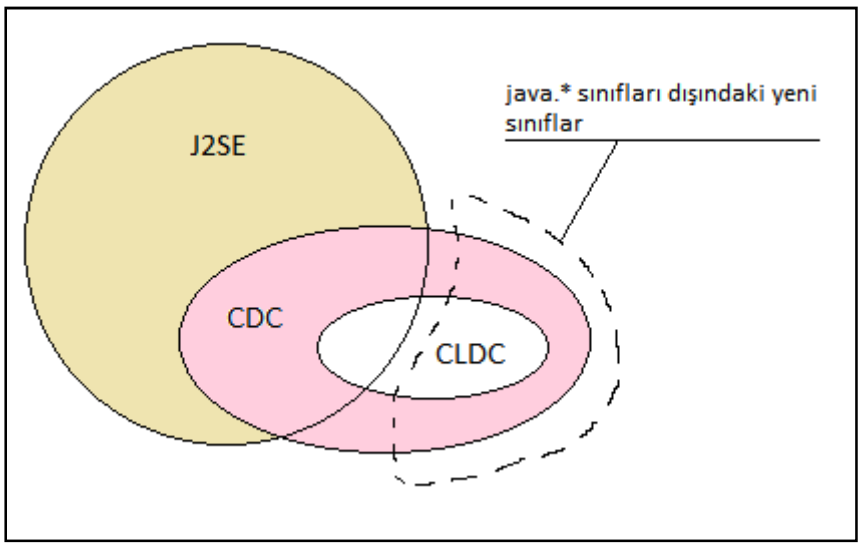
Cep telefonları, PDA ve bu tip diğer küçük cihazlar genellikle benzer işlemci güçlerine, hafız büyüklüklerine ve ağ bağlantı özelliklerine sahiptirler. Bu nedenle J2ME tasarlanırken bu tip benzer özelliklerdeki cihazları hedefleyebilmek için Konfigurasyon yapısı oluşturulmuştur. Konfigurasyon temelde Java sınıflarından oluşan bir API grubudur. Amacı kısıtlı cihazlarda ortak bir temel altyapı oluşturmaktır. Temel olarak iki adet konfigurasyon tanımı JSR olarak yayınlanmıştır.

- CDC
- CLDC

CDC (Connected Device Configuration) yerleşik olarak 2 Mb veya daha yüksek hafıza imkanı olan mobil cihazları hedefler. İşlemci hızı, hafıza kapasitesi ve ağ bağlantı özellikleri CLDC'ye göre daha iyi olan cihazlar için kullanılan Java API grubudur. CDC'inin sanal makinası ile Standart Java'nın (J2SE) sanal makinası çok

benzerlik gösterir ve bu yüzden sanal makina CVM (Compact Virtual Machine) olarak adlandırılır.

CLDC (Connected Limited Device Configuration) CDC'nin bir alt kümesidir.



Şekil 6.2 CDC ve CLDC

Şekil 6.2'de görüldüğü gibi CDC'de CLDC'de J2SE'nin tam bir alt kümesi değildir fakat ortak yanları vardır. CLDC ise CDC'nin bir alt kümesidir. Her iki konfigurasyonun da kendine özel sınıfları ve özellikleri vardır. Çünkü hedefledikleri cihaz aileleri farklı olduğundan birbirlerinden farklı sınıflara ihtiyaç duyarlar.

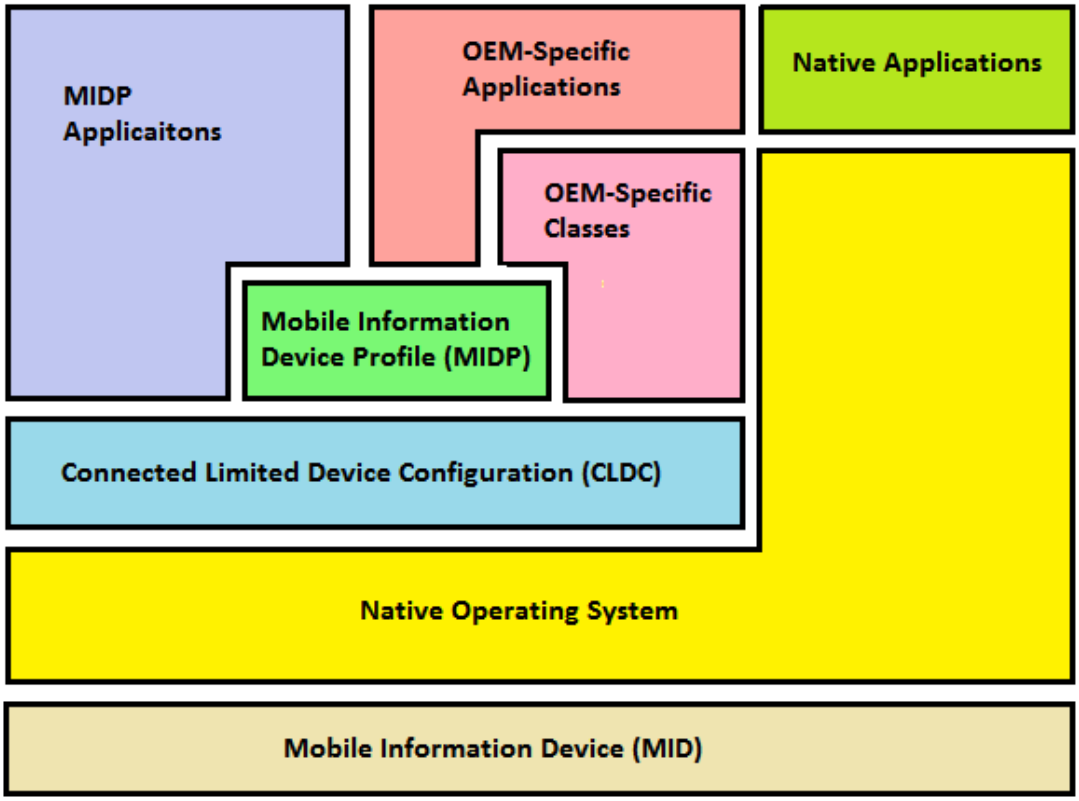
CLDC konfigurasyonunun hitap ettiği cihazlar ortalama olarak aşağıdaki özelliklere sahiptir.

- 160 – 512 Kb Java Platformu için hafıza
- 16 bit veya 32 bit işlemci
- Düşük güç desteği, çoğunlukla pil ile çalışma
- Sınırlı ve düşük bant genişliği sağlayan telsiz bağlantı

Şu an Java destekleyen telefonlar CLDC 1.0 versiyonunu desteklemektedir ve JSR 30 ile tanımlanmıştır. Bir sonraki versiyonda floating point, ek hata yakalama ve güvenlik içeren daha gelişmiş bir CLDC versiyonu ise JSR 139 ile tanımlanmaktadır.

6.1.2. Profil

Gerek işletim sistemleri gerekse de donanım özellikleri birbirinden farklı olan çok sayıda mobil cihaz için ortak bir uygulama geliştirme alt yapısı Profil ile sağlanır. JSR olarak tanımlanmış olan tek profil MIDP profilidir. MIDP 1.0 versiyonu JSR 37 ile JSP tarafından tanımlanmıştır. HTTPS, soket bağlantısı, işletim sistemine ulaşımı destekleyen alt seviye sınıflar ve XML parser içeren MIDP ise JSR 118 ile tanımlanmıştır. MIDP sınıfları ve fonksiyonları şekilde görüldüğü gibi CLDC sınıflarının ve fonksiyonlarının üzerinde yer alır. Uygulama geliştiricilerin telefonlar için uygulama geliştirmelerinde kullandıkları kullanıcı arayüzleri gibi yapıların sınıfları MIDP içinde yer almaktadır. Şekil 6.3’de donanım ve işletim sistemi üzerinde MIDP, CLDC ve uygulamaların nasıl bir şekilde çalıştıkları gösterilmektedir.



Şekil 6.3 Mobil uygulama genel mimarisi

6.1.3. OEM-specific classes ve OEM-specific applications

MIDP ve CLDC'nin mobil cihazlar için standart ve ortak bir altyapı oluşturmalarına rağmen, cep telefonu üreticilerinin desteklemek istedikleri bazı özellikleri içermemektedirler. Ekranın tam olarak kullanımı, cihazın titreşim ve ses özelliklerinin kullanımı gibi. Bu yüzden cihaz üretici firmalar cihazlarını üretirken kendi istediklerini yapabilen Java sınıflarını ekleyerek üretim yapmaktadırlar. Örneğin NOKIA'nın kendi telefonları için kullnadığı com.nokia.mid.ui.* paketi gibi. Tabii ki bu sınıfları kullanarak yazılan uygulamalar da her mobil cihazda değil sadece o paketi ve sınıfları destekleyen cihazlarda çalışmaktadır. OEM-Specific Applications'a Nokia'nın kızılötesi kullanılarak oynanabilen çok oyunculu yılan oyunu örnek olarak verilebilir.

Native Applications telefonun kendi işletim sistemi özelliklerini kullanarak geliştirilmiş uygulamalardır. Dikkat edilirse, uygulama geliştiriciler işletim sisteminden CLDC katmanı ile ayrılmaktadırlar. Yani sadece CLDC'nin tanımladığı Java sınıflarının izin verdiği kadarı ile işletim sistemine erişebilirler. Uygulama geliştiriciler son kullanıcılar için önyüzler ve grafik arabirimleri MIDP sınıflarını kullanarak geliştirirler.

MIDP'nin içinde bulunan Java sınıfları ile aşağıdaki fonksiyonlar gerçekleştirlebilir.

- Uygulamanın geliştirilmesi (MIDP uygulama kontrolü)
- Kullanıcı arayüzü
- Cihaz üzerinde bilgi saklama (Persistent Storage)
- Ağ bağlantısı
- Zamanlayıcılar (Timers)

Bu işlerin yapıldığı MIDP paketleri ise şunlardır:

- javax.microedition.lcdui: Kullanıcı arayüzleri ve interfaceleri
- javax.microedition.rms: Cihaz üzerinde veri saklama
- javax.microedition.midlet: MIDP uygulaması yapısını oluşturan sınıflar
- javax.microedition.io: Ağ bağlantı fonksiyonları
- javax.io: Standart Java giriş/çıkış fonksiyonları
- java.lang: Sanal makina sınıf ve interfaceleri
- java.util: Standart sınıf ve interfaceleri

6.1.4. CLDC'nin sanal makinasının J2SE sanal makinasından farklılıkları

J2ME, hafıza ve işlem gücü olarak düşük seviyede olan cihazlar için tasarlanmış olan Java uygulama çalıştırma ortamı olduğundan, hedeflediği cihazlarda çalışması için J2SE'den cihazları hafıza ve işlem gücü olarak zorlayacak yada cihazların hiç

çalıştıramayacakları sınıflar ve özellikler çıkartılmıştır. Fakat sonuç olarak J2SE'den farklı bir cihaz kitlesine hitap ettiğinden ilave sınıf ve özellikler de getirilmiştir.

CLDC'de olmayan J2SE özellikleri şunlardır:

- Floating Point hesaplama .
  float ve double gibi değişken tipleri kullanılamaz. Çünkü CLDC'nin üzerinde çalıştığı cihazlar donanım olarak kayan noktalı aritmetiği desteklemezler.
- Finalization

object.finalization() metodu kullanılamaz. Böylece kullanılmayan nesneleri garbage collector yoketmeden önce finalization metodu kullanılarak işlem yapılamaz.

- Sınırlı hata anlama

CLDC'nin desteklediği sadece üç hata sınıfı vardır. java.lang.Error, java.lang.OutOfMemory ve java.lang.VirtualMachineError

- JNI

Hem güvenlik hem de yüksek hafız gereksinimleri yüzünden JNI (Java Native Interface) desteklenmemektedir.

- Kullanıcı tanımlı sınıf yükleyici

Güvenlik sebeplerinden ötürü sadece cihaz içinde önceden yüklenmiş olan sınıflar kullanılır. Kullanıcıların kendi sınıf yüklemelerini yapmaları mümkün değildir.

- Reflection

J2SE'de çalışma sırasında sanal makina hakkında bilgi almak mümkündür. Hangi sınıflar yüklü, metodları, özellikleri gibi bilgiler çalışma anında alınabilir. CLDC'nin çalıştığı cihazlarda reflection desteklenmemektedir.

- Thread grupları

CLDC'de multithreding desteklenmesine rağmen thread grupları mantığı desteklenmemektedir. Threadler için sınırlı sayıda komut kullanılabilirdir.

- Weak Referances

J2SE’de kullanılan ve garbage collector’un nesneler üzerindeki referanslarını ayarlayan weak references kavramı CLDC’de desteklenmemektedir.

6.1.5. CLDC ile gelen yenilikler

Sınıf Doğrulayıcı:

J2SE’nin sanal makinesinde olan sınıf doğrulayıcı’nın (Class Verifier) görevi geçersiz sınıfları elemektir. CLDC’nin yapısında da güvenlik için bu tip bir doğrulama gerekmektedir. Fakat cihazların hafıza ve işlem gücü olarak kısıtlı olmasından dolayı sınıf doğrulama işlemi java sınıflarının derlendiği ortamlarda yani PC’lere taşınmıştır. Böylece sınıf doğrulama işlemi cihazlardan alınarak hem güvenlik sağlanmış hem de cihazın üzerinde çalışan sanal makinanın görevi hafifletilmiştir. Bu şekilde sınıf doğrulama işlemine önceden doğrulama (pre-verifying) denir. Normalde J2SE’nin sanal makinasında yaklaşık 50 Kb hafıza gerektiren sınıf doğrulama kodundan CLDC’nin çalıştığı sanal makinada tasarruf edilmiştir. Sadece önceden doğrulanan sınıflarda hedef cihaz üzerinde çalışabilmesi için bazı eklemeler yapıldığından sınıfları boyutları %5 kadar artmaktadır.

CLDC’ye özel sınıflar

CLDC’ye özel sınıf olarak ağ bağlantılarını destekleyen paket eklenmiştir.

java.microedition.io (Standart olarak J2ME’deki özel sınıflar java.microedition ile başlar)

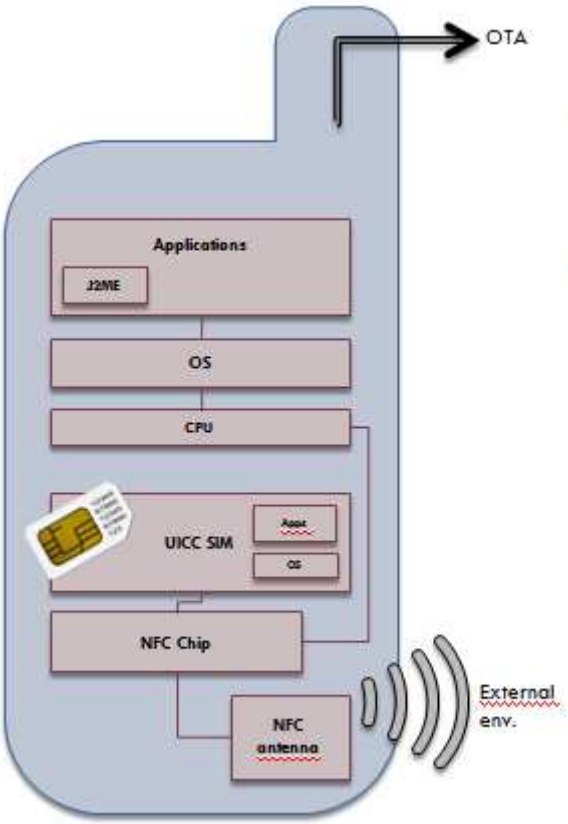
java.microedition paketi içindeki sınıflar ise şunlardır:

Connection, ConnectionNotFoundException, Connector, ContentConnector, DataGram, DataGramConnection, InputConneciton, OutputConnection, StreamConnection, StreamConnectionNotifier

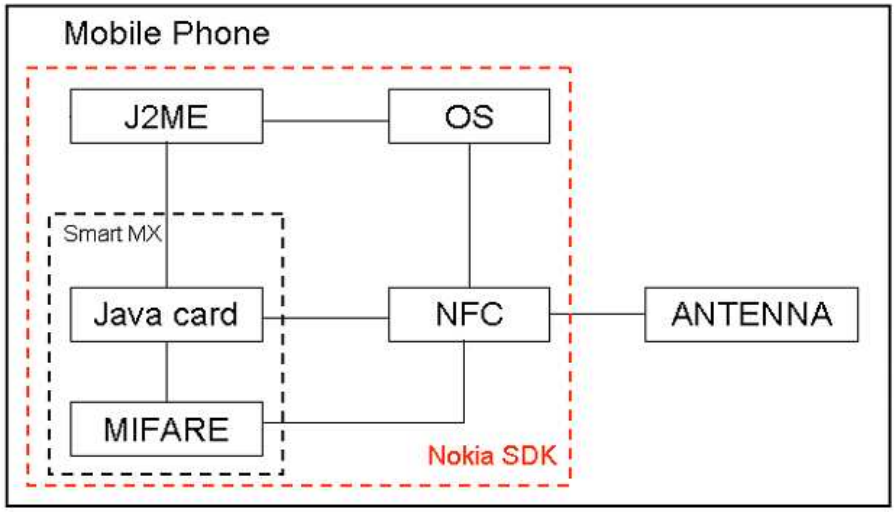
6.2. NFC Cihazlarda Yazılımsal Yapı

Geliştirici açısından bir Secure Elementin nerede bulunduğunun çok fazla önemi yoktur. Secure Element'in programlanmasında geliştiriciler daha çok GlobalPlatform'un spesifikasyonları ile çalışırlar. Secure Element'in nerede olduğunun önemi daha çok uygulama dağıtım modelinin seçimi ile ilgilidir. Bazı durumlarda Secure Element mobil servis sağlayıcıların sağladığı SIM üzeride bulunurlar.

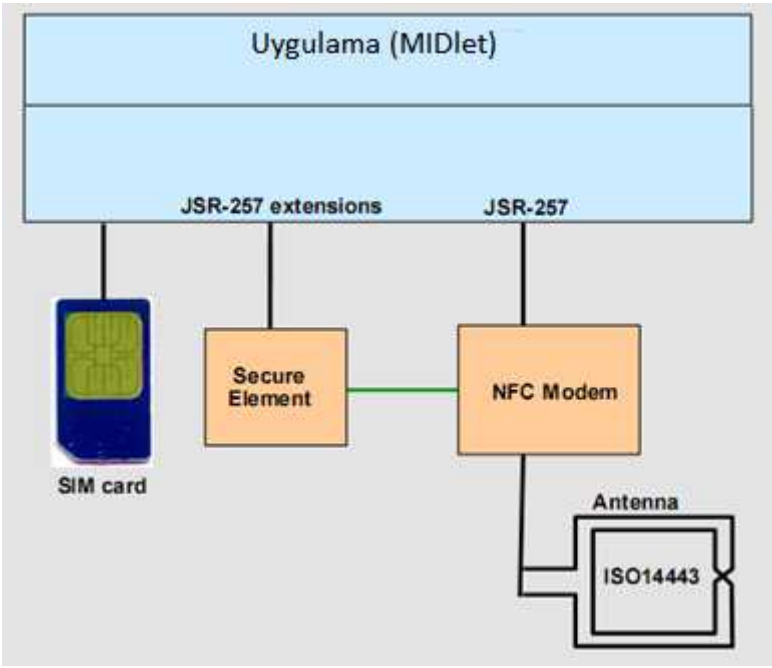
Şekil 6.4a, Şekil 6.4b ve Şekil 6.4c'te bir mobil cihaz üzerindeki donanım ve yazılım ilişkisi gösterilmektedir.



Şekil 6.4a Mobil cihazda yazılım donanım ilişkisi - I



Şekil 6.4b Mobil cihazda yazılım donanım ilişkisi - II



Şekil 6.4.c Mobil cihazda yazılım donanım ilişkisi - III

Geliştirme ortamları çeşitli kaynaklar tarafından sağlanmaktadır. Bunlar:

- Eclipse veya Netbeans gibi Tümleşik Java Geliştirme Ortamları
- Nokia gibi üreticilerin sağladığı SDK'lar
- Gemalto ve Oberthur gibi kart üreticilerinin sağladığı geliştirme kitleri
- Orange gibi mobil servis sağlayıcılarının verdiği geliştrime kitleri

6.3. Contactless Communication API

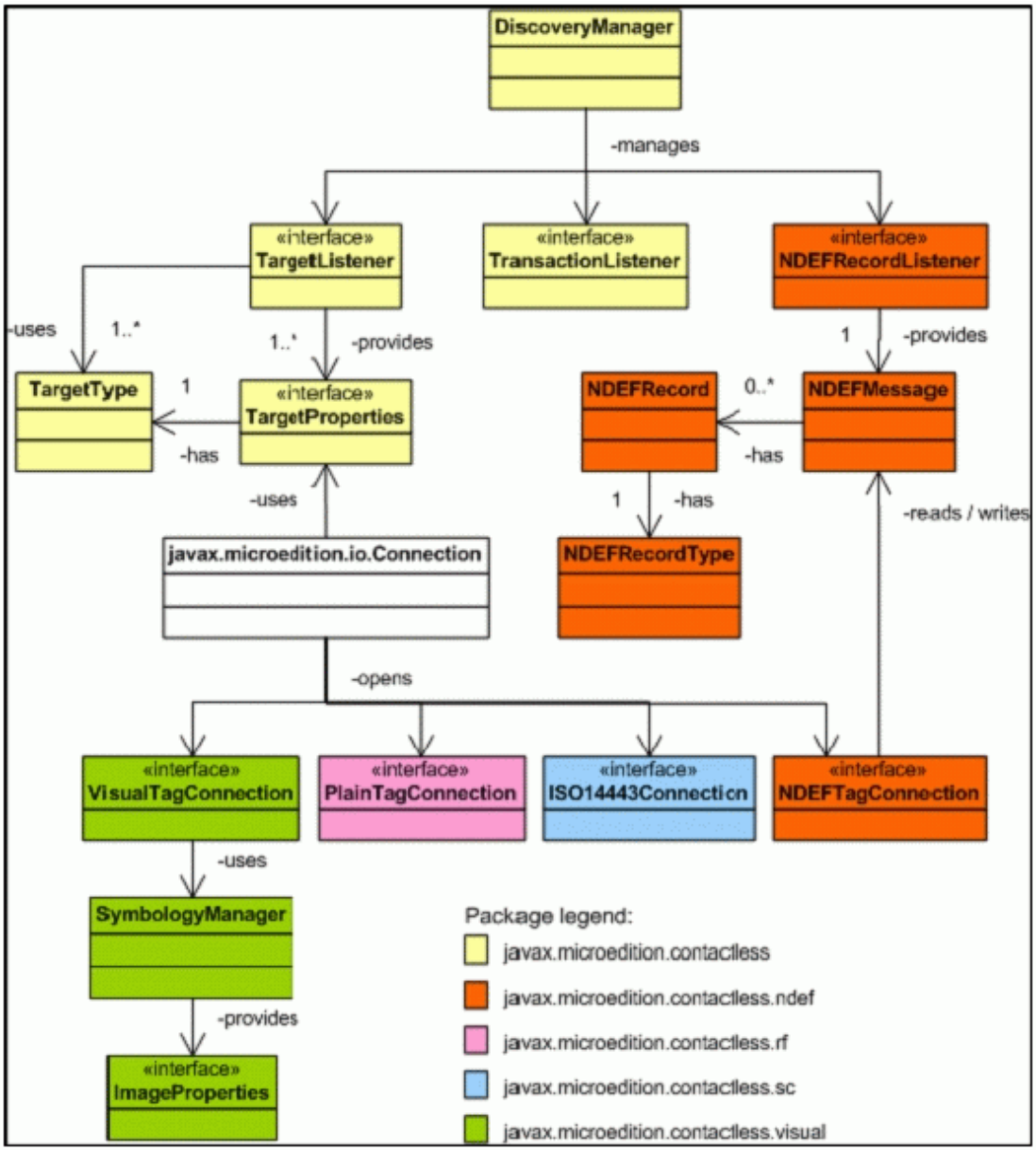
Nokia'nın liderliğinde geliştirlen ve JSR-257 ile tanımlanan temassız haberleşme API grubu java spesifikasyonları mobil cihazlarda temassız yakın alan haberleşmesi için kullanılabilecek API ve sınıfları tanımlar. JSR-257 kullanılarak mobil cihazlarda NFC yakın alan haberleşmsi yapabilen uygulamalar geliştirilebilmektedir. JSR-257 beş Java paketi içermektedir. Tablo 6.1'de bu Java paketleri ve sağladığı interface, sınıf ve exceptionlar gösterilmiştir.

Tablo 6.1 JSR-257 Java paketi

Java Paketi	Interface'ler	Sınıflar	Exception'lar
javax.microedition.contactless	TagConnection TargetListener TargetProperties TransacitonListener	DiscoveryManager TargetType	ContactlessException
javax.microedition.contactless.ndef	NDEFRecordListener NDEFTagConnection	NDEFMessage NDEFRecord NDEFRecordType	
javax.microedition.contactless.rf	PlainTagConnection		
javax.microedition.contactless.sc	ISO14443Connection		
javax.microedition.contactless.visual	ImageProperties VisualTagConnection	SymbolManager	VisualTagCodingException

Temassız haberleşme fonksiyon grubu NDEF tag'ler, RFID tag'ler ve temassız akıllı kartlar gibi temassız haberleşen cihazlarla haberleşebilemek için Bulma (Discover) ve VeriTransferi (Exchange) özelliklerini sağlar.

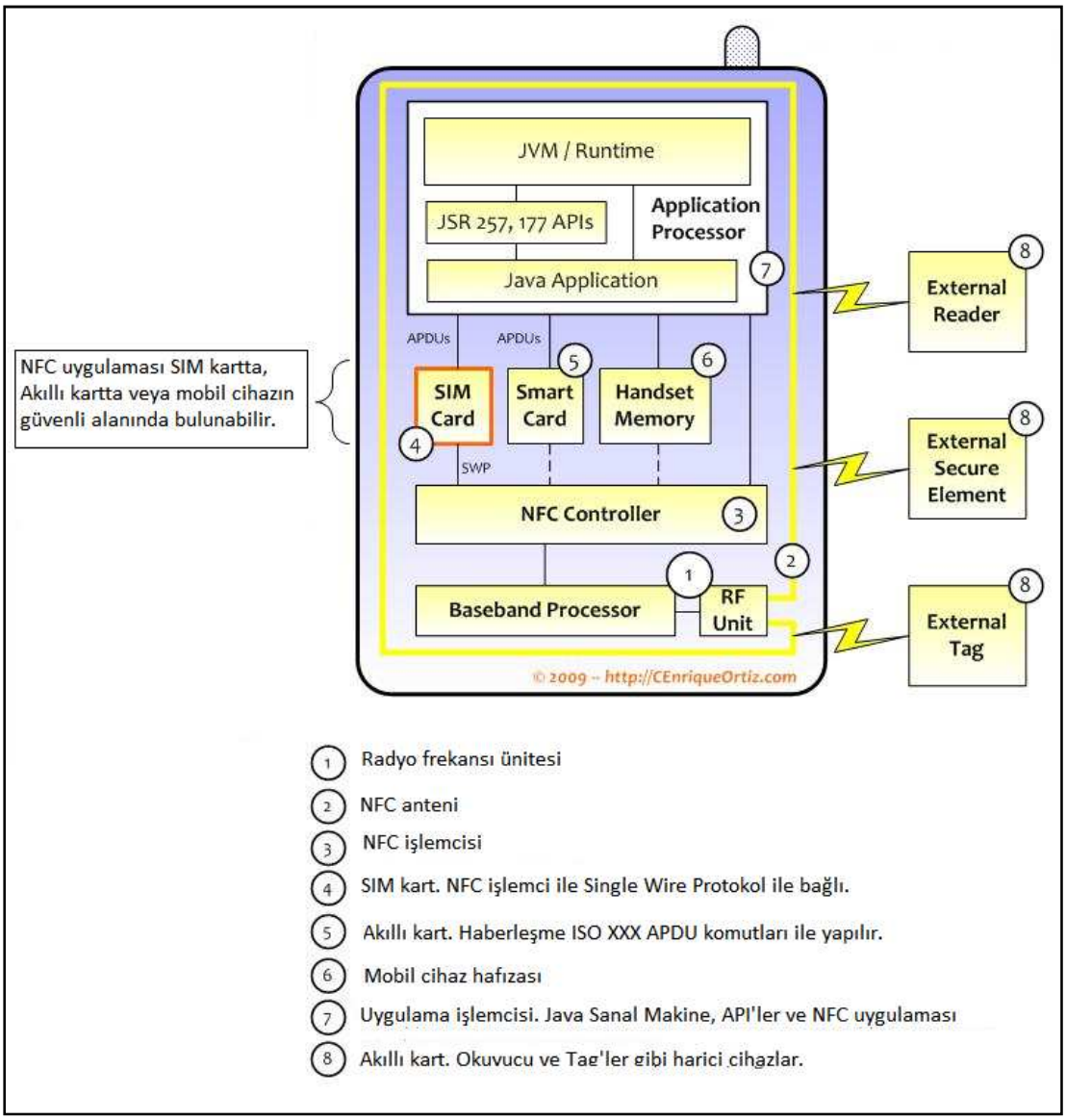
Şekil 6.5'de farklı API sınıfları ve interface'lerinin ilişkileri gösterilemektedir.



Şekil 6.5 JSR-257 Temassız haberleşme API grubu

Bu fonksiyon grubu ile mobil cihazlar hem NFC hem de IrDA bağlantıyı kurabilmektedir. JSR-257 API grubu J2ME için seçimlik, isteğe bağlı olarak kullanılan bir pakettir. Paket içindeki DiscoveryManager ve TargetListener herhangi bir tip kısıtı olmaksızın çalışır. JSR-257 ile NDEF ve ISO14443 protokolünde bağlantılar kurulabilmektedir.

JSR-257 temassız haberleşme API grubu ile geliştirilen bir mobil uygulamanın genel görünümü Şekil 6.6'daki gibidir.

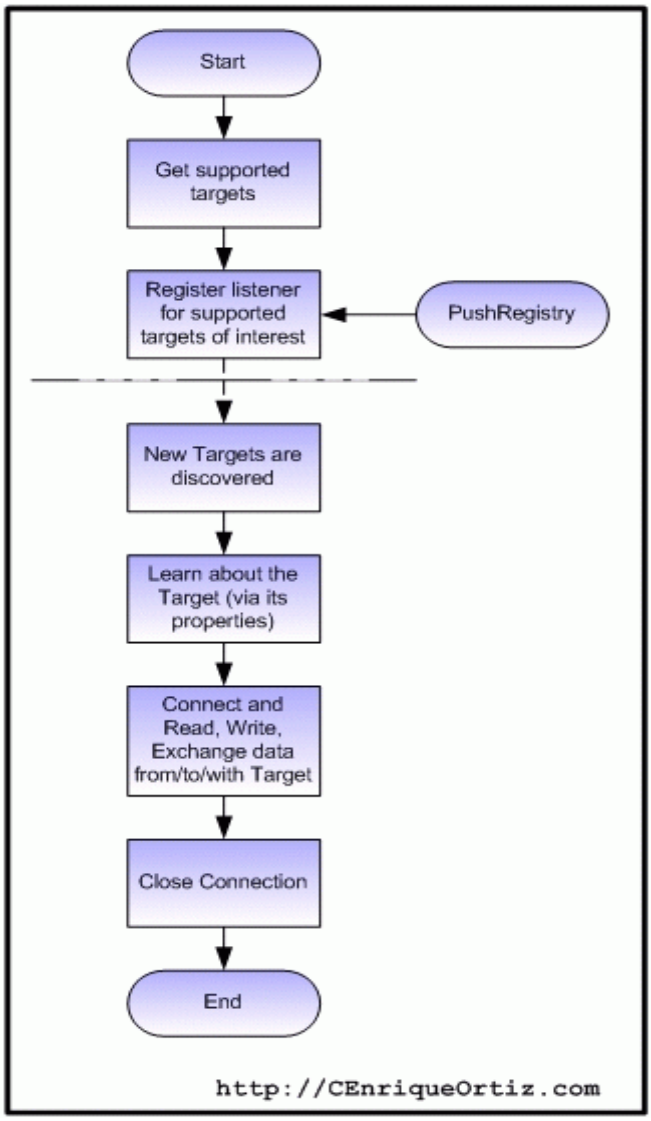


Şekil 6.6 JSR-257 uygulaması ve mobil mimari

Şekildeki sistemde bulunan bileşenler şunlardır. JSR-257 temassız haberleşme API grubunu içeren bir Java Sanal Makinesi, mobil cihaz üzerinde çalışan J2ME ile geliştirilen bir MIDlet, RFID, NFC alıcı vericisi, işlemcisi, Secure Element'i ihtiva eden SIM kart.

Şekilde gösterilen Externel Reader, temassız kart okuyucu bağlantısı olan POS cihazını ifade eder. Güvenli eleman (SE) dahili veya harici olabilir. MIDlet Güvenli Eleman'a Security and Trust Service API (SATSA) ile veya JSR-257 ile erişebilir.

Temassız haberleşme API grubu JSR-257 mobil cihazın RFID taglerin ve temassız akıllı kartların bulunmasını (Discover) ve haberleşilmesini (Exchange Data) sağlar. Temassız haberleşme API'lerinin kullanımı ve temel işlem akışı Şekil 6.7'de gösterilmiştir.

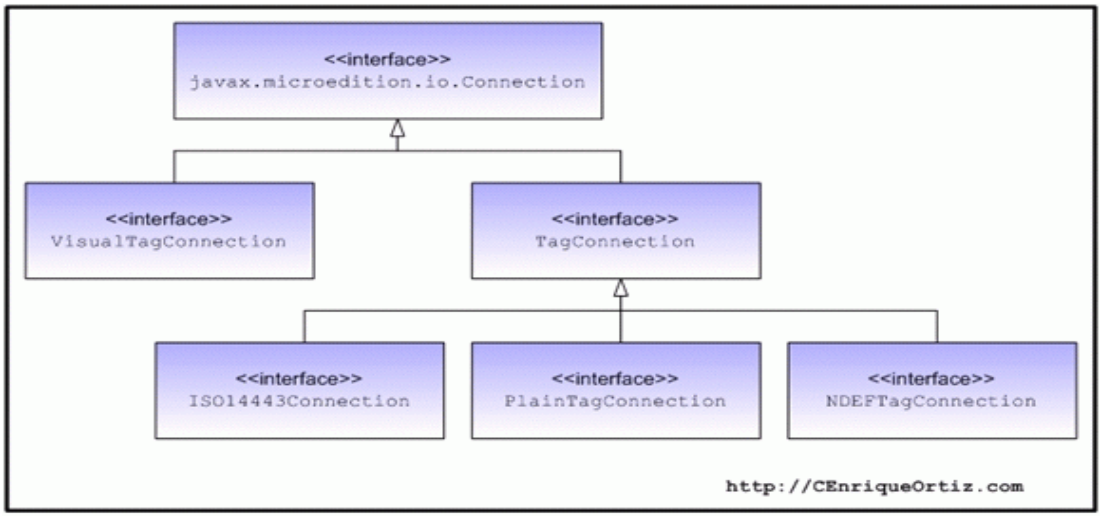


Şekil 6.7 Temel temassız haberleşme akışı

Temassız haberleşme işlem akışında şu adımlar gerçekleşir.

- İlk adımda mobil cihazın bulmak için desteklediği tag tipleri tespit edilir.
- Desteklenen herbir tag tipi için mobil uygulama eylem haberini alabilecek bir hedef dinleyici (target listener) kaydı oluşturur.
- Hedef tag okuyucuya yaklaştığında, tag uygulama tarafından tespit edilir. İlgili eylem dinleyicisinin işlem yapabilmesi için bir uyarı oluşturur.
- Tespit edilen her bir hedef tag için, mobil uygulama taglerin özelliklerini alır.
- Mobil uygulama tespit edilen her bir hedef tag ile haberleşebilir, veri okuyup yazabilir.
- İşlem bittiğinde mobil uygulama sistem kaynaklarını serbest bırakır. Açık olan tag bağlantılarını kapatır.

Temassız haberleşme API grubu, JSR-257, Generic Conneciton Framework (GCF)'den türerilmiştir. General Communication Framework Java'da temel giriş çıkış işlemleri için geliştirilmiştir. General Communication Framework ile HTTP, datagram ve stream bağlantılar kurulabilir. Şekil 6.8'de temassız haberleşme API grubu ve General Communication Framework ilişkisi görülmektedir.



Şekil 6.8 Temassız haberleşme API ve GCF ilişkisi

Temassız haberleşme API grubu bağlantı temelli iki interface'i tanımlamaktadır.

- TagConnection:
- Tüm RFID tag, temassız akıllı kart ve NFC bağlantılarını ifade eder.

ISO14443Connection, TagConnection'dan türetilmiştir. ISO 14443-4 spesifikasyonuna uyumlu temassız akıllı kartlar ile haberleşmede kullanılır.

PlainTagConnection, TagConnection arayüzünden türetilmiştir. NFC uyumlu olmayan RFID tagler ile haberleşmek için kullanılır.

NDEFTagConnection, bu arayüz de TagConnection arayüzünden türetilmiştir. NFC Forum'un tanımladığı spesifikasyonlarda formatlanmış RFID tag ve temassız akıllı kartlar ile haberleşmede kullanılmaktadır.

- VisualConnection, Bu bağlantı barcode gibi görsel taglerin okunmasında kullanılır.

6.3.1. Destekelenen taglerin izlenmesi ve bulunması

Desteklenen taglerin bulunması (Discover), platform tarafından DicoveryManager.getSupportedTargetTypes() metodunun çağırılması ile sağlanır. Bu medod çağırıldığında desteklenen tagler için bir TargetTypes türünden dizi döner. Daha sonra desteklenen bu hedef taglerin her biri için bir hedef izleyici, Target Listener oluşturulur. Şekil 6.9'daki java kodu registerTargetListener() isimli bir metodu göstermektedir. Bu metod ile platfomun desteklediği hedef tag türleri tespit edilir. Daha sonra ISO 14443-4 uyumlu temassız akıllı kart türünden bir hedef tagi izleyecek olan bir hedef tag izleyici oluşturulur.

```
import javax.microedition.contactless.TargetListener;
// :
DiscoveryManager dm = DiscoveryManager.getInstance();
// :
/**
 * Discover supported targets, registers listeners
 * @param targetListener the target listener
 */
public void registerTargetListeners(TargetListener targetListener) {
   // Discover supported types
   TargetType[] tp = DiscoveryManager.getSupportedTargetTypes();
   try {
      // Register listener for each of the supported types
      for (int i=0; i<tp.length; i++) {
         if (tp[i].equals((TargetType.ISO14443_CARD))) {
            dm.addTargetListener(
               targetListener, TargetType.ISO14443_CARD);
         } else...
           //:
         }
      }
   } catch (Exception e) {
      // ...
   }
}
```

Şekil 6.9 Taglerin bulunması

Temassıs haberleşme API grubu örnekte görüldüğü gibi ISO14443_CARD tag tipini desteklediği gibi NDEF_TAG, RFID_TAG ve VISUAL_TAG tag tiplerini de desteklemektedir.

Bir kere istenilen ve desteklenen hedef tag tipleri yukarıda gösterildiği gibi bulunup uygun hedef izleyiciler kurulduktan sonra her hangi bir hedef tag bulunduğunda uygulama TargetListener.targetDetected(TargetProperties[]) metodunu çağırır. Şekil 6.10'da bir hedef tag'in bulunduğunda çağırılacak olan kod gösterilmektedir.

```
import javax.microedition.contactless.TargetListener;

public void targetDetected(TargetProperties[] prop) {
   for (int i = 0; i < prop.length; i++) {
      // Get UID
      String uid = prop[i].getUid();
      // Get Connection Classes
      Class[] classes = prop[i].getConnectionNames();
      // Get Target Types
      TargetType[] types = prop[i].getTargetTypes();
      // Connect to each Target
      String url = prop[i].getUrl();
      try {
         // Open NDEFTagConnection to the target
         NDEFTagConnection conn = (NDEFTagConnection) Connector.open(url);
         //:
      } catch (IOException e) {
         // ...
      }
   }
}
```

Şekil 6.10 Hedef tag bulunduğunda çalıştırılacak kod

Şekil 6.10'da gösterilen targetDetected() metodu tipik olarak şu adımları yapar:

- targetDetected() metodu tespit edilen hedef taglerin özelliklerini ifade eden TargetProperties yapısında bir obje alır.
- Her bir tespit edilen hedef tag için, hedef tag'in özelliklerini içeren nesneden bir URL alınır.
- General Conneciton Framework (GCF) kullanılarak hedef tag ile bir bağlantı oluşturulur.
- İstenen veriler hedef tag ile alınıp verilir.

- Gelen mesajlar, mesaj özelliklerine göre işlenirler.
- İşlemler tamamlandığında hedef tag ile kurulan bağlantı kapatılır, sistem kaynakları geri bırakılırlar.

6.3.2. NDEF taglerin izlenmesi

Temassız haberleşme API grubu ayrıca özelleştirilmiş NDEF hedef taglar ile haberleşmek için de kullanılır. Bunun için özelleştirilmiş NDEF taglerin yapısının detaylı olarak bilinmesine de gerek yoktur. Haberleşmek için ihtiyaç duyulan tek şey NDEF tag üzerinde bulunan kayıt tiplerinin nasıl olduğu ve bunların nasıl işleneceğidir. Böylece veri haberleşmesi çok daha basitleşmiş olmaktadır. NDEF hedeflerin izlenmesi için NDEFRecordListener arayüzü ve bu arayüzün bir metodu olan recordDetected(NDEFMessage ndefMessage) metodu kullanılır. Bir NDEF kayıt izleyicisinin sisteme kaydının yapılıp çalıştırılması DiscoveryManager'in addNDEFRecordListener(listener, recordType) metodu ile yapılmaktadır. Şekil 6.11'de gösterilen kod parçası bu işlemleri göstermektedir.

```
import javax.microedition.contactless.ndef.NDEFRecordListener;

DiscoveryManager dm = DiscoveryManager.getInstance();

// Register NDEF_TAG target (smart poster) to discover
try {
   NDEFRecordType rt = new NDEFRecordType(
      NDEFRecordType.NFC_FORUM_RTD, "urn:nfc:wkt:Sp");
   dm.addNDEFRecordListener(this, rt);
} catch (IllegalStateException e) {
  // :
} catch (Exception e) {
   //:
}
```

Şekil 6.11 NDEF taglerin izlenmesi

Temassız haberleşme API grubu aşağıdaki NDEF kayıt tiplerini desteklemektedir:

- **EMPTY**: Boş kayıtlar için tanımlanmış olan kayıt tip adıdır.
- **EXTERNAL_RTD**: NFC Forum isimlendirme kurallarına göre uygulamaya özel olarak tanımlanmış kayıt tiplerini tanımlar.
- **MIME**: RFC 2046'ya göre tanımlanmış MIME tipinde kayıt türlerini ifade eder.
- **NFC_FORUM_RTD**: NFC Forum Kayıt Tip Tanımı (Record Type Identifier) için ifade edilen kayıt tipidir.
- **UNKNOWN**: Bilinmeyen kayıt tipini ifade eder.
- **URI**: RFC 3986 spesifikasyonunda tanımlanan URI tiplerini ifade eder.

6.3.3. NDEF mesajlarının işlenmesi

Sistemde bir defa NDEF izleyici kaydedildiğinde, platform istenen NDEF için recordDetected(NDEFMessage ndefMessage) isimli metodu çağırır. Bu metoda NDEF hedef aktif ve görünür olduğunda NDEF mesaj parametre olarak verilir. recordDetected() metodu kayıt ve kayıt tipini verir. Ayrıca NDEF mesajına ilişkin diğer bilgileride vererek, mesajın özelliklerine göre mesajı işler. Şekil 6.12'deki kod parçasında NDEF hedef mesajlarının işletilmesi gösterilmektedir.

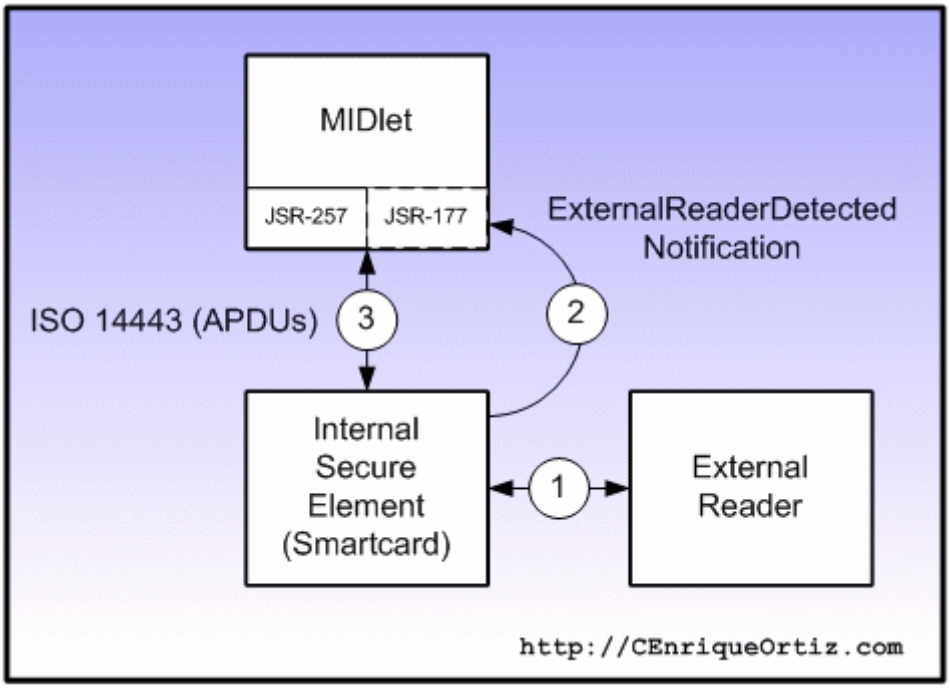
```
/**
 * Called by the platform, when the requested NDEF record type is
 * discovered by the device from the contactless target.
 * @param ndefMessage the NDEF message to process
 */
public void recordDetected(NDEFMessage ndefMessage) {
   // Get records and record types from NDEF Message
   NDEFRecordType[] rTypes = ndefMessage.getRecordTypes();
   NDEFRecord[] records = ndefMessage.getRecords();
   for (int i=0; i<records.length; i++) {
      // Handle data, based on type of NDEFMessage
      NDEFRecordType t = recordTypes[i];
      NDEFRecord r = records[i];
      byte[] id = r.getId();
      long len = r.getPayloadLength();
      byte[] p = r.getPayload();
      // Process the record
      // ...
   }
}
```

Şekil 6.12 NDEF mesajların işletilmesi

Bir NDEF mesajın işlenmesinin maliyeti uygulamaya bağlı olarak değişir. Örneğin bir URL bağlantısı içeren bir NDEF kaydın işlenmesi için mobil cihazda web browser'in açılması ve bazı bilgilerin bu URL'ye gönderilmesi işlemleri yapılmalıdır.

6.3.4. Kart emülasyonu aktivite bildirimleri

Kart emulasyonu modundaki haberleşmede mobil cihaz üzerindeki Güvenli Eleman (Secure Element) harici bir temassız kart okuyucu ile RFID donanım üzerinden haberleşir. Mobil uygulamalar her bir kart emulasyonu modundaki işlemler için bilgilendirilirler. Ancak yapılan işlemin akışına müdahale edemezler. Şekil 6.13'de kart emulasyonu aktivite bildirimi gösterilmektedir.



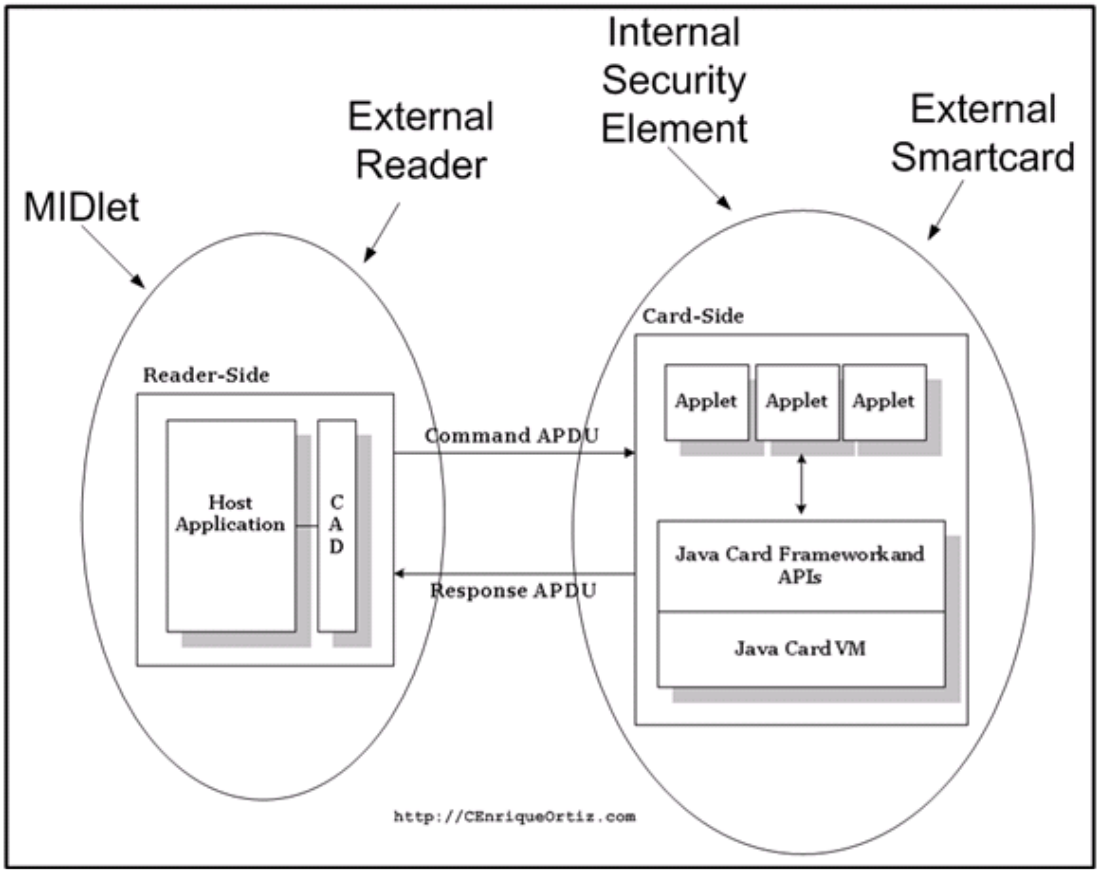
Şekil 6.13 Kart emulasyonu aktivite bildirimi

Şekil 6.13’de;

- Mobil cihaz üzerindeki dahili Güvenli Eleman harici bir temassız kart okuyucu ile etkileşime geçmektedir.
- Mobil uygulama (MIDlet), harici temassız okuyucu tespit edildiğinde bilgilendirilir.
- Eğer gerekiyorsa, mobil uygulama (MIDlet) mobil cihaz üzerindeki Güvenli Eleman ile haberleşir. Mobil uygulamanın Güvenli Eleman ile haberleşmesinde Temassız haberleşme API grubu JSR-257 ISO 14443 bağlantı arayüzü veya varsa SATSA bağlantısı kullanılır.

Güvenli Eleman ile harici temassız kart okuyucu arasındaki haberleşme mobil uygulama için transparent, görülmezdir. Temassız kart okuyucu ile Güvenli Eleman arasındaki haberleşme Java Card haberleşmesinde de olduğu gibi APDU komutları kullanılarak yapılmaktadır. Mobil uygulama ile Güvenli Eleman arasında haberleşme yapabilmek için Güvenli Eleman uygulaması olan applet hakkında detaylı bilgiye ihtiyaç vardır. Güvenli Eleman appletinin hangi komutları kabul ettiğini ve geri döndürdüğü cevapların yapısını mobil uygulama bilmek zorundadır. Akıllı kart teknolojisinde kullanılan APDU komutları ISO 7816-4 spesifikasyonunda tanımlanmıştır.

Şekli 6.14’te bir Java Card uygulamasının mobil cihaz üzerinde çalışan bir MIDlet ile ilişkisini göstermektedir. Mobil cihaz uygulaması bu ilişkideki rolü “Okuyucu” olmasıdır. Güvenli Eleman “Card-side” rolünde çalışmaktadır.



Şekil 6.14 Javacard uygulamasının tipik bileşenleri, Temassız haberleşme senaryosu

Şekil 6.14'te gösterildiğine göre;

- Temassız kart okuyucu içeren NFC mobil cihazda sol taraf dahili bir okuyucu, bir mobil uygulama MIDlet veya NFC'nin Kart emulasyon modunda çalıştığı bir harici temassız kart okuyucu olabilir.
- Şekilde sağ taraf bir akıllı karttır. Bu akıllı kart dahili veya harici güvenli eleman olabilir. Bu güvenli elemana erişim SATSA, JSR-257 veya RFID donanım üzerinden olur.
- Şeklideki tüm haberleşmeler APDU komut yapısında gerçekleşir.

6.3.5. Kart emulasyonu aktivitelerinin işlenmesi

Daha önceden de ifade edildiği gibi mobil cihaz Kart Emulasyonu modunda çalışıyorken uygulama harici bir temassız kart okuyucuya yaklaşıldığının uyarısını alır. Ancak uygulamanın kendisi temassız kart okuyucu ile güvenli elemanın gerçekleştirdikleri işleme dahil olmaz. Sadece işlem yapıldığı hakkında bilgilendirilir. Ayrıca eğer gerekiyorsa mobil uygulamanın güvenli eleman ile APDU komutlarını kullanarak haberleşmesi mümkündür. Bu durumda da mobil uygulama güvenli eleman üzerinde yerleşik olan appletin yapısı hakkında bilgiye sahip olmalıdır. Appletin hangi komutları kabul ettiğini ve hangi cevapları verdiğini bilmelidir.

Bir mobil uygulamanın güvenli elemanın Kart Emulasyonu modundaki işlemlerini izleyebilmesi için javax.microedition.contactless.TransactionListener arayüzünü ve onun externalReaderDetected(byte slot) metodunu uyarlamalıdır. Bir işlem izleyicisi de DiscoveryManager'in addTransactionListener() metodu ile kaydedilmelidir. Aşağıdaki kodda bir Kart Emulasyonu işleminin izlenmesi örneği gösterilmektedir.

```
import javax.microedition.contactless.TransactionListener;
// Register Transaction Listener
try {
   dm.addTransactionListener(this);
} catch (IllegalStateException e) {
  // ...
} catch (Exception e) {
}
/**
 * Called by the platform, when a card emulation event
 * has happened on the RFID hardware.
 * @param slot is the slot needed to open the APDUConnection defined
 *           in JSR 177 to the external secure element, may be
 *           UNKNOWN_SLOT constant defined in this interface, if the
 *           slot can not be identified.
 */
public void externalReaderDetected(byte slot) {
   // Based on slot number above, using ISO14443Connection or SATSA
   // connect to applet, query applet, update screen, etc.
}
```

Şekil 6.15 Kart emulasyonu işleminin izlenmesi

6.4. PushRegistry Metodu ile NFC Uygulamalarının Çalıştırılması

Mobil cihazlarda NFC uygulamalarının kullanıcının bir akıllı poster, tag veya diğer bir NFC cihaza tek dokunuşla otomatik olarak çalıştırılması başarım ve kullanıcı memnuniyeti için önemlidir. PushRegistry metodu Mobile Information Device Profile (MIDP)'nin sağladığı bir tekniktir. Push Registry tekniği ile zamanlayıcılara veya bağlantı olaylarına bağlı olarak uygulamalar otomatik olarak çalıştırılabilir. Ancak şimdilik Temassıs Haberleşme API grubu JSR-257 uygulamaların otomatik

olarak başlatılabilmesi için sadece NDEF Kayıt tipinde olan kart emulasyonu modunda çalışan güvenli eleman aktiviteleri için desteklediğini unutmamak lazım.

Bağlantı URL'leri spesifikasyonlarda belirtildiği gibi isimlerndime kurallarına uygun olarak kayıt işlemleri için kullanılır.

- NDEF Push kayıt bağlantı için URL formatı "ndef:"<record_type_format>?name=<record_type_string> şeklinde olmalıdır.
- Burada;
  <record_type_format> "rtd","external_rtd", "mime" veya "uri" olabilir.
  <record_type_string> UTF-8 formatında kayıt tipini tam ifade eden ve uygulama tarafından tam olarak tanımlanmış isimdir. Örneğin urn:nfc:wkt:Sp Nokia Smart Poster'i ifade eder.
- Kart Emulasyonu aktivitesi için URL formatı "secure-element:"?aid=<aid_string> şeklindedir.
- Burada;

<aid_stirng> ISO 7816-5 spesifikasyonuna uygun şekilde tanımlanmış ve kart üzerindeki appleti ifade eden isimdir.

Bir uygulamanın çalıştırıldığında temassız okuyucu tarafından tespit edilen NDEF kayıt için veya kart emulasyonu modu aktivitesi için uygun bildirimi alıp almadığından emin olabilmek için uygulama açılır açılmaz NDEFRecordListener ve TransactionListener'i register etmelidir.

6.5. Yazılım Güvenliği

Temassız Haberleşme API grubu JSR-257 güvenlik denetimlerini ve konularını mobil platformun sorumluluğuna bırakmıştır. Bir MIDP uygulaması için tablo 6.2'de gösterilen metodlar veya operasyonlar güvenlik iznine tabidir.

Tablo 6.2 Temassız haberleşme API grubu MIDP güvenlik izinleri

DiscoveryManager.getInstance()	javax.microedition.contactless.DiscoveryManager
NDEFMessage yazma	javax.microedition.contactless.ndef.NDEFTagConenction.write
NDEFTagConnection açma	javax.microedition.io.Connector.ndef
PlainTagConnection açma	javax.microedition.io.Connector.rf
ISO14443Conneciton açma	javax.microedition.io.Connector.sc
VisualTagConnection açma	javax.microedition.io.Connector.ctag

Bu modelde, JAD dosyası veya JAR manifestosu üzeriden MIDlet-Permissions özelliklerinin oluşturulması ile izin talep edilir. MIDlet-Permissions'da tablo 6.2'deki isimler kullanılır. Güvenlik için izin alınmamış bir metodun çağırılması veya operasyonun gerçekleştirilmesi durumunda sistem bir SecurityException oluşturur.

CDC profil destekleyen mobil cihazlarda çalışacak olan uygulamada kullanılacak temassız haberleşme API grubu JSR-257 için uygulama java.security.Permission kullanılmalıdır. Aşağıdaki şu metodlar gerekli olan izni sistemden almış olmalıdırlar.

- DiscoveryManager.getInstance()
- NDEFTagConnection.write(NDEFMessage message)

BÖLÜM 7.
BİR NFC UYGULAMASI VISA MOBİL PLATFORM

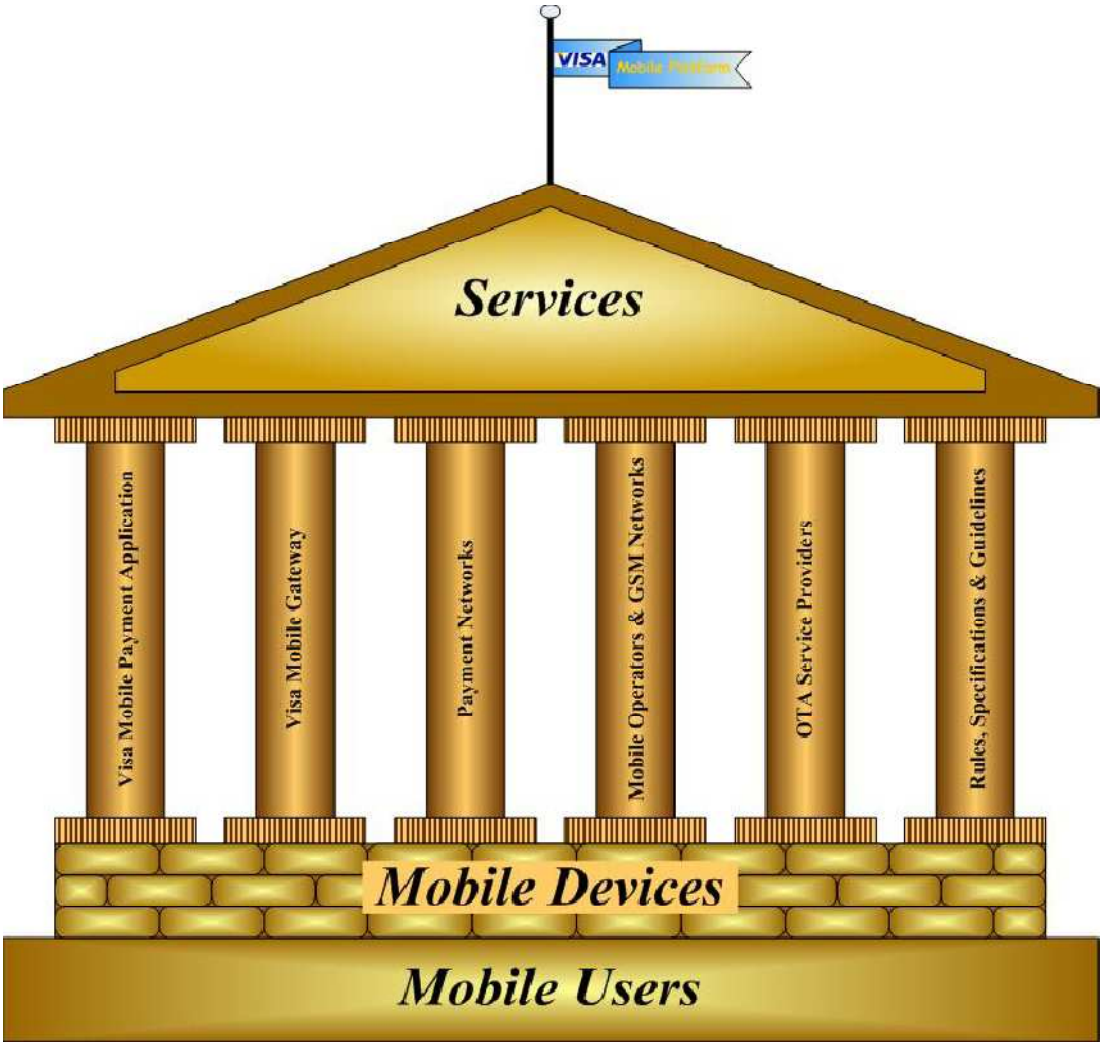
Bu bölümde Visa'nın mobil NFC sistemlerde ödeme işlemleri için geliştirdiği Visa Mobile Platform incelecektir. Visa Mobile Platform'un yapı taşları şunlardır:

- Yaygın olarak kullanılan mobil ağ üzerinden dağıtılabilir,
- Yüklenen mobil uygulamalarının kişiselleştirilmeleri herhangi bir Visa payWave temassız okuyucunun bulunduğu satış noktasında gerçekleştirilebilir.
- Mobil uygulamaların işletilmesi yerel mobil ağ üzerinden yapılabilir.

7.1. Mobil Ödeme

Mobil Ödeme kavramı, ödeme işleminin cep telefonları, PDA'lar gibi mobil cihazlar üzerinden onay alınarak yapılmasını ifade etmektedir. NFC cihazlar Visa'nın payWave teknolojisini sunacak olan dahili bir Güvenli Elemanına (SE) sahiptir.

Mobil Ödeme Sistemleri hem alış verişte geleneksel yüzyüze iletişimi, hemde uzaktan para transferi gibi çeşitli ödeme ilişkilerini sağlar.



Şekil 7.1Visa Mobil Platform genel mimarisi

Visa Mobil Platform (VMP) uygulamalar, ağlar, sistemler, iş birimleri ve işlem kurallarının birlikte oluşturduğu bir sinerjidir. Bu sinerjinin hedefi müşterilerin ödeme işlemlerini yakın veya uzak mesafeli olarak mobil cihazları üzerinden gerçekleştirmelerinin sağlayacak uygulamaları geliştirmek ve dağıtmaktır.

Visa Mobil Platformunun temel elemanları şunlardır.

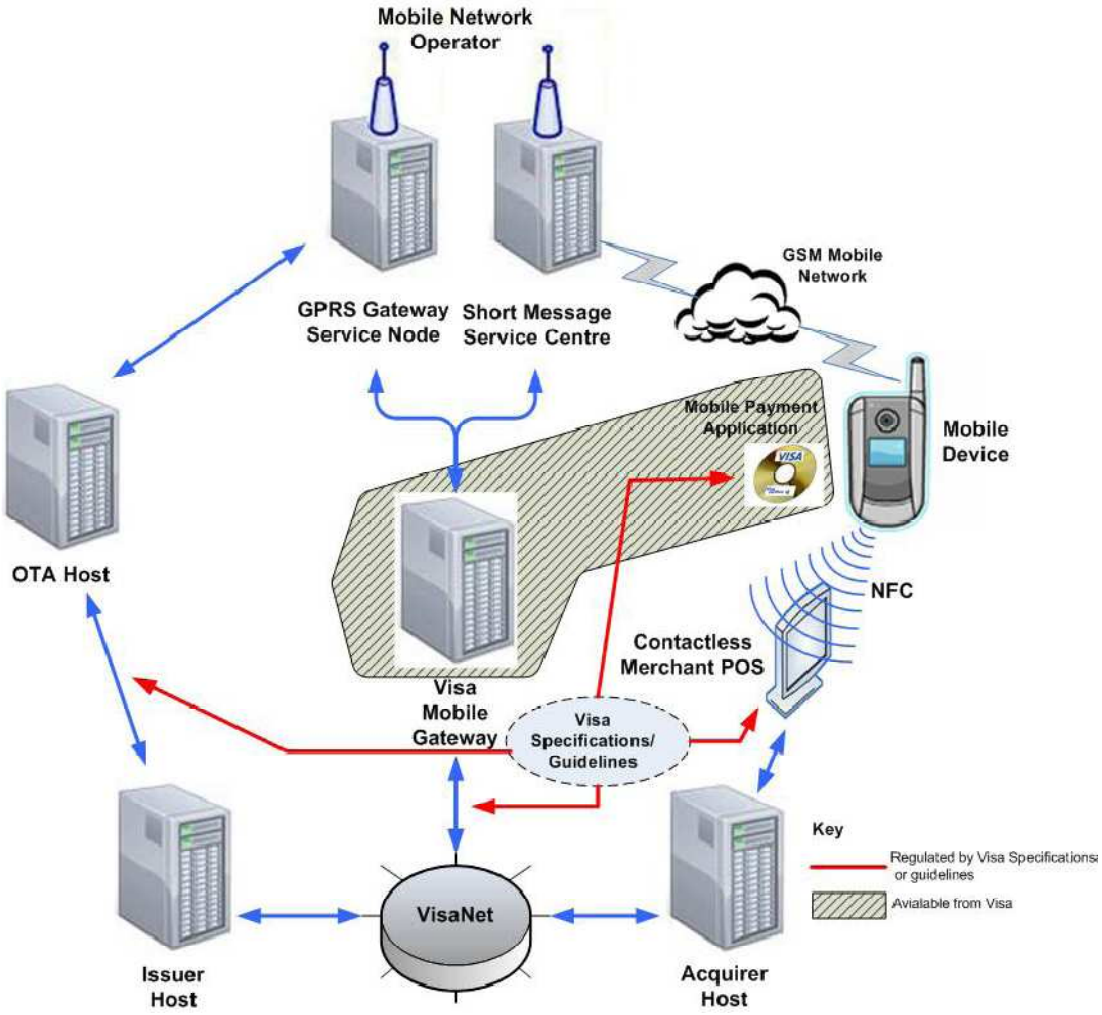
- Mobil Ödeme Uygulaması (Mobile Payment Application)
  VMP Mobil uygulama, ödeme ve kişisel güvenlik hizmetlerini son kullanıcıya çok zengin ve görsel ifadelerle sunan yazılımdır.
- Visa Mobile Gateway:
  Visa Mobil Platform, mobil cihazların GPRS ağ üzerinden hesap işleten bankanın

host sistemine direk olarak bağlanmasını sağlayan web temelli VisaNet portalını sağlar.

- Ödeme Ağı (Payment Networks)
  Visa Mobil Platform, Visa payWave kullanan işyerleri ile yakın alan ödeme sisteminin kullanılabileceği bir ödeme ağı sağlar.
- Mobil Operatötler ve GSM Ağları:
  Mobil operatörler ve ağlar Visa Mobil Platformun kablosuz bağlantı ile, ihtiyaç duyulan uzaktan provizyon sağlamak için bağlantı ihtiyacını giderir.
- OTA Servis Sağlayıcılar
  Kart sahibi bankanın mevcut hesap işletim sistemi ile mobil cihazların kişiselletirilmesi, servisin aktifleştirilmesi, konfigurasyonlarının yapılması ve ilklendirme işlemlerinde OTA servis sağlayıcılar bu boşluğu doldururlar.
- Kurallar, Tanımlamalar ve Klavuzlar:
  Visa'nın kuralları, Tanımlamaları ve Klavuzları tüm Visa Mobil Platform kullanıcı ve geliştiricileri için servis erişimleri ve ödeme sistemleri güvenliği için küresel bir birlikte çalışabilirlik sağlar.

7.2. VISA Mobil Platfom Mimarisi

Visa Mobil Platform mimarisinin genel görünümü Şekil 7.2'deki gibidir.



Şekil 7.2 Visa Mobil Ödeme Platformu Mimarisi

Visa Mobil Platform, mevcut ödeme sistemlerine daha fazla yük olmaması için mümkün olduğunca mevcut yapı bileşenlerini kullanacak şekilde tasarlanmıştır.

Mobil ödemeyi sağlayabilmek için, Visa tüm müşterileri için yeni ve yenilikçi ürünler ve servisler sunmaktadır. Şekil 7.2 Visa'nın müşterilerine sunduğu, platform güvenliğini en üst ve kullanıcı deneyimini en iyi düzeye taşıyan sistem bileşenlerini göstermektedir. Visa'nın Tanımlama ve Klavuzları hem mobil ödeme hemde bankacılıkla ilgili servis ve uygulamaların geliştirilip dağıtılmasının kurallarını ihtiva etmektedir.

Üçüncü parti Katma Değer Hizmet üreticilerinin geliştirdileri servis ve uygululamaları Visa Mobil Platformun sağladığı Mobile Gateway gibi harici portallara, arayüz bileşenlerine entegre olabilirler.

7.2.1. Yeni Visa mobil platform ödeme bileşenleri

Mobil ödeme uygulamaları (Mobil Payment Applications, MPA)

Geleneksel Chip ve PIN temeli ödeme ürünleri, akıllı kartlar üzeride sunulan ödeme uygulamalarını kullanırlar. Visa Mobil Platform ödeme uygulamalarının yetenekleri geliştirmiş, özelliklerini genişletmiştir. Mobil ödeme uygulamaları hem kullanıcı arayüzü hem de bir mobil cihaz üzerinde erişilebilen servisler ve donanımlar sayesinde daha fazla imkana sahiptirler.

Mobil cihazlar

Mobil cihazlar Visa Mobil Platformun merkezinde yer almaktadır. Mobil cihazlar, Visa payWave işlemleri için temasız iletişim kurabilecek arayüze sahip ve uzak servislere bağlanabilecek bağlantı seçeneklerine sahip taşınabilir cihazlardır.

Temassız işyeri POS'u

İşyerinde temassız ödeme işlemi yapabilmek için işyerinin Visa payWave ürününe sahip olması gerekmektedir. Temassız okuyucuya sahip işyeri POS'u müşterilerinin temassız Visa işlemleri yapabilmesine imkan verir.

Visa mobil gateway

Visa Mobil Gateway, VisaNet kullanan mobil bankacılık servisleri ve uygulama yönetimlerine erişimleri kolaylaştırmak için tasarlanmıştır. Visa Mobil Gateway'in bu özelliği sayesinde mobil uygulamalar ve hesap hizmeti veren bankaların birbiri ile iletişime geçmsei için OTA servis sağlayıcılarına veya temassız okuyucuya sahip üye işyeri POS'una ihtiyaç yoktur.

Mobil network operatör

Mobil operatörler ve temassız bağlantılar Visa Mobil Platform'un uzak servislere erişiminin alt yapısını sağlarlar. Visa Mobil Platform mobil ağ servis sağlayıcıların

sunduğu SMSC (Short Message Service Centre) ve GGSN (GPRS Gateway System Node) hizmetlerine doğrudan bağlanır. Bu her iki hizmet sayesinde Visa Mobil Platform kullanıcıları hesap işleten bankaların hizmetlerine erişebilirler.

OTA sunucular

OTA (Over The Air) sunucular Visa Mobil Platform kullanıcılarına servis aktivasyonları, uygulama dağıtımı, veri iletimi hizmetlerini sağlarlar.

7.2.2. Geliştirilmiş ödeme sistemleri bileşenleri

Acquier host

Visa Mobil Platform mevcut ödeme sistemini, otorizasyon, günsonu ve takas sistemlerini kullanır. Şekil 7.2'de gösterildiği gibi üye işyerleri ve Visa Mobil Platformu mevcut ödeme sistemlerini kullanmaktadır. Ödeme işlemleri, Günsonu işlemleri, Takas işlemleri ve Otorizasyon işlemleri Visa Mobil Platform'da VisaNet veya üye işyerinin POS'u üzerinden mevcut olan Acquier sunucusuna gönderilebilir. Acquier sunucusu, POS'un sahibi olan ve ilk bağlantının yapıldığı sunucudur. Visa Mobil Platform'un mevcut iletişim desenine herhangi bir etkisi olmamaktadır.

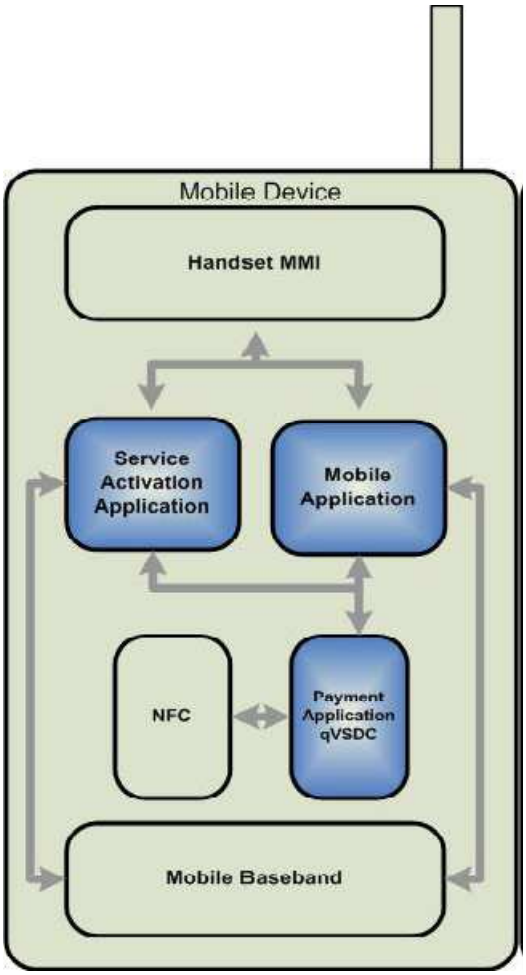
VisaNet

Visa Mobil Platform mobil ödemeler için de mevcut olan otorizasyon, Günsonu ve Takas sistemini kullanabilir. Şekil 7.2'de görüldüğü gibi VisaNet, mobil ödeme uygulamaları hizmetini veren hesap sağlayan (Issuer) sunucu ile Acquier sunucu arasında bağlantı sağlar.

Issuer host

Issuer sunucusu Otorizasyon, Günsonu ve Takas işlemlerini yapar. Şekil 7.2'de görüldüğü gibi, Visa Mobil Platform kullanıcılarının mobil ödeme bilgileri Issuer sunucuya VisaNet üzerinden veya mobil cihazın SMS veya GPRS network altyapısını kullanarak OTA sunucu üzerinden gelmektedir.

7.3. Visa Mobil Ödeme Uygulaması



Şekil 7.3 Visa Mobil Ödeme Uygulaması Mimarisi

Visa'nın mobil ödeme uygulamasının genel yapısı Şekil 7.3'de görüldüğü gibidir. Mobil ödeme uygulaması, mobil cihazların sunduğu kaynaklar ile etkileşimde bulunan ve son kullanıcıya hizmet veren üç temel unsurdan oluşmaktadır.

7.3.1. Servis kurulum uygulaması (Service Activation Application, SSA)

Visa Mobil Platform kullanıcılara EMV temelli ödeme sistemini kullanan mobil bir ödeme uygulaması sunmaktadır. Visa'nın zorunlu kıldığı ve güvenlik ve gizliliği en yüksek seviyede sağlayacak uygulamaların dağıtımını ve kurulumunu sağlamakla yükümüdür. Servis Kurulum Uygulaması OTA servis sağlayıcıların kurulum için sağladığı bir uygulamadır. Mobil Ödeme uygulamasının kurulumu önce OTA servis sağlayıcısından bir Servis Kurulum Uygulaması içeren bir SMS gönderilerek

başlatılır. Mobil kullanıcının gelen SMS uygulamasının çalıştırılması ile Servis Kurulum Uygulaması mobil cihaza yüklenir. Kurulan Servis Kurulum Uygulaması çalıştırıldığında OTA servis sağlayıcısına güvenli bir bağlantı kurar. Bu bağlantı Visa'nın klavuzlarında belirtildiği gibi sırasıyla mobil ödeme uygulamasının ve mobil uygulamanın indirilmesi, kurulması, açılması ve kişiselleştirilmesi işlemlerini yapar.

7.3.2. Ödeme uygulaması (Payment Application, PA)

Ödeme uygulaması Visa'nın temassız ödeme kurallarında belirtildiği gibi çalışan bir uygulamadır. Ödeme Uygulaması, hesap işleten bankanın verdiği güvenli işlemlerin yapılabilceği kriptografik anahtarlar ile müşteri bilgileri ile kişiselleştirilir. Ödeme Uygulaması, temassız işlem yapılırken üye işyerinin POS cihazı ile haberleşen NFC bileşenlerini kullanır.

7.3.3. Mobil uygulama (Mobile Application, MA)

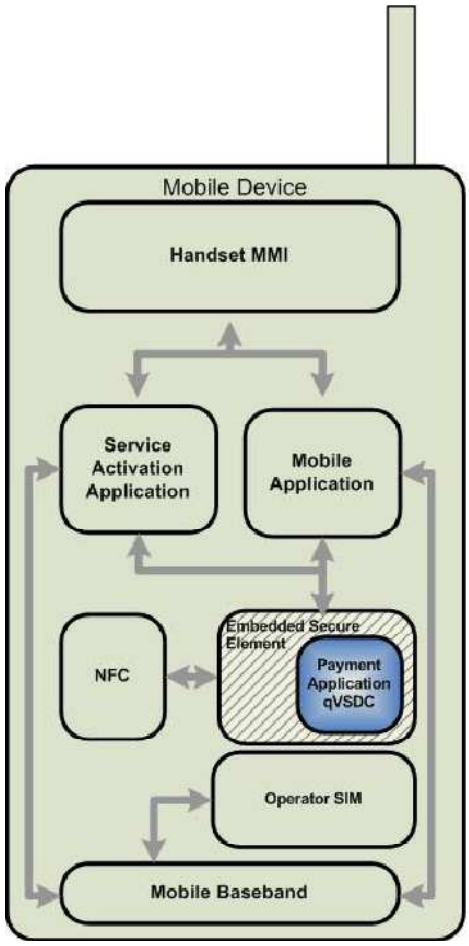
Mobil Uygulama, Ödeme Uygulamasının kontrolünü ve üçüncü parti hizmetlere erişimini sağlar. Mobil uygulama cihaz üzerindeki özellikleri kullanabilecek kullanıcı arayüzlerini sunar. Kullanıcılar bu arayüz ile Visa Mobil Platform hizmetlerini yürütebilirler.

7.4. Ödeme Uygulamasının Sunumu

Ödeme Uygulaması, yapısı gereği mobil cihazlarda Güvenli Eleman (Secure Element, SE) üzerinde bulunmak zorundadır. Bir mobil cihazın Visa Mobil Platform içinde kabul edilebilir olması için akıllı kart işlevlerini sağlaması gerekir. Bu yüzden Ödeme Uygulaması mobil cihazlar üzerinde üç farklı ortamda sunulabilir. Ödeme Uygulaması, mobil cihazlarda mobil cihaz üzerinde gelen Güvenli Eleman üzerinde, Mobil Operatörün sağladığı SIM kart üzerinde veya SmartMX kart gibi genişleme yuvalarında sunulabilirler.

7.4.1. Gömülü güvenli eleman mimarisi

Bu tür mimariye sahip mobil cihazlarda, cihazdan ayrıştırılamayan çoklu uygulamayı destekleyen akıllı kart elektronik bileşeni vardır. Gömülü Güvenli Elemana sahip bir mobil cihazın mimarisi Şekil 7.4'de gösterildiği gibidir.



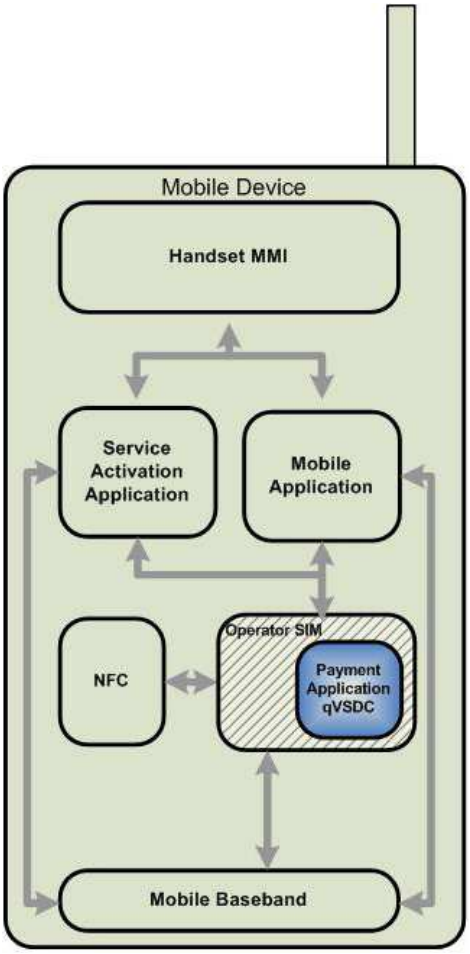
Şekil 7.4 Gömülü Güvenli Eleman mimarisi

Ödeme Uygulaması, servis aktivasyonu sırasında mobil cihazın gömülü güvenli elemanında yüklenirler. Ödeme Uygulaması bir kere yüklendikten sonra diğer kart temelli uygulamalar gibi aynı güvenlik seviyesini sağlamaktadır. Ödeme Uygulaması diğer kart uygulamalarından güvenlik hizmeti olarak farksızdır. Ödeme Uygulaması Güvenli Elemana yüklenip kişiselleştirildikten sonra kullanıcı tarafından kolaylıkla kaldırılamaz. Uygulamanın kaldırılması da çeşitli güvenlik kurallarını gerçekleştirerek yapılır.

7.4.2. SIM Kart temelli mimari

Mobil Operatörlerin SIM kartları aslında GSM kurallarını gerçekleştiren birer akıllı karttan başka bir şey değildir. SIM karta yüklenmiş uygulamalar, geleneksel temassız akıllı kartların sağladığı güvenlik mekanizmaları ile aynı güvenliğe sahiptirler.

Şekil 7.5'te SIM kart temelli mimarinin şeması görülmektedir.SIM kart temelli mimari Ödeme Uygulamalarının çalıştırılması için mobil cihaz bağımlılığını ortadan kaldırır.

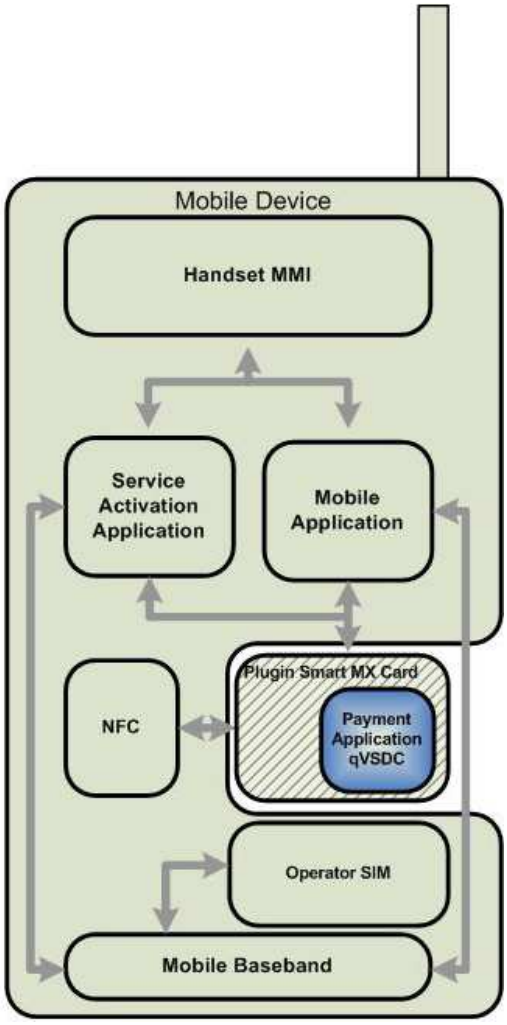


Şekil 7.5 SIM Kart temelli mimari

7.4.3. Genişleme yuvası mimarisi

Genişleme yuvası mimarisinde Ödeme Uygulamaları mobil cihaza takılıp çıkarılabilen akıllı kart özelliklerine sahip olan genişleme yuvası kartları üzerinde

sunulurlar. Gömülü Güvenli Eleman ve SIM kart temelli mimariler gibi Genişleme yuvası mimarisi de Ödeme Uygulamaları için aynı seviyede güvenlik imkanları sağlamaktadır. Şekil 7.6'da mobil cihazlarda Genişleme Yuvası Mimarisinin genel görünümü gösterilmektedir.

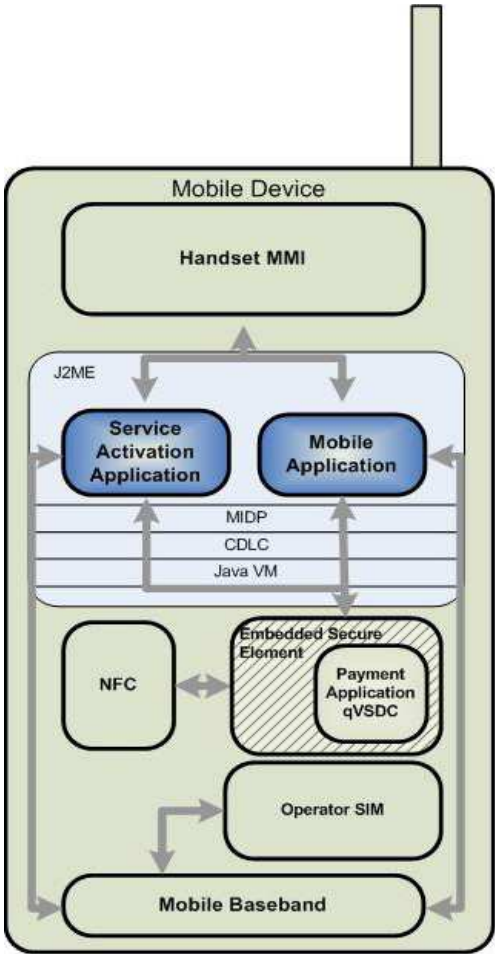


Şekil 7.6 Genişleme Yuvası Mimarisi

Çoklu uygulamalı akıllı kartlar genellikle Java temelli kartlardır. Ayrıca Ödeme Uygulamaları da Java kullanılarak gerçekleştirilirler. Ödeme Uygulamaları Java teknolojileri ile geliştirldiğinden dolayı bazen Ödeme Applet'i (Payment Applet, PA) olarak da isimlendirililer.

7.5. Mobil Uygulamanın Sunumu

Visa Mobil Platform, halen CDLC üzerinde MIDP kullanan Java sanal makinelerini destekleyen mobil cihazlar ile çalışmaktadır. Bu protokoller üst seviye uygulamaların cihazın donanımına erişimesini sağlamaktadır. Mobil Uygulama da MIDP üzerinde çalışmasında dolayı Mobile Midlet olarak da isimlendirilir. Şekil 7.7'de bir mobil cihaz üzerinde Mobil Uygulamanın sunumu gösterilmektedir.



Şekil 7.7 Mobil Uygulama sunumu

Mobil cihaz üzerinde çalışan Servis Aktivasyon uygulaması ve Mobil Uygulama Java sanal makinesi üzerinde çalışan birer J2ME uygulamalarıdır. Her iki uygulama da mobil cihazın donanımına erişebildiği gibi Güvenli eleman üzerinde bulunan Ödeme Uygulaması ile de haberleşirler.

Servis Aktivasyon uygulaması OTA sunucular üzerinden mobil cihazlar üzerine yüklenirler. Bir SMS ile yüklenen uygulama kurulup çalıştırıldığında Issuer sunucusundan Güvenli Elemana yüklenecek olan Ödeme Uygulamasını indirir ve kurulumunu yapar. Ödeme Uygulaması Güvenli Elemana kurulduktan sonra Issuer sunucudan alınan bilgilerie göre kişiselleştirilir. Servis Aktivasyon Uygulaması daha sonra Mobil Uygulamayı mobil cihaza indirir ve yüklemesini yapar. Bundan sonra mobil cihaz kullanıcısı yüklenen bu mobil uygulamayı kullanarak Ödeme Uygulamasını kullanabilir. Servis Aktivasyon Uygulaması ve Mobil Uygulama mobil cihazın sunduğu kablosuz iletişim olan GPRS ve SMS hizmetlerini kullanabilirler.

7.6. Ödeme Uygulaması

Visa Mobil Platformun bir parçası olarak sunulan Ödeme Uygulaması, EMVCo'nun ödeme sistemleri için koyduğu ICC kuralları ve Visa'nın genellikle Visa Smartcard Debit Credit (VSDC) olarak isimlendirilen Visa ICC Kuralları (VIS)'na göre oluşturulmuştur.

Visa bu kuralları daha da geliştirip, performasnını arttırarak qVSDC'yi üretimiştir. qVSDC temassız ödeme işlemlerinde sistemin daha hızlı cevap verebilmesi için optimize edilmiş VSDC kurallarının bir alt kümesini oluşturur. Böylece Ödeme Uygulaması, kartın okuyucunun elektro manyetik alanı içinde iken hızlıca işlem yapabilmektedir.

qVSDC, Visa Mobil Platform kullanıcılarına normal temaslı kartlardaki VSDC kurallarının sağladığı güvenlik imkanını daha hızlı işlem yapılması, Ödeme Uygulaması ile üye işyeri POS'unun arasında daha optimize edilmiş komutların taşınması ile sağlamaktadır.

7.6.1. Ödeme uygulamasının işlevselliği

Visa mobil Platform Ödeme Uygulamasının sağladığı temel işlevler tablo 7.1'de özetle ifade edilmiştir.

Tablo 7.1 Ödeme uygulamasının sağladığı temel işlevler

Özellik	*Tanım*
qVSDC işlemleri	qVSDC işlevleriVisa'nın temassız ödeme kurallarında tanımlandığı gibi yapılmaktadır. qVSDC küresel kullanımı ve işlem güvenliğini sağlar.
Çok Noktadan Şifre Doğrulama	Güvenlik şifresi doğrulama servisi, Güvenli eleman üzerinde kayıtlı şifrelenmiş güvenlik şifresine erişimi Mobil uygulama ile genişletilmiş komut seti ile alıabilir.
Yüksek Değerli Offline Ödemeler	Visa'nın temassız ve offline olarak izin verdiği sınırları aşan miktarlardaki işlemler yapılırken kullanıcıdan ekstra onay alınır.
Düşük Değerli Offline Ödemeler	Visa'nın temassız ve offlien olarak izin verdiği sınırları aşmayan değerlerdeki işlemler kullanıcıdan herhangi bir ekstra onay istemeksizin bir defada gerçekleştirilir.
Uygulama Yönetiminin OTE sunucu ile yönetilmesi	Visa Mobil Platform kullanan hesap işleten bankaların sunucuları, mobil uygulamalrın portföylerini, kartın bloke edilmesi, unblock edilmesi gibi script işlemlerini yönetebilirler.
EMV tabanlı doğrulama	EMV uyumlu hem online hem de offline doğrulama işlemlerinde, hesap işleten bankanın sağladığı halihazırda kullanılmakta olan sertifika ve kriptografik anahtarlar kullabilir.
Dinamik Offline Doğrulama	Visa Mobil Platform'un Ödeme Uygulaması offline işlemlerde onaylama mekanizması olarak Dinamik Veri Doğrulama (Dynamic Data Authentication, DDA) özelliği sağlayabilir.

7.7. Mobil Uygulama

7.7.1. Ödeme işlemi

Visa Mobil Platformun sunduğu Mobil Ödeme uygulaması mobil cihazlar üzerinde son kullanıcıya zengin bir içerik ve görsellikle ödeme işlemlerini ve çeşitli bilgileri

sunar. Mobil Uygulama ile kullanıcı temel işlemleri yapabildiği gibi çeşitli ilave özelliklerle yaptığı işlemleri izleyebilir. Mobil Uygulama mevcut temassız terminallerle sorunsuz şekilde çalışabilir.

Mobil Uygulamanın ödeme işlevlerine Şekil 7.8'de gösterildiği gibi Ödeme Ana Ekranından erişilir. Bu işlevlere manuel olarak menülerden seçimle erişilebileceği gibi ileride anlatılacağı üzere diğer durumlarda da erişilebilir.

Şekil 7.8 Visa Mobil Platform Mobil Uygulama Ödeme işlemi ekranı

7.7.2. Ödeme tipleri

Visa Mobil Platform'un güçlü ve esnek yapısı sayesinde, mobil ödeme işlemlerinin takibi ve gerçekleştirilmesi, halihazırda kullanılan temassız işlemleri yaptığından daha zengin imkanlar ve sunum sağlar. Mevcut işlemlerde kullanılan CVM doğrulama mekanizmasında 4 haneli şifre kullanılarak doğrulama yapılmaktadır. Mobil Uygulamaların ve mobil cihazların gelişmesiyle beraber çok yakın bir gelecekte CVM doğrulama adımında sade 4 basamaklı şifreler değil parmak izi gibi daha farklı doğrulama mekanizmaları da kullanılabilir hale gelecektir. Böylece Visa Mobil Platform içinde işlemlerin güvenliği bir kat daha arttırılmış olur. Mobil

cihazlar bu tür genişletme ve gelişmeler için uygun ortamlar sağlayabilir. Ancak halihazırda kullanılan temassız kart ve ödeme teknolojilerinde bu imkanları kullanmak mümkün değildir.

Yüksek değerli ödemeler

Temassız ödeme işlemlerinde, her bir ödeme işlemi Visa'nın belirlediği limitlere göre yönetilirler. Bu limitler Avrupa'da farklı yerlere göre değişebilmektedir. Bu değer İngiltere'de 10£ iken diğer Avrupa ülkelerinde ise 20€ civarındadır.

Visa Mobil Platform'da bu limit değerleri aşan temassız işlemlerde Mobil Uygulama kullanıcıdan doğrulama istemektedir. Eğer diğer sayaçlar ve limitler aşılmıyorsa işleme izin verilir.

Düşük değerli ödemeler

Bölgesel limitlerin altında gerçekleşen temassız ödeme işlemleri, eğer Ödeme Uygulamasının çeşitli sayaçları ve limitleri açısından herhangi bir ihlal yok ise kabul edilir. Bu işlem gerçekleşirken Ödeme Uygulamasının offline risk yönetimi ile karar verilir.

7.7.3. Ödeme işleminin başlatılması

Visa Mobil Platform, kullanıcının ödeme işlemini istediği şekilde başlatabilmesine olanak tanır. Mobil Uygulama kullanıcısı gerekli ayarlamaları yaparak, mobil cihazını temassız kart okuyucuya yaklaştırdığında Mobil Uygulamanın Ödeme işleminin otomatik olarak çalışmasını ayarlayabilir. Mobil cihaz temassız kart okuyucuya yaklaştırıldığında Ödeme Ekranı çalıştırılır. Mobil Uygulama kullanıcısı isterse gerekli ayarlamaları yaparak Ödeme ekranının kullanıcının kendi kontrolünde çalışmasını sağlayabilir. Bu durumda kullanıcı mobil uygulamayı kullanarak Ödeme Ekranını seçer ve gerekli izinleri verdikten sonra bir dokuşta temassız ödeme işlemlerini yapabilir.

Ödeme işleminin elle başlatılması

Visa Mobil Platform kullanıcıları mobil cihazlarında yüklü olan Mobil Uygulamayı menüden elle seçerek başlatırlar. Kullanıcının daha önceden yapmış olduğu ayarlamalara göre mobil uygulama çalıştırıldığında doğrudan ödeme ekranı gelir veya mobil uygulamanın ana menü ekranı gelir. Mobil Uygulama açıldığında ana menü ekranı geliyorsa kullanıcı "PAY" seçeneğini seçerek ödeme işlemine geçebilir. Duruma göre ödeme ekranına girerken Mobil Uygulama kullanıcıdan şifre girmesini isteyebilir. Açılan ekranda kullanıcı tarafından girilen şifre kabul edilip onaylandıktan sonra mobil cihaz artık temassız kart okuyucuya yaklaştırılarak ödeme işlemi yapabilir. Şekil 7.9, Şekil 7.10, Şekil 7.11, Şekil 7.12 ve Şekil 7.13'de mobil cihaz ile elle ödeme işleminin yapılışı adım adım gösterilmektedir.

Şekil 7.9 Mobil uygulamanın seçimi.

Kullanıcı mobil cihazın menüsünden Mobil Uygulamayı seçer ve çalıştırır. (Şekil 7.9)

Şekil 7.10 Mobil Güvenlik şifresi sorulma ekranı

Mobil Uygulama kullanıcıyı doğrulamak için güvenlik şifresini sorar. (Şekil 7.10)

Şekil 7.11 Temassız okuyucuya yaklaştır mesajı

Güvenlik kodu doğrulandığında mobil cihaz temassız okuyucu üzerine getirilmesi için mesaj çıkar. (Şekil 7.11)

Şekil 7.12 Temassız okuyucu ile ödeme işlemi

Kullanıcı ödeme işlemi yapmak için mobil cihazı temassız kart okuyucu üzerine yaklaştırır. (Şekil 7.12)

Şekil 7.13 Ödeme sonuç ekranı

Ödeme işlemi yapılır. Kullanıcıya ödeme bilgisi mesaj olarak bildirilir. (Şekil 7.13)

Visa Mobil Platform kullanıcısı mobil uygulamanın çalışmasını elle yapılır şekilde ayarladığında, ödeme işlemini tek dokunuşta, mobil cihaz temassız kart okuyucusuna bir defa yaklaştırılarak gerçekleştirilir.

Ödeme işleminin başlatılamasından önce kullanıcı güvenlik şifresini girdiğinden dolayı, Ödeme Uygulamasının CVM mekanizması onay verir. Böylece tek dokunuşluk işlem yapılabilir.

Ödeme işleminin otomatik başlatılması

Visa mobil Platform Ödeme Uygulaması ayrıca otomatik ödeme imkanını da sunar. Kullanıcının bu seçimi ile mobil cihazın doğrudan temassız kart okuyucusuna yaklaştırılması ödeme işleminin yapılması için yeterli olacaktır. Mobil cihaz temassız kart okuyucuya yaklaştırıldığında işlemler Şekil 7.14 ve Şekil 7.15'te gösterildiği gibi işletilecektir.

Şekil 7.14 Mobil cihaz temassız okuyucuya yaklaştırılır

Kullanıcı mobil cihazı temassız kart okuyucuya yaklaştırır ve otomatik olarak ödeme uygulaması çalışır. (Şekil 7.14)

Şekil 7.15 Ödeme bilgi ekranı

Temassız Ödeme işlemi tamamlanır ve kullanıcıya bilgi verilir. (Şekil 7.15)

Kullanıcıdan onay alınması veya bilgilendirilmesi, ödeme işleminin değeri ile belirlenir. Bu değer hem üye işyerinin terminal limitleri hem de mobil cihazda bulunan Ödeme Uygulamasının üzerinde bulunan krediye göre kıyaslanır.

Kullanıcı düşük değerli ödeme yapmak istediğinde, mobil cihazda otomatik ödeme şekli seçilmişse, Ödeme Uygulamasının sahip olduğu kredi miktarı işlemi yapmaya yeterli ise mobil cihazın tek dokunuşu ile işlem tamamlanır.

Eğer Ödeme Uygulamasının kredisi işlemi yapmak için yeterli değilse veya işlem tutarı yüksek değerli ise Mobil Uygulama kullanıcıdan onay ister. Şekil 7.16, Şekil 7.17, Şekil 7.18, Şekil 7.19 ve Şekil 7.20'de bu durumdaki ödemelerin akışı gösterilmektedir.

Şekil 7.16'da kullanıcı yüksek tutarlı bir ödeme miktarı ile işlem yapmak istemektedir. Mobil Uygulama otomatik ödeme seçeneği ile ayarlanmıştır.

Şekil 7.16 Mobil cihaz temassız okuyucuya yaklaştırılır

Kullanıcı mobil cihazı temassız kart okuyucuya yaklaştırır ve Mobil Uygulama otomatik olarak çalışır. (Şekil 7.16)

Ödeme Uygulaması mobil cihazda yüklü kredinin işlem için yetersiz olduğunu tespit eder. İşlem durdurulur ve kullanıcıdan onay istenir. Kullanıcı güvenlik kodunu girerek işleme onay verir. (Şekil 7.17)

Şekil 7.17 Kullanıcı onayı girişi

Kullanıcı şifresini girdikten ve Ödeme Uygulaması tarafından onaylandıktan sonra işlemin devam etmesi için kullanıcıya mesaj verilir. Mobil cihazın temassız kart okuyucuya tekrar yaklaştırılması istenir. (Şekil 7.18)

Şekil 7.18 Mobil cihaz tekrar temassız kart okuyucuya yaklaştırılmalıdır

Şekil 7.19 Mobil cihaz temassız kart okuyucuya tekrar yaklaştırılır

Mobil cihaz ikinci defa temassız kart okuyucuya yaklaştırıldığında işleme devam edilir. (Şekil 7.19). İşlem sonunda kullanıcıya bilgi verilir. (Şekil 7.20)

Şekil 7.20 İşlem tamamlanır ve kullanıcıya mesaj verilir

Online ödeme işlemleri

Visa Mobil Platform, online ödeme işlemlerinde de Visa'nın kurallarına uymaktadır. Eğer Temassız kart okuyucusu ve ödeme uygulaması online işlem yapma yeteneğine sahip ise ve yapılan işlem offline olarak gerçekleştirilemiyorsa işlem Visa'nın kuralları dahilinde online olarak gerçekleştirilebilir.

7.7.4. Hesap bakiyeleri

Mobil Uygulama kullanıcıları mobil cihaz üzerinde yüklü olan Visa Mobil Platform Ödeme uygulamasının offline bakiye bilgisini görebilirler. Mobil Uygulamanın ana menüsünden "Account Balance" seçeneğini seçerek offline bakiye bilgi ekranı gösterilir. Şekil 7.21'de mobil uygulama üzerinde Bakiye İzleme ekranının bir görüntüsü vardır.

Şekil 7.21 Offline Bakiye ekranı

7.7.5. İşlem geçmişi ve detaylandırma

Visa Mobil Platform'un Mobil Uygulaması kullanıcılara alışverişin doğasına daha yakın bir görsellik sunar. Kullanıcıların yapmış olduğu işlemlerin bilgilerini tuttuğu gibi ayrıca alış verişte çeşitli bilgileri de kaydedebilir. Bu bilgiler çeşitli resim, ses, video ve not bilgileri olabilir. Aşağıdaki sekillerde ödeme işlemi sırasında mobil uygulamanın bu özelliği gösterilmektedir.

Kullanıcı ödeme işlemini yaptığında mobil uygulama ödeme işlemi için herhangi bir hatırlatma notu alınıp alınmayacağını sorar. (Şekil 7.22)

Şekil 7.22 Kullanıcı temassız ödeme işlemini yapar

Örnekte kullanıcı hatırlatma not tipi olarak Resim tipini seçer. Mobil Uygulama mobil cihazın kamerasını açar ve ürünün resmini çeker. (Şekil 7.23)

Şekil 7.23 Ürün resmi çekilir

Çekilen resim mobil cihaz üzerine kaydedilir ve kullanıcı isterse bir not mesajı girebilir. (Şekil 7.24, Şekil 7.25) Kayıt işlemi sonunda işlemin başarı durumu kullanıcıya bir mesaj ile bildirilir (Şekil 7.26)

Şekil 24 Resim kaydedilir

Şekil 25 Kullanıcı not girebilir

Şekil 26 Hatırlatma notu alındı mesajı

Mobil Uygulama kullanıcısı daha sonra menüden seçerek önceki işlemlerde alınmış hatırlatma notlarını görebilir. Visa Mobil Platform'un Mobil Uygulamasında kayıt mekanizması FIFO temelli bir sistem ile çalışır. Kapasitesi dolan mobil cihazın üzerindeki en eski hatırlatma notu silinir. Yeni hatırlatma notu eklenir.

Şekil 7.27'de mobil uygulamanın hatırlatma notu izleme ekranı görülmektedir.

Şekil 7.27 Hatırlatma notu izleme ekranı

7.7.6. Banka yardım masası erişimi

Kullanıcının herhangi bir sorununda bankanın yardım masasına kolayca erişebilmesi için Mobil Uygulamada otomatik arama seçeneği vardır. Kullanıcılar isterlerse yardım alabilecekleri yardım masası telefonlarını değiştirebilirler. Şekil 7.28'de yardım masası bağlantı ekranı görülmektedir.

Şekil 7.28 Yardım masası bağlantısı

7.7.7. Konfigurasyon yönetimi

Visa Mobil Platform Mobil Uygulama kullanıcıları Ayarlar ekranından kendi uygulamalarının ayarlarını değiştirebilirler. Bu ayarlar menüsünde Ödeme Uygulamasının default uygulama olması ve güvenlik şifresini değiştirebilirler. Şekil 7.29'da ayarlar ekranı görülmektedir.

Şekil 7.29 Ayarlar ekranı

7.7.8. Yardım konuları

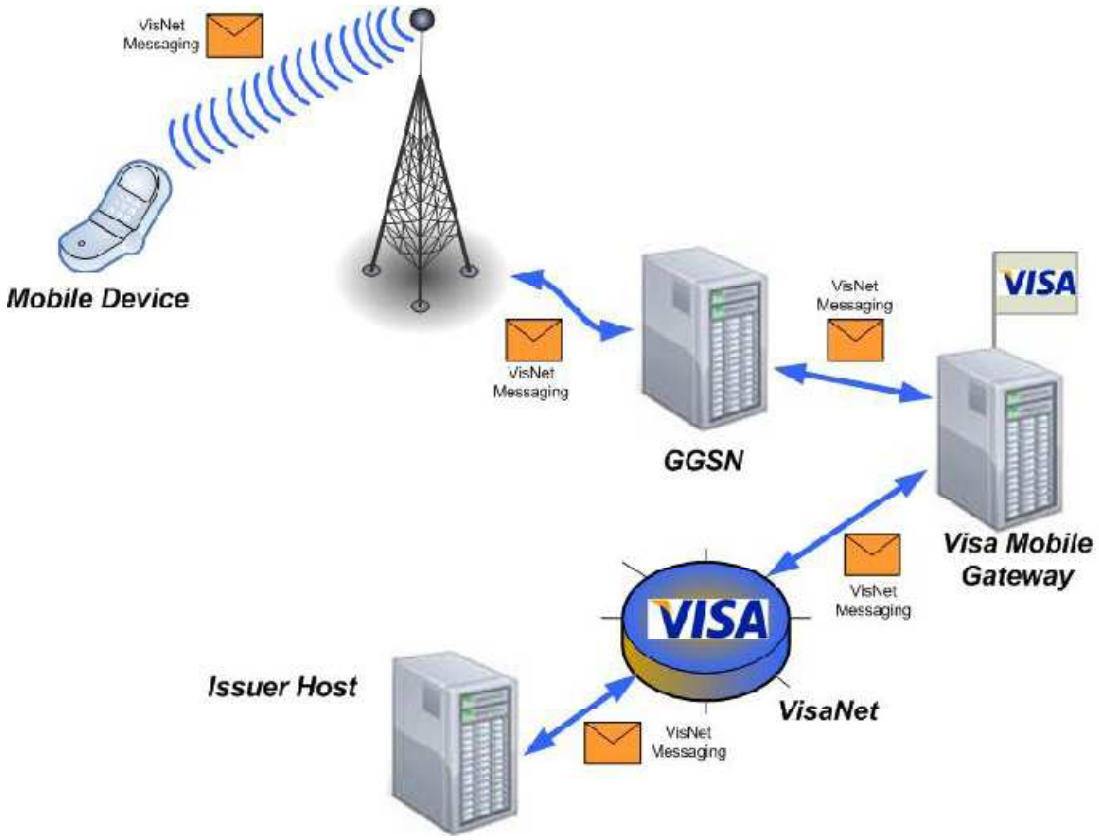
Visa mobil Platform Mobil Uygulaması alan duyarlı yardım özelliğine sahiptir. Uygulama içinde bağlantısı olan yerlerden yardım istendiğinde yardım bilgileri ekranda gösterilir. Ayrıca kullanıcılar isterlerse ana menüden yardım seçeneğini seçerek de yardım bilgilerine ulaşabilirler. Şekil 7.30'da yardım bağlantıları ekranı gösterilmektedir.

Şekil 7.30 Yardım bilgileri ekranı

7.8. Visa Mobil Gateway

Visa Mobil Gateway, mobil uygulama kullanıcılarının işlem akışlarını mevcut host sistemlerinin değiştirilmeden kullanılabilmesi için tasarlanmıştır. Visa Mobil Gateway, Mobil operatörlerin GGSN'lerine bağlanan web sunucularının mevcut ödeme sistemi arayüzlerine bağlanarak bu işlemi gerçekleştirirler. Mobil cihazlar bankanın verdiği URL'leri kullanarak GPRS bağlantısı ile bankaların ödeme servislerine erişirler.

Mobil Uygulama bir kere Visa Mobil Gateway'e bağlandıktan sonra banka sunucusu ile VisaNet üzerinden herhangi bir kısıtlama olmaksızın iletişimine devam edebilir. Bu şekilde bağlantı ile Ödeme uygulaması kilitleme, güvenlik kodu kilitleme gibi işlemler Acquier banka ve üye işyeri temassız okuyucusu olmaksızın uzaktan işletilebilirler.



Şekil 7.31 Visa Mobil Gateway mimarisi

Şekil 7.31'de Visa Mobil Gateway'in mimarisi ve çalışma şekli gösterilmektedir.

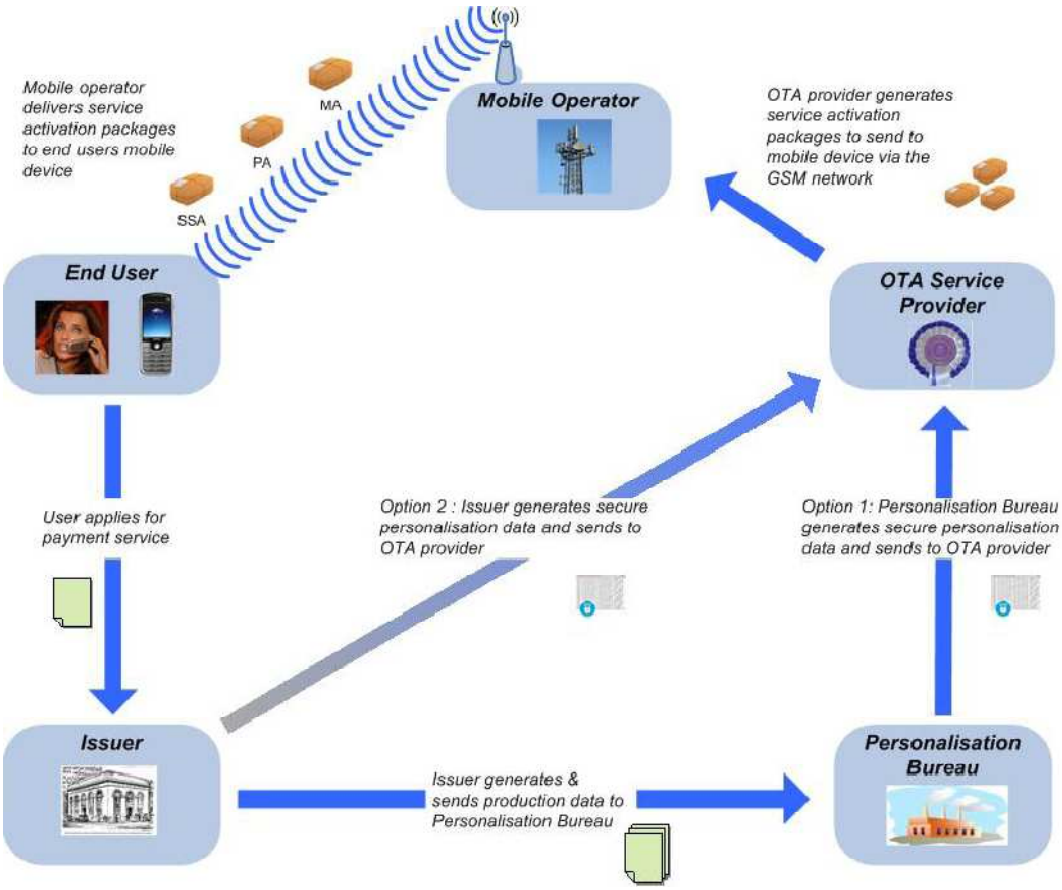
Visa Mobil Gateway'in gücü ve esnekliği, mevcut olan VisaNet mesajlaşmasının hali hazırda kullanılmakta olan geleneksel kart işlem ve ortamlarını yeniden kullanabilmesidir. VisaNet mesajlaşmaları mobile gateway ile kablosuz olarak taşınabilmektedir.

7.9. Servis Aktivasyonu

Mobil Ödeme uygulamasının dağıtımı ve yönetimi mevcut kullanılan kart uygulamalrının dağıtım ve yönetiminden önemli şekilde farklıdır. Her iki platform da aynı kart sahibi bilgilerini kullanıyorsa ve benzer kişiselleştirme gereksinimlerine sahipse de, kart uygulamasını kişiselleştiren Personalizasyon ofisinin mobil cihaza erişiminin mümkün olamamasından dolayı dağıtım ve yönetim şekli değişecektir. Normal kartlı ödeme sistemlerinde, kart sahibi bilgileri kart uygulamaları üzerine

Personalizasyon Ofisinde yazılmaktadır. Akıllı kartlar Personalizasyon Ofislerinde fiziksel olarak bulunurlar. Visa'nın güvenlik kuralları altında kişiselleştirilirler.

Mobil cihazların Ödeme uygulamalarını kişiselleştirmek için mobil cihazlar Personalizasyon Ofisine gönderilemeyeceği için farklı teknikler geliştirilmiştir. Bu ihtiyacı karşılamak için kişiselleştirme servislerini mobil cihazlara taşıyan güvenli bir kablosuz kanal oluşturulur. Şekil 7.32'de bir mobil cihazın Visa Mobil Platform Ödeme uygulamasının servis aktivasyonu işlemi gösterilmektedir.



Şekil 7.32 Mobil Ödeme uygulaması dağıtım modeli

Visa Mobil Platform kullanıcıları bu servislerin kullanım kanallarını geleneksel iletişim kanalları kullanarak da yapabilirler. Ancak Visa Mobil Platform uygulama dağıtım modeli kullanımında, kart sahibi bankaların mobil ödeme uygulamalarını müşterilerinin mobil cihazlarına yükleyebilmeleri için bir çok seçeneğe sahiptir.

Her nekadar sonuçta kart sahibi bankanın seçimi Visa Mobil Platform servislerinin dağıtımını belirlese de OTA'nın kısıtlarına bağımlıdır. Daha önce OTA'nın işlevinde anlatıldığı gibi Mobil Uygulama ve Mobil uygulamanın kişiselleştirme bilgilerinin son kullanıcılara ulaştırılmasında mobil operatörlerin belirleyiciliğindedir.

Şekil 7.32'de mümkün olan iki dağıtım modeli gösterilmektedir. Birinci seçenekte kart sahibi bankanın kişiselleştirme bilgilerini OTA sunucularına eriştirmek için Personalizasyon Ofisine göndermesi ve onunda OTA sunuculara ulaştırması ile yapılamaktadır. Bir diğer yöndem de Personalizasyon bilgilerinin OTA sunucularına doğrudan ulaştırılmasıdır.

Bazı ticari uygulamalarda OTA sunucuları Personalizasyon Ofislerini de içermektedir. Böylece mobil cihazlara gönderilecek güvenli veriyi OTA sunucuları kendileri üretebilmektedirler. Diğer bir şekilde de kart sahibi banka kişiselleştirme bilgilerini kendi ofislerinde güvenli hale sokmaktadırlar. Bu daha az maliyetlidir. Güvenli data doğrudan OTA servis sağlayıcılarına gönderilir.

Bu aşamadan sonra OTA servis sağlayıcısının görevi mobil servis aktivasyon paketlerinin oluşturulması, mobil uygulama, ödeme uygulaması ve kişiselleştirme verilerinin aktifleştirilmesidir. Servis aktivasyon paketleri mobil cihazlara OTA servis sağlayıcılar tarafından mobil operatörlerin sağladığı GSM mobil ağ üzerinden ulaşılarak kurulur.

Mobil cihaza ilk gönderilen paket Servis aktivasyon uygulamasını içeren SMS servis aktivasyon paketidir. Servis aktivasyon uygulaması mobil cihaza yüklenir. Servis Aktivasyon SMS mesajı mobil cihaz kullanıcısının onayı ile çalıştırılır. Bundan sonra mobil cihazın kapasitesi ölçülerek, gerekli ek yüklemeler yapılır.

Mobil cihaz, Visa Mobil Platform Mobil Uygulamayı çalıştırabilir hale geldikten sonra Mobil Uygulama indirilir ve kurulur. Daha sonra Ödeme Uygulaması indirilir ve kurulur. En son olarak da kart sahibi bankanın gönderdiği kişiselleştirme verileri indirilir. Bir kere Servis Aktivasyon uygulaması yüklendikten sonra, kullanıcının

mobil cihazında hem mobil uygulamayı hem de ödeme uygulamasını kurar ve kişiselleştirerek uygulamaları aktifleştirir.

7.10. Visa Mobil Platform Güvenliği

Visa Mobil Platform Mobil Ödeme Uygulaması güvenlik için içerik tabanlı bir güvenliği kabul eder ve uygular. Uygulamanın güvenliği her bir bileşen ve tabaka içinde gerçekleştirilir. Böylece yeterince kararlı ve sağlam bir güvenlik mekanizması sağlanmış olur. Devam eden bölümlerde Visa Mobil Platform bileşenlerinin uygulama içerikleri ve güvenlik sınırlamaları ifade edilmektedir.

7.10.1. Mobil uygulama

Mobil Uygulama, mobil cihaza bir kere yüklendikten sonra iki güvenlik metodunu gerçekleştirir. Bunu gerçekleştirmesinin sebepleri;

- Mobil uygulama sadece ilişkilendirilmiş bir tane ödeme uygulaması ile çalışabilir.
- Ödeme uygulamasına erişim sadece uygulamanın güvenlik kodu ile gerçekleştirilebilir.
- Önemli kişisel bilgilere sadece uygulama güvenlik kodu ile erişim gerçekleştirilebilir.

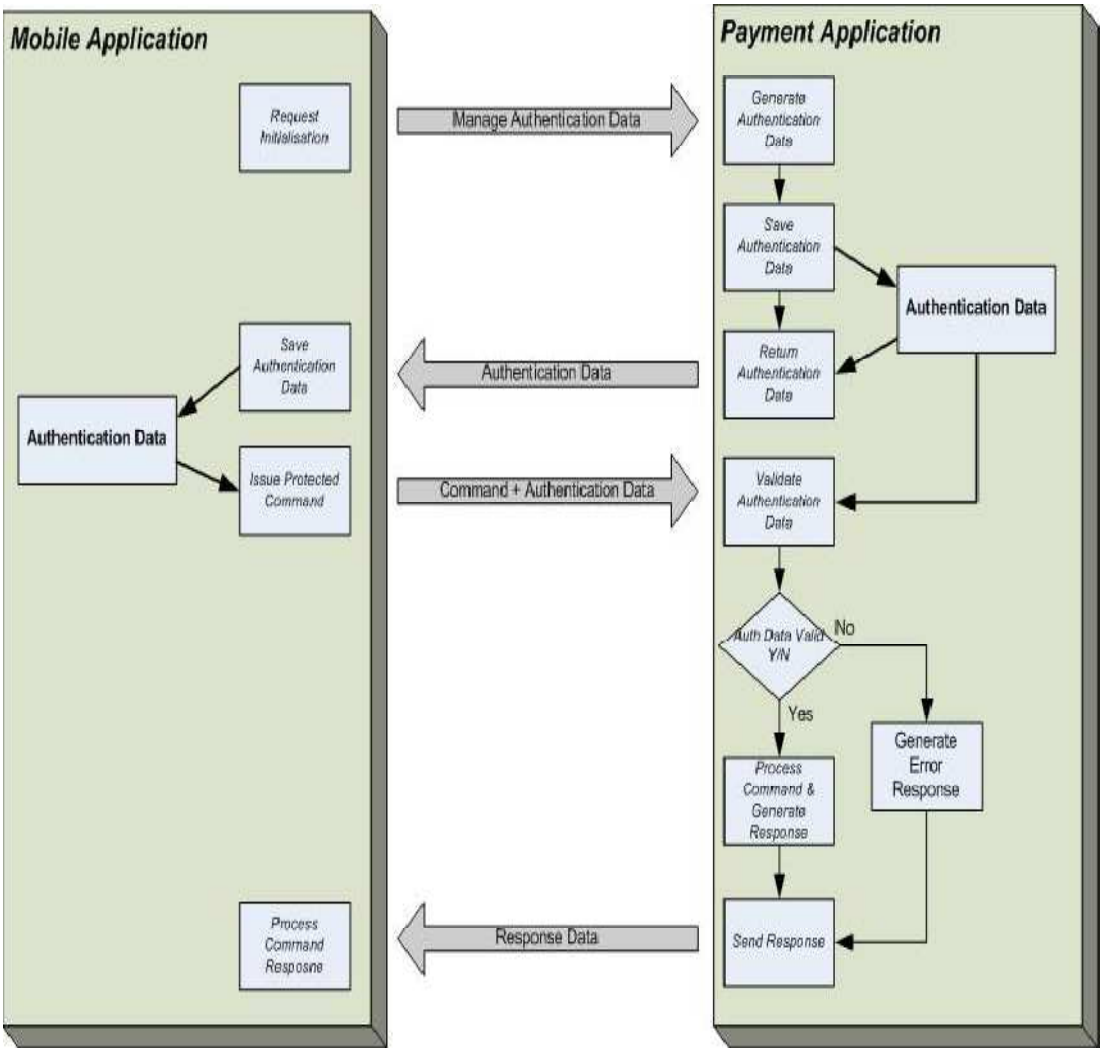
Mobil Uygulama – Ödeme Uygulaması eşleştirmesi

Servis aktifleştime işlemlerinin bir parçası da Ödeme Uygulaması ve Mobil Uygulamanın karşılıklı olarak eşleştirilmesidir. Uygulamaları eşleştirilmesinde karşılıklı olarak karşılıklı doğrulama (Mutual Authentication) verilerinin üretilmesi ve takası yapılır. Doğrulama verisi Ödeme Uygulaması tarafından, mobil cihazdan gelen MANAGE AUTHENTICATION DATA komutu ile üretilmektedir. Doğrulama verisi mesajın bir parçası olarak mobil cihaza geri gönderilir.

Gönderilen doğrulama verisi geçerli değil ise, Ödeme Uygulaması Mobil Uygulamadan gelen hiç bir komutu çalıştırmayacaktır.

Doğrulama verisi Ödeme Uygulamasının talep ettiği durumlarda Mobil Uygulama tarafından tekrar üretilebilir. Doğrulama verisi sadece kurulum ve servis aktivasyonları sırasında üretilemezler.

Mobil Uygulama, doğrulama verisini karıştırarak, mobil cihazın silinmeyen bir hafıza bölgesine yazarak saklar.



Şekil 7.33 Doğrulama verisi üretim ve kullanımı

Şekil 7.33'te Mobil uygulama ve Ödeme Uygulaması arasında takas edilen doğrulama verisinin üretilmesi ve kullanımı gösterilmektedir.

Güvenlik kodu

Ödeme Uygulaması fonksiyonellikleri, kişisel veriler dört basamaklı bir sayı ile korunabilirler. Ödeme Uygulaması bu güvenlik kodunun oluşturulmasını servis aktivasyonu sırasında yapar.

Mobil Uygulama, Visa Mobil Platform Ödeme Uygulamasının komut setini kullanarak yeni bir güvenlik kodunun oluşturulmasını sağlayabilir. Ödeme Uygulaması oluşturulan bu güvenlik kodunu, ileride güvenlik doğrulama işlemlerinde kullanmak üzere dahili bir yazmacında saklar. Bu güvenlik koduna Ödeme Uygulamasının dışından erişim mümkün değildir. Güvenlik koduna sadece Ödeme Uygulaması erişebilir.

Visa Mobil Platform Mobil Uygulaması, her bir özel korunmuş metodun çalıştırılmasından önce güvenlik kodunu istemektedir. Eğer girilen güvenlik kodu doğru ise Ödeme Uygulaması tarafından olumlu bir cevap verilir.

Ödeme Uygulaması dahili yazmaçlarında sakladığı güvenlik kodu ile girilen değeri karşılaştırır. Yanlış güvenlik kodu girişlerinde, dahili bir PIN deneme sayısı değeri bir arttırılır. Eğer bu pin deneme sayısı, yine dahili yazmaçlardan birinde tutulan PIN deneme limiti değerini geçmiş ise Ödeme Uygulaması bloke olur. Bu durum gerçekleştikten sonra artık Ödeme Uygulaması hiç bir komuta cevap vermez. Bu PIN deneme limit aşım durumu kart sahibi banka tarafından gönderilecek olan özel komutlar ile kaldırılabilir. Kart sahibi bankanın göndereceği komutlar PIN demene sayısını sıfırlar, Ödeme Uygulamasını tekrar kullanılabilir hale getirir.

7.10.2. OTA ve servis aktivasyonu

Global Platform güvenlik alanı

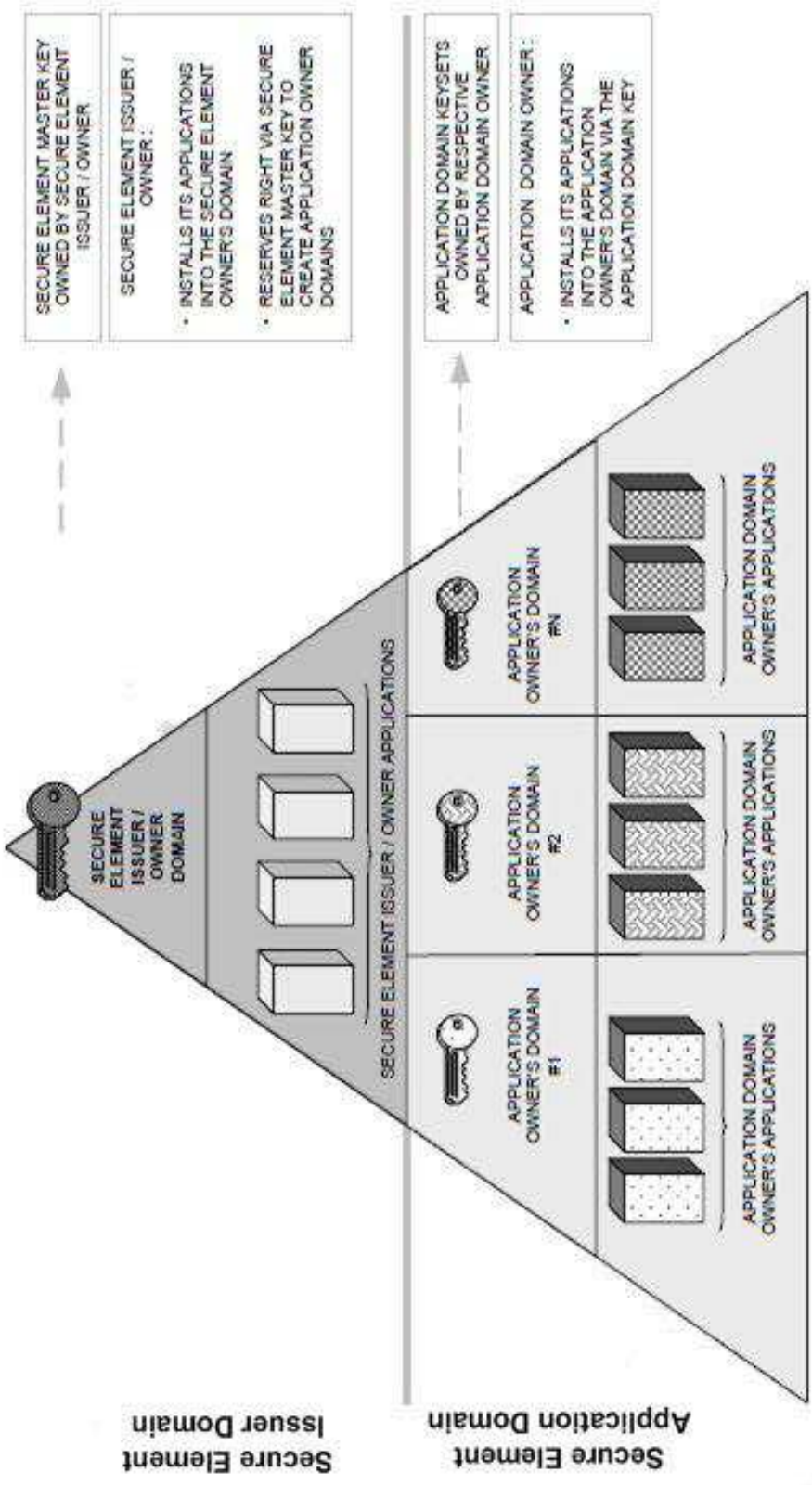
Mobil cihazların Visa Mobil Platform içinde kullanılabilmesi için mutlaka güvenli elemanı (Secure Element) içermeleri gerekmektedir. Bölüm 7.5’te Ödeme Uygulamasının mobil cihazlarda hangi şekillerde GlobalPlatform tarafından sunulan güvenli elemanlar üzerinde sunulabileceğini göstermektedir. Visa Mobil Platform,

servis aktivasyon ve OTA işlem onaylama sırasında GlobalPlatform'un dahili güvenlik mimarisini kullanmaktadır.

Şekil 7.34'te gösterildiği gibi GlobalPlatfrom bir kaç seviye halinde dahili güvenlik mimarisini kurmuştur. En yüksek seviye Kart sahibi Güvenlik Alanı (Issuer Security Domain, ISD) şeklinde isimlendirilir. Bu alan Güvenli Elemanın sahibi tarafından yönetilir.

Güvenli Elemanı sağlayan firma ile Ödeme Uygulamasını sağlayan firmanın aralarındaki iş ilişkisine ve anlaşmalarına bağlı olarak Ödeme Uygulamaları Kart sahibi Güvenlik Alanında, ISD, veya ayrı bir Uygulama Güvenlik Alanında (Application Security Domain, ASD) bulunabilirler.

Bir güvenlik alanı, içinde bulunan uygulamalara erişimi denetleyen bir koruma uygulaması altında korunan uygulamalardır. Bu güvenlik alanındaki uygulamalara erişim, bölgeyi koruyan uygulamanın onaylayacağı doğrulama verisi ile gerçekleşebilir. Onaylama verisi doğrulanmayan girişlere izin verilmez. Onaylama verisi doğrulanmayan girişler bu bölgedeki uygulamalara erişemez ve onların durumlarını değiştiremezler.



Şekil 7.34 GlobalPlatform Güvenlik Mimarisi

Bu kuralın bir istisnası Kart Sahibi Güvenlik Alanının, ISD, sahibinin bir Uygulama Güvenlik Alanınındaki, ASD, uygulamalara erişebilmesidir. ISD güvenlik bölgesine sahip olan kart üzerindeki diğer ASD alanlarındaki uygulamaları yönetebilir. Onları etkisiz hale getirebilir.

Güvenlik alanları uygulamaları ve onların verilerini kriptografik anahtarlar ile korurlar. Her bir ISD veya ASD üç kriptografik anahtar ile oluşturulur. Güvenlik alanları bu üç kriptografik anahtarı kullanarak erişimleri ve güvenliği yönetirler.

BÖLÜM 8. SONUÇ VE DEĞERLENDİRMELER

Akıllı kartlar ve Radyo frekanslı tanıma sistemleri uzun süreden beri gerçek uygulamalarda kullanılmaktadır. Bu süre içinde her iki teknoloji de rüşdünü ıspatlamıştır. Çok yakın bir süreden beri de mobil dünyanın gelişmesiyle beraber bu her iki teknolojiyi taşınabilir cihazlarda toplayan teknoloji de gelişmektedir. NFC teknolojisinin gelişiminde katkısı olacak pazarın lokomotif unsuru bankalardır. Bankaların katkısı ile NFC uygulamaları yaygınlaşacaktır.

Visa ve Mastercard'ın önemli katkıları ile temassız ödeme işlemlerinde hatırı sayılır ilerlemeler kaydedilmiştir. Ödeme işleminin doğasına daha yakın olan temassız ödeme basit, hızlı, güvenli ve kolay anlaşılır şekilde gerçekleşir. NFC temel olarak bir temassız ödeme teknolojisi şeklide tanıtılsa da diğer bir çok çeşitlilikte uygulamaları da mevcuttur. Teoride NFC uygulamaları sonsuz çeşitliliktedir. Kullanıcılar NFC mobil cihazlarını markette alışveriş yaparken, otopark ve konutlara girerken, ulaşımda, karayolları geçiş ödemelerinde, yakıt alırken, elektrik, su ve doğalgaz sayaçlarının yüklenmesinde, elektronik bilet kullanımında, akıllı posterlerde, sosyal network uygulamalarında ve bunun gibi bir çok uygulamalarda kullanabilirler. Ayrıca bilgi servislerinin yüklenmesi de yepyeni bir kullanım alanı oluşturmaktadır. Akıllı posterlerden içerik yükleme, etkinlik bileti satma, müzik ve film indirme gibi yeni özellikler yeni iş şekillerini de üretecektir.

NFC ürün denemeleri global ölçekte yaygınlaşmakta ve bir biri ile iletişime geçmektedir. 2007 yılında başlanan ve GSMA tarafından yönetilen, dünya çapında 50 mobil network operatörünün katılımı ile gerçekleşen Pay-Buy-Mobile (PBM) projesi olumlu sonuçlar vermeye başlamıştır. GSMA'ya göre kullanıcılar artık PBM ile ödemeyi tercih etmektedirler.

Elbette her yeni teknoloji gibi NFC teknolojisinin kullanımında da çözülmesi gereken bazı sorunlar vardır. NFC teknolojisi halen test edilmekte olan bir teknolojidir. Henüz cevaplanamamış bir çok soru vardır.

Katı kurallara bağlı bankacılık uygulamaları temassız servislerini mobil operatörlere açacaklar mı? Teknolojideki "Smart" vurgusu NFC kullanıcılarını sinemaya veya stadyuma sevkedecek mi? Stadyumlardaki gibi kalabalık grupların mobil teknolojiyi kullanmaları mobil servis sağlayıcıları nasıl etkiler?

NFC'nin gücü aynı zamanda zayıflığıdır. Bir çok temassız teknolojiyi bir tek standart altına toplamak neredeyse imkansızdır. Zaman içinde spesifikasyonların oluşturulması kaçınılmazdır.

Mobil cihazlar kime aittir? Sorumluluğu kimdedir? Mobil cihaz çalındığında üzerindeki işlemlerden banka mı yoksa mobil operatörler mi sorumludur? Birden fazla sadakat uygulamasının mobil cihazlar üzerinde sunulduğu uygulamalarda, bu uygulamaların sahibi bankalar bu uygulamalarını ve güvenlik özelliklerini paylaşmaktan memnun olurlar mı? Güvenliği kim yönetecek?

Marka da ayrıca önemli. Bankacılıkta kartlar üzerinde gösterilen logolar spesifikasyonlarda belirtilmiştir. Mobil cihazda bu bilgiler nasıl sunulacak? Müşteri bankaya mı yoksa mobil operatöre mi aittir?

Bunun gibi bir çok soru NFC teknolojisinin yaygın kullanımını etkilemektedir. Kar amacı gütmeyen bir kuruluş olan NFC Forum'un ve diğer teknoloji firmalarının yaptıkları bilimsel katkılar sayesinde teknolojinin artık rahatça kullanımını mümkün hale gelmiştir.

Çok yakın gelecekte etrafımızdaki bir çok nesne NFC sayesinde "Smart" hale gelecektir. Her akıllılaşan şeyle birlikte yeni iş imkanları ve modelleri de gelişerek yeni ekonomileri oluşturabilir.

KAYNAKLAR

[1] Kavas,A. “Enduktif Bağlaşımlı Radyo Frekans Kimlik Tanımlama Sistemi”, İstanbul, s.1, 2005

[2] http://www.rfidjournal.com/glossary/nearfield%20communication 05.02.2010

[3] http://www.nfc-forum.org 01.02.2010

[4] http://www.stolpan.com/uploadfiles/1_StoLPaNCartes%202007.pdf 12.12.2009

[5] NFC Data Exchange Format, Technical Specification, NFC Forum, NDEF 1.0 NFC-Forum-TS-NDEF_1.0 2006-07-24

[6] The J2ME Platform – Which APIs come from the J2SE(tm) Platform, Quasay Mahmoud, 2001 Java.sun.com>java>wirelessDeveloper>Technologies>MIDP>Articles

[7] Wireless Java 2 ME Platform Programming, Vartan Piroumian, 2002, Sum Microsystem Press

[8] Introduction to Wireless Java (tm) Technology, 2002 Java.sun.com>java>wirelessDeveloper>Quicklinks>Intro to Wireless

[9] Java 2 Platform Micro Edition (J2ME) Technology for Createing Mobile Devices, 2000, Sun Microsystems, White Paper

[10] Attacks On and Countermeasures for USB Hardware Token Devices, Kinpin

ÖZGEÇMİŞ

Mehmet Suyuti DİNDAR, 22.07.1975 yılında İstanbul'da doğdu. İlk, Orta ve Lise eğitimini İstanbul Fatih'te tamamladı. 1993 yılında İstanbul İmam Hatip Lisesinden mezun oldu. 1994 yılında başladığı Sakarya Üniversitesi Elektrik ve Elektronik mühendisliğini, bir yılı ingilizce hazırlık olmak üzere 1999 yılında tamamladı. 2000 yılından itibaren yazılım sektöründe çalışmaya başladı. Gömülü sistemler üzerine bir çok projede görev aldı. Halen kartlı sistemler ve Ödeme sistemleri alanında faaliyet gösteren Smartsoft firmasında Terminal ve Gömülü Sistemler Grup yöneticisi olarak görev yapmaktadır.