T.C. İSTANBUL TİCARET
ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AKILLI ŞEHİR OTOPARK SİSTEMLERİNDE NFC KARTLARIN ÖDEME ARACI OLARAK KULLANILMASI VE GÜVENLİK ALT YAPISI; İSPARK VE İSTANBUL KART ÖRNEĞİ

ALİ GÜNGÖR
1460Y63101

YÜKSEK LİSANS TEZİ
SİBER GÜVENLİK ANABİLİM DALI
İSTANBUL, TEMMUZ 2017

T.C. İSTANBUL TİCARET
ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AKILLI ŞEHİR OTOPARK SİSTEMLERİNDE NFC KARTLARIN ÖDEME ARACI OLARAK KULLANILMASI VE GÜVENLİK ALT YAPISI; İSPARK VE İSTANBUL KART ÖRNEĞİ

ALİ GÜNGÖR
1460Y63101

DANIŞMAN
Yrd. Doç. Dr. Erdinç ÖZTÜRK

YÜKSEK LİSANS TEZİ
SİBER GÜVENLİK ANABİLİM DALI
İSTANBUL, TEMMUZ 2017

KABUL VE ONAY SAYFASI

Ali GÜNGÖR tarafından hazırlanan **Akıllı Şehir Otopark Sistemlerinde Nfc Kartların Ödeme Aracı Olarak Kullanılması Ve Güvenlik Altyapısı; İspark Ve İstanbul Kart Örneği** adlı tez çalışması 20.07.2017 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü **Siber Güvenlik Anabilim Dalı**'nda yüksek lisans tezi olarak kabul edilmiştir.

	Adı-Soyadı	İmza
Danışmanı	**: Yrd. Doç. Dr. Erdinç ÖZTÜRK**	
Jüri Üyesi	**: Yrd. Doç. Dr. Muhammed Ali AYDIN**	
Jüri Üyesi	**: Yrd. Doç. Dr. Ali BOYACI**	

Onay Tarihi : 15.08.2017

Yrd. Doç. Dr. Berk AYVAZ

Enstitü Md. V.

AKADEMİK VE ETİK KURALLARA
UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

15../08../2017

Ali GÜNGÖR

İÇİNDEKİLER

ÖZET

Günümüzde akıllı tablet ve cihazlar sayesinde bilgisayar çağı bir üst seviyeye çıkmış bulunmakta ve yaşam standartlarımız da bu doğrultuda değişmektedir. Kullandığımız ödeme sistemleri, kredi kartları, debit kartlar vb. hayatımızın bir parçası olmuştur. Artan nüfus popülasyonu beraberinde güvenli alternatif ödeme sistemlerinide getirmiştir.

Bunlardan en önemlisi gelecekte hayatımıza daha çok etki edecek olan akıllı kartlardır. İstanbul gibi metropoliten ve trafiğin yoğun olduğu bir şehirde toplu taşımada büyük rol oynayan akıllı kartlar otopark sektöründe de kullanılmalıdır.

Akıllı kartlar kredi kartlarından ve diğer debit kartlardan daha güvenlikli diyebileceğimiz bir DES şifreleme yapısına sahiptir. Ayrıca her akıllı kartın kendine ait bir ID numarası olması, otoparkları kullanan müşterilerin bıraktığı kullanım istatistiklerinin toplanmasında ve kullanılmasında etkili olmaktadır.

Akıllı kartlar kullanımı kolay, güvenliği yüksek, kişisel veri açığı olmayan, dolumu basit, kırılması zor bir NFC ürünüdür. Bu nedenle otoparklarda ödeme aracı olarak kullanılması nakit ve diğer kartlara göre her zaman bir adım önde olmuştur.

Ayrıca İstanbul'da akıllı kartların toplu taşımadan sonra otoparklarda da ödeme aracı olarak kullanılması, hem kullanıcının işini kolaylaştırarak zaman tasarrufu yaptırmakta hem de İstanbul'u bir adım daha akıllı şehir düzeyine getirmektedir.

ABSTRACT

Today, with intelligent tablets and devices, the computer has reached an upper level and our living standards are changing in this direction. We use payment systems, credit cards, debit cards and so on. It is part of our life. The growing population has brought together safe alternative payment systems.<

The most important of these is the smart cards that will have more impact on our lives in the future. Smart cards, such as Istanbul, which play a major role in public transport in metropolitan and traffic-intensive cities, should also be used in the parking sector.

Smart cards have a DES encryption scheme which we can say is more secure than credit cards and other debit cards. In addition, each smartcard has its own ID number, which is effective in collecting and using usage statistics left by customers using car parks.

Smart cards are easy to use, high security, non-personal data-hungry, simple to refill, and difficult to break. For this reason, it is always one step ahead of cash and other cards to use as a payment tool in parking lots.

Furthermore, the use of smart cards in Istanbul as a means of payment in parking lots after mass transportation makes it easier for the user to save time and brings Istanbul to the next level of smart city.

TEŞEKKÜR

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli Danışman Hocam Yrd. Doç. Dr. Erdinç ÖZTÜRK'e teşekkürlerimi sunarım.

Tezimin yazım aşamasındaki desteklerinden dolayı İSPARK AŞ'ye teşekkür ederim.

Tezimin her aşamasında beni yalnız bırakmayan aileme sonsuz saygı sevgi ve saygılarımı sunarım.

Ali GÜNGÖR
İSTANBUL 2017

ŞEKİLLER

TABLOLAR

SİMGELER VE KISALTMALAR

FIFA : Uluslar Arası Futbol Federasyonu
İSPARK : İstanbul Otopark İşletmeleri
BT : Bilgi Teknolojileri
A.B.D. : Amerika Birleşik Devletleri
ISO : Uluslar Arası Kalite Standartları
TCB : Güvenli Hesaplama Esaslarının
TSE : Türk Standartları Enstitüsü
BGYS : Bilgi Güvenliği Yönetim Sistemi
ID : Kimlik
GSM : Mobil İletişim İçin Küresel Sistem
NFC : Yakın Alan İletişimi
ISIS : Ortaklık,Verizon, Barclaykart ve Discover
RFID : Radyo Frekansı ile Tanımlama
POS : Satış Noktaları Terminali
LLCP : Mantıksal Bağlantı Kontrol Protokol
URL : Standart Kaynak Bulucu
UICC : Evrensel Entegre Devre Kartı
ETSI : Avrupa Telekomünikasyon Standartlar Komitesi
SD : Çıkarılabilir Flash Hafıza Kart
AES : Gelişmiş Şifreleme Standardı
MAC : Ortam Erişim Yönetimi
CMAC : Yüksek Kripto Seviyesine Sahip Algoritma
OTA : Şebeke üzerinden güncelleme
HSM : Donanım Güvenlik Modülü
EPPROM : Elektronik Olarak Silinebilir, Programlanabilir Salt Okunur Bellek
SP : Servis Sağlayıcı
TSM : Güvenilir Hizmet Yöneticisi
MNO : Mobil Ağ Operatörleri
APDU : Uygulama Protokol Veri Birimi
IC : İçsel Alan
IEC : Uluslararası Elektroteknik Komisyonu
CAT TP : Card Application Toolkit Transport Protocol, Kart Uygulama Aracı İletişim Protokolü
HTTP : Üst metin Transfer Protokolü
SWP : Tek Tel Protokol
TDES : Üçlü Veri Şifreleme Standardı
IPSEC : İnternet Protokolü Güvenliği
IETF : İnternet Mühendisliği Görev Gücü
EPC : Olay Süreç Zinciri

GİRİŞ

Ülkemizde sanayinin ve ticaretin gelişmesi ile beraber, tarımla uğraşan kırsal kesimden sanayinin ve ticaretin geliştiği şehirlere göç başlamıştır. Bu göçün etkisi ile ülkemizde her dört kişiden üçü Cumhuriyetin ilk yıllarında kırsalda yaşarken, günümüzde şehirlerde yaşamaktadır. Şehirlerde artan nüfus yoğunluğu konut, altyapı, ulaşım, eğitim, sağlık, güvenlik, çevre ve enerji gibi alanlarda sorunları da beraberinde getirmiştir. Yerel idareciler, hem bu sorunları "akıllı"ca çözmeli hem de şehir halkına daha yaşanabilir şehirler sunmalıdır. Hızla gelişen bilgi ve iletişim teknolojileri, daha yaşanabilir şehirler için "Akıllı Şehir" çözümleri sunar. Bu çözümler birbiri ile uyumlu, ihtiyaçlara hitap eden, mümkün olan en son teknolojileri kapsayan Akıllı Şehir sistemlerinden oluşur. Akıllı sistemlerin akıllı çözümler üretmesinin de tek yolu, her gün binlerce donanımdan toplanan "Büyük Veri"nin akıllı süreçlerden geçerek şehir halkına ve yöneticilerine katma değerli bir bilgiye dönüşmesidir.

Şehrin nüfusu arttıkça enerji, su, sağlık, barınma, ulaşım, haberleşme, güvenlik gibi yaşamsal ihtiyaçların artması; bu ihtiyaçları karşılayan kaynakların daha verimli kullanılması için akılcı stratejiler geliştirmeyi zorunlu kılmaktadır. Günümüzde bir yandan şehirlerin sorunlarını çözerek onları daha yaşanabilir hale getirmek amaçlanırken, diğer yandan insanların hayat kalitesini iyileştirecek "Akıllı Şehir" çözümleri önem kazanmaktadır. Ayrıca gelişen teknolojiyle birlikte 1990'larda kullanılmaya başlayan mobil cihazlar ve telefonlar günümüzde kişisel bilgisayarların bile yerini alarak dijital ödeme dünyasında zirve yapmıştır [1].

İşte tamda bu noktada akıllı şehir kartları önemli bir role sahip olmaktadır. Gerek alışverişlerde kullanılması gerekse toplu taşıma, gerekse de parklanma.

Parklanma tabiri son yıllarda ortaya çıkmış yeni bir kelimedir. Artan nüfus yoğunluğu beraberinde tarik ve park sorununu da getirmiştir. İnsanlar kolay parklanacakları alanlar ve sistemlere gereksinim duymaktadır. İstanbul'daki trafiğin ise %49 gibi bir rakamı park yeri arama veya parklanma ihtiyacı için duraklama gibi sebeplerden meydana gelmektedir.

Bu tarz durumların yaşanmaması için akıllı şehir kartları ve uygun ödeme sistemleri bir arada müşteriye sunulmalı ve hizmet transferinin bedeli hızlı bir şekilde gerçekleşmelidir.

Bugün gerek Dünya Futbol Şampiyonası (FIFA), gerek Avrupa Futbol Şampiyonası (Günümüzde Euro 2016), gerekse de Olimpiyat Oyunları için Türkiye'nin simgesi İstanbul olmaktadır. İstanbul bu gibi organizasyonlarda New York, Singapur, Sydney, Tokyo, Barcelona, Roma, Londra, Lizbon gibi akıllı şehirciliğin üst düzeyde olduğu şehirler ile kıyaslanmakta ve rekabete tutulmaktadır. Tüm bu şehirlerin ortak yanı ise, her şehrin kendisine has city kartını vatandaşların şehirdeki her aktive de etkili bir biçimde kullanabilmeleridir.

Örneğin herhangi bir vatandaş sahip olduğu city kartını park etmede, alışverişte, benzin alımlarında, market alışverişlerinde, hatta anlaşmalı olan çoğu giyim firmalarında kullanabilmektedir.

İstanbul, bu gibi rakipler ile baş edebilmek için İSPARK gibi akıllı şehirciliği destekleyen kamu iştiraki firmaların gücüne ve yaratıcılığına ihtiyaç duymaktadır. Fakat önce bu firmaların kendi içlerinde BT sistemlerini oturtmuş etkili teknoloji kullanan ve çağdaş bir kurum olması gerekmektedir.

1. AKILLI ŞEHİRLER

BT, bir işletmenin üretkenlik ve etkinliğini arttırabilmek için yöneticilerin kullanabileceği en önemli araçlardan biridir. Aynı zamanda diğer standart sistemlere güvenlik düzeyi politikaları bir hayli gelişmiştir.

Bilgi teknolojileri sürekli gelişen ve değişen bir yapıda olduğundan, bilgi güvenliğinin bir defaya mahsus sağlanması veya yapılandırılması kurumsal bilgi sistemleri açısından yeterli değildir. Kurumsal bilgi güvenliğinin sağlanabilmesi amacıyla bilgi güvenliği yaşayan bir süreç olarak ele alınmalı, sistemler güncellenmeli, eğitimler alınmalı, oluşabilecek yeni riskler karşısında yatırımların zamanında ve doğru bir şekilde yapılması gerekmektedir. Ayrıca tüm bu evrelerde güvenlik seviyesinin istenilen düzeyde sağlanıp sağlanamadığının saptanması, varsa mevcut zafiyetleri açığa çıkarmak, açık kapıları bulmak, uygulanan kurumsal bilgi güvenliği politikalarında yeni açıklar olup olmadığını anlamak amacıyla belirli zaman dilimlerinde sistemlerin gözden geçirilmesi gerekmektedir.

Kurumsal bilgi sistemlerinin güvenliğinin sağlanmasında zafiyetlerin erken tespitinin önemi büyüktür. Saldırı gelmeden önce güvenlik zafiyetlerinin tespit edilerek giderilmesini sağlayan güvenlik testleri kurumsal bilgi güvenliğinin sağlanması açısından büyük önem taşımaktadır. Güvenlik testlerinin sınıflandırılarak kurumların ihtiyaçları doğrultusunda, belirli bir yöntem ve disiplin çerçevesinde etik kurallara saygılı güvenlik uzmanları tarafından yapılması güvenlik testlerinin başarılı olması için önemlidir. Bu testlerin amacı kurumsal bilgi sistemlerine düzenlenebilecek saldırıları, saldırgan gözüyle kontrollü olarak saldırı gelmeden önce kontrollü saldırılar düzenleyerek gerekli tedbirlerin önceden alınmasında kurumlara yardımcı olmaktır. Kurumsal bilgi sistemlerinin güvenliği sadece teknik önlemlerin alınmasıyla sağlanamaz. Teknolojik sebeplerden kaynaklanmayan konularda bilgi sistemlerinin güvenliğini tehdit etmektedir. Güvenlik testleriyle sınanan bilgi sistemleri teknik (bilişim sistemleri, doküman yönetim sistemleri, süreç analizleri, vb.) ve teknik olmayan (çalışanların bilinci, kurum kültürü, yönetimsel prosedürler, fiziksel güvenlik vb.) etkenler dikkate alınarak bir bütün olarak değerlendirilmelidir. Güvenlik testleri değişen risklere paralel olarak periyodik zaman aralıklarında tekrarlanmalıdır.

Tekrarlama zaman dilimi kurumların riskleri dikkate alınarak belirlenmelidir. Kurumsal bilgi güvenliğinin sağlanmasında önemli bir role sahip olan, ülkemizde bu alanda kullanımı çok yaygın olmayan güvenlik testleri konusunda bu çalışmada kapsamlı bir araştırma yapılmıştır. Yapılan incelemelerde öncelikle literatürdeki mevcut tanımlar gözden geçirilmiştir. Daha sonraki bölümlerde güvenlik testlerinin amaçları, sınıflandırılması, kapsamı ve sınırları, standartlar, kullanılan yaklaşımlar, test teknikleri, test aşamaları ve test aşamalarında kullanılan araçlar sırasıyla açıklanmıştır.

2. KURUMSAL BİLGİ GÜVENLİĞİ VE STANDARTLARI

İletişim ortamlarının yaygınlaşması ve kullanımının artması sonucunda elektronik ortamlarda bulunan bilgilerin her geçen gün katlanarak artmasından paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit oluşturması ve en önemlisi kişisel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir.

Kişi ve kurumların bilgi güvenliğini sağlamadaki eksikliklerinin yanında saldırganların saldırı yapabilmeleri için ihtiyaç duydukları yazılımlara internet üzerinden kolaylıkla erişebilmeleri fazla bilgi birikimine ihtiyaç duyulmaması ve en önemlisi ise kişisel ve kurumsal bilgi varlıklarına yapılan saldırılardaki artışlar, gerek kişisel gerekse kurumsal bilgi güvenliğine daha fazla önem verilmesine yeni yaklaşımların ve standartların kurumlar bünyesinde uygulanması zorunluluğunu ortaya çıkarmıştır. Kurumsal bilgi güvenliği, bilginin üretildiği, işlendiği ve saklandığı her ortamda sağlanmak zorundadır. Bunun için mevcut yazılımlar, donanımlar, ortamlar ve insan kaynakları dikkate alınmalıdır. Bilginin korunmasına çalışıldığı ilk günden itibaren güvenlik zincirinin en zayıf halkasını her zaman insanlar oluşturmuşlardır . Birçok teknik veya teknik olmayan güvenlik kontrolleri uygulansa dahi bu kontroller saldırganlar tarafından en zayıf halka olan insan faktörü kullanılarak çeşitli yöntemlerle aşılabilmektedir.

Genel bir söylem olan “gücünüz en zayıf halkanız kadardır” ilkesi bilgi güvenliği içinde geçerlidir. Yapılan çalışmalarda bilgi güvenliği açıkları ve kayıplarının artması sebebiyle bu konunun henüz doğru olarak anlaşılmadığı, gereken önemin verilmediği ve bilinçlenmenin gereken seviyede olmadığını bizlere göstermektedir. 2005 yılında yaygın olarak kullanılan ve 2006 yılının son aylarına damgasını vuran ve günümüzde hala popüler olan sazan avlama (phishing) saldırganlar tarafından kullanılan etkili bir saldırı yöntemidir. Geçmiş yıllarda bilgi sistemlerine en büyük zararları veren virüsler 2006 yılı itibariyle yerlerini casus programların sazan avlama yöntemiyle kullanıldığı saldırılara bırakmıştır.

Dünyada olduğu gibi ülkemizde de sıkça karşılaşılan bu yöntemde genellikle bilgi güvenliği bilinci olmayan kullanıcılar kurban olarak seçilmekte ve internet bankacılığı odaklı soygunlar yapılmaktadır.

Sazan avlama çalışma grubu (Anti-Phishing Working Group) tarafından Temmuz 2006 tarihinde yayınlanan aylık rapora göre 14,191 web sitesi üzerinde kimlik hırsızlığı, soygun ve diğer kötücül amaçlar için kullanılan 23,670 tekil sazan avlama vakası tespit edilmiştir. Netcraft firması tarafından geliştirilen ve web tarayıcılarıyla bütünleşik olarak çalışan güvenlik yazılımı sayesinde sazan avlama saldırıları konusunda yapılan incelemelerde 2005 yılında 41.000 olan saldırı sayısının 2006 yılı sonunda 609.000'e çıktığı gözlemlenmiştir.

Dünyaca ünlü güvenlik firması tarafından verilen bu rakamlar tehlikenin hangi hızla ilerlediğinin gösterilmesi açısından önemlidir. Sazan avlama konusunda Messagelabs firması tarafından yapılan bir başka araştırmada Netcraft firmasının sonuçlarını desteklemektedir. Ocak 2006 tarihi itibariyle %10,6 olan sazan posta oranı Aralık 2006 sonu itibariyle %68,6 gibi yüksek bir rakama çıkmıştır. Bu artışın 2005 yılı genelinde %13,1 olduğu göz önüne alındığında 2006 yılındaki rakamın ne kadar büyük olduğu görülmektedir. Ülkemizde sazan avlama ve benzeri saldırı teknikleriyle ilgili araştırmalar yapılmadığından, bu konuda istatistikler verilememiştir. Ancak bu tür araştırmaların bilgi güvenliğine önem veren gelişmiş ülkelerde yapıldığını (A.B.D. İngiltere, Avustralya, vb.) göz önüne alırsak ülkemizde durumun daha da kötü olduğu ortaya çıkacaktır.

Buradan da anlaşılacağı gibi önümüzdeki yıllarda çok yüksek teknik bilgiler üzerine kurulu saldırılardan ziyade bilgi güvenliği bilincine haiz olmayan kişilerin kandırılması sonucunda ortaya çıkan güvenlik açıklarının saldırganlar tarafından ustaca kullanılacağı tahmin edilmektedir. Gartner ve Deloitte gibi bağımsız araştırma kuruluşlarının raporları incelendiğinde kurum ve kuruluşların güvenlik teknolojilerine yeterli ölçüde yatırım yapmadıkları görülmektedir. Deloitte firmasının 30 ülkede 2006 yılında gerçekleştirdiği araştırmada kurumların %73'nün güvenlik yatırımı yaptığı, yatırım yapan firmaların bilgi işlem müdürlerinin %54'nün ise bu yatırımları yetersiz buldukları belirtilmiştir.

Türkiye'de yapılan araştırmalarda ise 2005 yılı bilişim genel yatırımları 19 milyar dolar iken güvenlik yatırımları 30 milyon dolar, 2006 yılında bilişim yatırımları 23 milyar dolar iken güvenlik yatırımları 40 milyon dolara ulaşmakta ve 2007 yılında ise 47 milyon dolar olması beklenmektedir.

Literatürde yaşanan önemli olaylardan görüleceği üzere kurumsal bilgi güvenliğinin üst seviyede sağlanabilmesi için bilgi güvenliğinin devamlılık gerektiren bir süreç olduğu ve bu sürecin kurumsal bilgi güvenliği standartları çerçevesinde yönetilmesi gerektiği unutulmamalıdır.

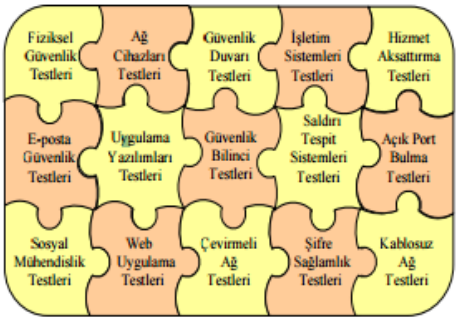
Sazan avlama saldırılarıyla kullanıcıların kandırılmasını önlemenin yegâne yolunun kurumsal bilgi güvenliği yönetim sistemleri çatısı altında yapılacak olan eğitim ve bilinçlendirme çalışmalarının olduğu unutulmamalıdır.

Bu çalışmanın amacı; kurumsal bilgi güvenliğini genel olarak incelemek, mevcut çalışmaları özetlemek, kurumsal bilgi güvenliğinin kurumlarda etkin bir şekilde hayata geçirilmesinin önemini vurgulamak, kurumsal bilgi güvenliğinin etkin bir şekilde hayata geçirilmesinde önemli bir yer tutan ISO tarafından yeni yayınlanan ve hali hazırda geliştirilmekte olan ISO/IEC 27000 serisi standartlarını kısaca sunmak, ülkemizde konuya daha çok önem verilmesini sağlamak ve kurumsal bilgi güvenliğinin önemini güncel açıdan değerlendirmek, kurumsal bilgi güvenliğinin üst seviyede sağlanmasına yönelik güncel tehditler ve eğilimleri incelemek, konunun önemini bir kez daha vurgulamak ve konuya tekrar dikkat çekmek, ülkemizde bu alanda yayınlanmış kapsamlı bir makale olmamasından dolayı bu konudaki bilgi açığını kapatmak, konuya geniş bir açıdan bakarak bu konudaki farkındalığını daha da artırmak, yüksek seviyede kurumsal bilgi güvenliğini tehdit eden önemli açıkları tespit etmek ve giderilmesine yönelik öneriler sunmak olarak sıralanabilir.

2.1. Kurumsal Bilgi Güvenlik Testleri

Güvenlik testleri bilgisayar sistemlerinin güvenliğini değerlendirmede kullanılan en eski yöntemlerden birisidir. 1970'lerin başında A.B.D Savunma Bakanlığı, daha güvenli sistemler oluşturmak için yazılımların geliştirilmesindeki ve bilgisayar sistemlerindeki güvenlik zafiyetlerinin gösterilmesinde bu yöntemi kullanmıştır. “Bilişim sistemlerinde sızma testi” kavramı 1995 yılında geliştirilen ve ilk Unix tabanlı ilk zafiyet tarama sistemi olan “SATAN” programıyla birlikte kullanılmıştır.

Genel bir fikir vermesi amacıyla güvenlik testleri (Şekil 2.1.1.)'de verilmiştir.



Şekil 2.1.1. Güvenlik Testlerinin Yap-Boz Gösterimi

Güvenlik testlerinin şematik gösterimi bir yapboz şeklinde tarafımızdan bu çalışma kapsamında ifade edilmiştir. Bu gösterimin amacı güvenlik testlerine bir bütün olarak bakılması, içlerinden herhangi birinin yapılmaması veya düzgün olarak yapılmaması durumunda kurumsal bilgi güvenliğini zafiyete uğratacağından bu testlerin tamamlayıcı olduğunu vurgulamaktadır. Bu yüzden şekilsel olarak dikkat çekici olması için bu çalışma kapsamında yapboz gösterim tercih edilmiştir. Literatürde güvenlik testleriyle ilgili yapılan tanımlardan önemlileri aşağıda özetlenmiştir.

• Bilgisayar ağı ve ağ kaynaklarındaki zafiyetlerin tespit edilerek bilgi sistemlerinin güvenlik seviyesini değerlendirmek üzere hazırlanan testlerdir. Çoğu zaman etik amaçlı saldırılar (Ethical Hacking) olarak da adlandırılır.

• Açık kapı bulma sanatıdır.

• Bilgisayar ağlarının güvenliğini artırmak, yeni zafiyet ve sömürüleri ortaya çıkarmak, bilgi sistemlerinin ne derece güvende olduğunu anlamak üzere yapılan testlerdir.

Kurum veya kuruluşların güvenliğini sağlamak amacıyla gerçek dünyadaki saldırı ve saldırgan mantığıyla bilgi sistemlerinin ne derece güvende olduğunu anlamak üzere bilgisayar ağlarına yetkisiz erişim sağlamak için yapılan testlerdir.

• Yetkili kişiler tarafından bilinen zafiyetlerin sistematik ve planlı olarak kullanılmasıyla bilgi kaynaklarına (uygulamalar, bilgisayarlar, bilgisayar ağları ve bileşenleri) yapılan kontrollü saldırılardır.

• Bilgi güvenliği ölçümlerinin yapılmasını sağlayan bir yöntemdir.

• Saldırganların yapabileceğine benzeyen kötücül saldırılar yapılarak bilgisayar sistemlerinin ve ağlarının güvenliğinin değerlendirilmesi yöntemidir.

• Güvenlik danışmanları (Ethical Hacker) tarafından sistem veya ağ üzerinde saldırganların hangi tür açıkları tespit edebileceği ve açıklara dayalı bilgilerle neler yapabileceklerinin görülmesi amacıyla yapılan güvenlik testleridir

• Bilgisayar ağları üzerinde saldırganların beceri ve teknikleri kullanılarak, var olan zafiyetlerin uzak konumlardan bulunması amacıyla ağların taranması, tarama sonuçlarının incelenmesi, var olan zafiyetlerin kötüye kullanılması ve son olarak zafiyetin giderilmesi amacıyla yapılan güvenlik testleridir.

• Bilgi varlıklarının (uygulamalar, bilgisayar ağları, bilgisayar sistemleri) güvenlik durumunu değerlendirmek için zafiyet, yapılandırma hataları, zayıflıklar yönünden saldırgan teknikleri ile analiz edilmesi sürecidir.

• Kurumlar tarafından saldırılar ve yetkisiz erişimlerden bilgisayar sistemlerinin nasıl korunacağıyla ilgili zafiyetlerin değerlendirilmesinde kullanılan ortak bir yoldur.

• Koruma sistemlerinin sahip olduğu zafiyetlerin gösterilmesi amacıyla yapılan sızmalardır.

• Teknik donanımlı ehil kişiler tarafından yapılan sistematik testlerdir.

• Sızma testlerinin amacı güvenliğin test edilmesi olup, kurumsal bilgi sistemlerinin kırılması olarak algılanmamalıdır.

• Güvenli Hesaplama Esaslarının (TCB) güvenlik seviyesinin değerlendirmede kullanılan yöntemlerden bir tanesidir. Yukarıda yapılan tanımlar dikkate alındığında, bu çalışma kapsamında kişisel tanımımızı şu şekilde yapabiliriz. Kurumsal bilgi varlıklarının (bilişim sistemleri, insan faktörü, iş süreçleri) zafiyetlerinin saldırgan gözüyle ortaya

çıkarılarak giderilmesi amacıyla belirli zamanlarda, yazılımlar, donanımlar ve insanlar üzerinde işinin ehli bir ekip tarafından yapılan etik testlerdir.

2.2. Kurumsal Bilgi Güvenlik Testlerinin Amaçları

1974 yılında Paul A. Karger ve Roger R. Schell tarafından yazılan "zafiyet analizi", 1975 yılında Richard R. Linde tarafından uluslararası bir konferansta sunulan "işletim sistemleri ve sızma testleri" isimli bildiriler literatürdeki bu konuyla yapılmış ilk çalışmalardır. O günden bu güne, kurumsal bilgi güvenliğinde güvenlik testlerinin kullanımı ve önemi gün geçtikçe artmaktadır.

Yapılan bu testlerin ortak amacı, kurumsal bilgi varlıklarına ait güvenlik tehditlerinin (zayıflıklar, zafiyetler, yapılandırma hataları, vb.) kötü niyetli saldırganlardan önce belirlenerek gerekli güvenlik önlemlerinin kurumlar tarafından alınmasına yardımcı olmaktır. Güvenlik testlerinin amacı kötü niyetli kişilerin yetkisiz erişimlerini engellemek amacıyla zafiyetlerin tanımlanarak giderilmesidir. Güvenlik testleri kurumlar tarafından çok çeşitli amaçlar için pek çok alanda kullanılmaktadır. Bu testler;

- Yeni zafiyetlerin bulunması,
- Tasarım zafiyetlerinin belirlenmesi,
- Güvenilir kurum imajının korunulması,
- Bilgi güvenlik politikalarının gözden geçirilmesi,
- Bilgi güvenliği sertifikasyonlarına uyumda sürekliliğin sağlanması,
- Etkili ve bilinçli güvenlik yatırımının yapılması,
- Güvenlik yatırımlarının geri dönüşümünün mümkün olduğunca yüksek olması,
- Teknik personelin sorumluluğunun gözden geçirilmesi,

• Kurumsal bilgi sistemlerine yapılabilecek olan muhtemel saldırı veya saldırılara karşı güvenliğimizi sürekli olarak yüksek seviyede sağlamak amaçlı yapılmaktadır. Yukarıda maddeler halinde açıklanan güvenlik testlerinin amaçları takibeden alt başlıklarda sırasıyla açıklanmıştır.

2.2.1. Yeni zafiyetlerin bulunması

"Güvenlik satın alınacak bir ürün değil devamlılık gerektiren bir süreçtir" yaklaşımı güvenlik dünyasında kabul görmüş bir yaklaşımdır. Bu yaklaşım güvenliğin sadece bir defaya mahsus olarak başlangıçtaki zafiyetler dikkate alınarak sağlanmasının yeterli olmayacağı, bu sürecin dinamik olduğunu ve güvenliğin sürekliliğinin sağlanmasının önemini vurgulamaktadır.

Kurumsal ihtiyaçların her geçen gün artması ve değişmesine bağlı olarak yeni teknolojiler ve yeni yaklaşımların kullanılmasıyla birlikte sistemler ilk kurulduğu andaki zafiyetlerden çok daha fazlasını içermektedir.

Güvenliğin yüksek seviyede sağlanabilmesi için bilgi güvenliği yaşam döngüsünde kullanılan yeni teknolojilerin veya yeni saldırı yöntemlerinin beraberinde getirdiği yeni zafiyetlerin güvenlik testleriyle bulunması ve önlemlerin önceden alınması gerekmektedir. Bilgi yaşam döngüsü boyunca meydana gelebilecek yeni zafiyetlerin (kurtçuklar, işletim sistemi açıkları, virüsler, protokol açıklıkları, personel, vb.) tespit edilememesine bağlı olarak güvenlik ihlalleri yaşanacak ve kurumlar zarar görecektir.

2.2.2. Tasarım zafiyetlerinin tanımlanması

Bilgi sistemlerinde kullanılacak yazılımların tasarımlarının veya bilgi sistemlerinin yerleşeceği fiziksel mekanların tasarımları yapılırken tasarımcılar çoğunlukla güvenlik gereksinimlerini atlamakta veya gereken önemi vermemektedirler. Yazılımların tasarlanması aşamasında tasarımcı programa dış dünyadan yapılacak erişimleri en aza indirgemeli ve dış dünya ile temasta olan kısımların güvenliğinin yüksek seviyede sağlanmasına yönelik bir tasarım ortaya koymaya özen göstermelidir. Bunu takiben dış

dünyadan yapılacak olan veri girişlerinin kodlayıcılar tarafından yeterince doğrulanmaması sonucunda zafiyetler oluşacaktır.

İlk bakışta fark edilmesi zor olan tasarım kaynaklı kusurları içeren zafiyetler ancak güvenlik testleriyle ortaya çıkarılabilecektir. Tasarım zafiyetlerinden dolayı başlangıçta güvenli olduğu varsayılan bilgi sistemleri çeşitli saldırılara maruz kalabilmekte ve büyük kayıplar yaşanabilmektedir.

Tasarım zayıflıklarından kaynaklanan zafiyetlere bir başka örnek ise fiziksel ağ tasarımları yapılırken ağ bileşenlerinin (router, switch, hub, kablo, panel, fiber optik kablo sonlandırıcıları) fiziksel güvenliğin (kilitsiz dolaplar, kilitsiz odalar, vb.) yeterince ciddiye alınmamasıdır. Bu tasarım zayıflığına bağlı olarak yetkisiz kişiler ağ aktif cihazları üzerinden bilgilere yetkisiz olarak erişebilecek ve bilgi güvenliği ihlallerinin yaşanmasına sebebiyet verecektir.

Bu tasarım zayıflığından kaynaklanan zafiyetlerin kullanılması durumunda ağ yönlendiricisinin saldırıya uğraması (hack edilmesi), verilerin dinlenmesi, hizmetin durması gibi ciddi saldırılar meydana gelebilecektir. Mantıksal ve fiziksel tasarımlardan kaynaklanan zafiyetlerinin güvenlik ihlallerine dönüşmeden önce güvenlik testleriyle tespit edilerek önlemlerin alınması kurumsal bilgi güvenliğinin yüksek seviyede sağlanması açısından önemlidir.

2.2.1. Güven sağlanması

Güvenilir kurum imajı, elektronik ortamlarda iş yapan kurum ve kuruluşların en büyük sermayelerinden birisidir. Müşteri sayısının artması ve mevcut müşterilerin korunması ancak ve ancak “güven” veya “güvenirlik” duygusunun sürekliliğidir. Elektronik ortamlarda kurumların bu imajını sağlamlaştırmaları için saldırıya uğramadan veya zafiyetlerle karşılaşılmadan önce önlemler alarak, maddi ve manevi kayıpları engelleyebilirler. Bunun için ise güvenlik testleri önemli bir yer tutmaktadır.

2.2.2. Bilgi güvenlik politikalarının oluşturulması

Bilgi güvenlik politikalarının oluşturulmasında, kurumsal bilgi sistemlerinin güvenliğini tehlikeye atan tehditler güvenlik testleriyle tespit edildikten sonra risk değerlendirmeleri ve risk analizleri yapılır. Risk analiz sonuçları kurumsal bilgi güvenliği politikaları içerisinde yer alan prosedürler ve standartların oluşturulması için yapılan çalışmalara teknik bir dayanak oluşturur.

2.2.3. Sertifikasyonlar

Güvenlik testleri kurumsal bilgi güvenliği sertifikasyonlarının alınması için çoğunlukla yapılması zorunludur.

Kurumsal bilgi güvenliği yönetim sistemlerinin oluşturulması ve işletilmesi adımlarında kurumsal bilgi varlıklarına ait güvenlik risklerinin tespiti ve analizi çalışmalarına yardımcı olması amacıyla güvenlik testlerinin uygulanması ve sonuçlarının değerlendirilmesi standartlar tarafından zorunlu tutulmuştur.

2.2.4. Güvenlik yatırımları

Güvenlik yatırımlarının doğru ve zamanında yapılması ile ilgili olarak birçok kurum ve kuruluş problem yaşamaktadır. Özellikle ticari kaygısı olan firmaların yanlış yönlendirmeleriyle yetersiz veya gereğinden çok fazla ürünler satın alınmakta dolayısıyla doğru yatırımlar yapılamamaktadır. Buna ek olarak güvenliğin sadece bazı yatırımlar yapılarak sağlanabileceği düşüncesini taşıyan yöneticilerin ikna edilebilmesi de yatırımlar konusunda yaşanan bir diğer zorluktur. Örneğin bir güvenlik duvarı ve antivirüs yazılımlarının satın alınmasıyla güvenliğin tamamen sağlanacağını düşünen birçok yönetici hatta teknik personel olduğu bilinmektedir. Ancak gerçekte bilgi güvenliğinin sağlanabilmesi için bu çözümlere ek olarak, ağ ve host tabanlı IDS/IPS (Intrusion Detection / Prevention Systems) kişisel bilgilerin gizliliğinin sağlanması için gerekli olan koruma sistemleri, e-posta temelli antivirüs yazılımları, içerik filtreleme, spam posta filtreleme, casus yazılım engelleme ve eğitim gibi yatırımların da yapılması gerekmektedir.

Güvenlik yatırımlarının doğru yapılmaması, yapılsa bile yanlış yapılandırılmasından kaynaklanan zafiyetler güvenlik testleriyle tespit edilebilir. Güvenlik testlerinin sonucunda ortaya çıkan bilgiler gerekli güvenlik yatırımlarının doğru, etkili ve ölçülü bir şekilde yapılması konusunda yöneticilere ve teknik sorumlulara yardımcı olacaktır. Ayrıca güvenlik yatırımlarının doğru yapılmasının bir diğer sonucu ise yatırımın geri dönüşümüdür.

Güvenlik testleri sayesinde doğru güvenlik yatırımları yapılması kurumların maddi ve manevi anlamda kâr etmelerini, saygınlığının, itibarının ve güvenilirliğinin artmasını sağlayacaktır.

2.2.5. İnsan faktörü

Bilgi güvenliğini en üst düzeyde tehdit eden ve güvenlik kontrollerinin aşılmasını sağlayan önemli risklerin başında insan faktörü gelmektedir. Örneğin teknik personelin verimliliğinin ve yaptığı işin kalitesinin ölçümlenmesi güvenliğin sağlanması için önemlidir. Çalışanlar bilgi eksiklikleri ve çalışma motivasyonlarının düşük olmasından kaynaklanan, bilerek veya bilmeden önemli hatalar yapmaktadırlar. Düzenli olarak yedek alınmaması veya alınan yedeklerin test ortamlarında sınanmamış olması, bilgi sistemlerinin üretim esnasında verilen varsayılan (default) şifre ve yapılandırmalarla kullanıma alınması, yayınlandığı halde yazılımlara ait güncelleme ve yamaların yapılmaması, güvenlik yazılımlarındaki kural hataları, gereksiz servislerin kapatılmaması, imza tabanlı güvenlik yazılımlarının veritabanlarının güncel tutulmaması gibi kusurlar insan faktöründen kaynaklanan hatalara örnek olarak gösterilebilir. Güvenlik testleriyle insan faktöründen kaynaklanan hatalar zamanında tespit edilerek gerekli önlemlerin alınması sağlanabilir.

3. İSPARK'IN KURUMSAL BİLGİ GÜVENLİĞİ VE NFC ALTYAPISI

İSPARK için kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Her birey otoparkları kullanırken bilgi sistemleri üzerinden hizmet almakta ve kurumsal bilgi varlıklarını doğrudan veya dolaylı olarak kullanmaktadır. Bu hizmetler kurumsal anlamda İSPARK için bir parklanma hizmet sunumu olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemler de olabilir. İSPARK'ın kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, müşterilerin kişisel güvenlikleride sağlanamaz.

Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanabilir.

Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir.

İSPARK'ın kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır.

Bu gibi firmalarda süreçlerin yönetilmesi, güvenlik sistemlerinin uluslararası standartlarda yapılandırılması ve yüksek seviyede bilgi güvenliğinin sağlanması amacıyla tüm dünyada olduğu gibi Türkiye'de de kurumsal bilgi güvenliğinin yönetiminde standartlaşma çalışmaları hızla sürmektedir. Standartlaşma konusuna önderlik eden İngiltere tarafından geliştirilen BS–7799 standardı, ISO tarafından kabul görerek önce ISO–17799 sonrasında ise ISO–27001:2005 adıyla dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir. Ülkemizde Avrupa Birliği Uyum Kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalışmalar yetersiz olup bu standardı uygulayan kurum ve kuruluşların sayısı yok denecek kadar azdır.

ISO–27001:2005 standardı ülkemizde Türk Standartları Enstitüsü (TSE) tarafından TS ISO/IEC 27001 "Bilgi Güvenliği Yönetim Sistemi" standardı adı altında yayınlanmış ve belgeleme çalışmaları başlatılmıştır. Bu standart kapsamında kurumsal bilgi varlıklarının güvenliğinin istenilen düzeyde sağlanabilmesi amacıyla; gizlilik, bütünlük ve erişilebilirlik gibi güvenlik unsurlarının kurumlar tarafından sağlanması gerekmektedir.

İSPARK'ın Bilgi Güvenliği Yönetim Sistemleri (BGYS); insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. İSPARK açısından önemli bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması, BGYS'nin tüm otoparklarda hayata geçirilmesiyle mümkün olmaktadır.

BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir.

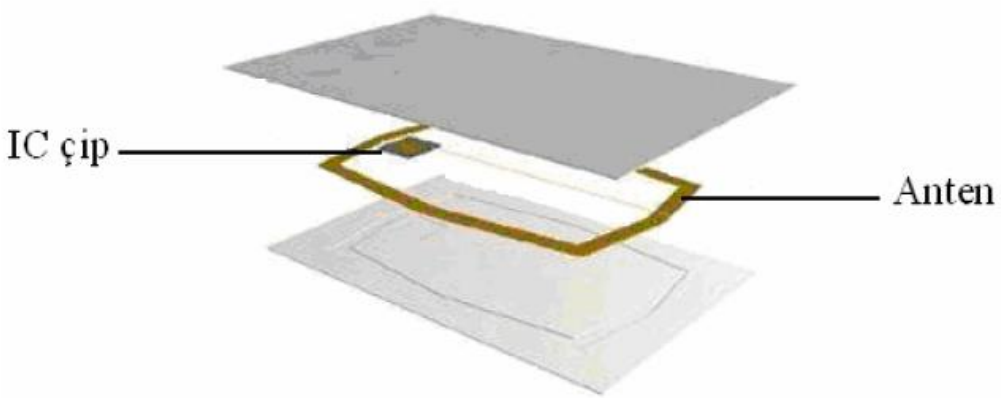
Kurumsal bilgi güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, risk yönetimi, denetim kontrollerinin seçilmesi, uygulanabilirlik beyannameleri BGYS kurulabilmesi için, yapılması gereken adımlardır. İSPARK tüm bu adımları ISO–27001 standartların uygun şekilde gerçekleştirmiştir.

3.1. Temassız Akıllı Kartlar

Temassız kartlar, okuyucuya yaklaştırıldığında okuyucu ile iletişime geçip çalışabilirler. Hem kart okuyucu hem de akıllı kart, birer antene sahiptirler. Bu sayede iki taraflı bir iletişim kurulur. Aşağıdaki şekilde de görüldüğü gibi, anten ve çipi barındıran ortadaki kısım, kartın üst ve alt katmanlarının arasında yer alır. Anten, kartın etrafını 4-5 tur dönen ince bir telden ibarettir.

Temassız akıllı kartların bir işlem gerçekleştirebilmeleri için bir anten yanından geçirilmeleri gerekir. 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 kart (Şekil 3.1.1.)'de gösterilmiştir.



Şekil 3.1.1. Temassız Akıllı Kart

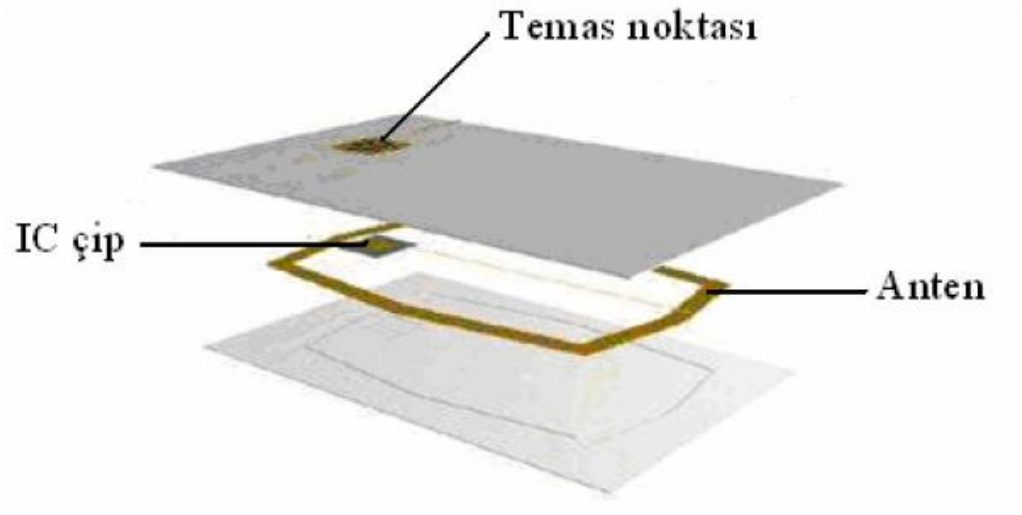
3.1.1. Temassız kartların diğer kartlara göre avantajları

- Akıllı kart geçiş sistemlerinde anahtar vazifesi görür.
- Çip kart içinde gömülü olduğundan sudan güneşten etkilenmez.
- Diğer kartlardan etkilenmez, diğer kartları etkilemez.
- Manyetik ortamdan etkilenmez kolay deforme olmaz.
- Kartın kopyalanması neredeyse imkânsızdır.
- Kartın okuyucuya fiziksel teması yoktur.
- Personel geçişleri daha seri ve sorunsuz olmaktadır.
- Kartın kapalı bir kılıf içinden okutulması mümkündür.

3.2. Kombi Kartlar

Temaslı ve temassız akıllı kartların avantajları ve dezavantajları vardır. Temaslı kartlar daha güvenlidir ve mevcut bir alt yapıları vardır. Temassız kartlar ise daha elverişli ve verimli bir işlem ortamı sunar.

Bu iki kartın da avantajlarından yararlanmak için her iki özelliğe sahip kombi kartlar geliştirilmiştir. (Şekil 3.2.1)'de Kombi kart gösterilmiştir.



Şekil 3.2.1. Kombi Kart

Akıllı kartlar standartları aşağıdaki gibidir.

• ISO 7810 Fiziksel Karakteristikleri

• ISO 7811 Manyetik Şerit, Kabartma Kayıt Tekniği

• ISO 7813 Finansal İşlem Kartları

• ISO 7816 Kontaklı Tümleşik Devre Kartları

• ISO 10373 Test Metodları

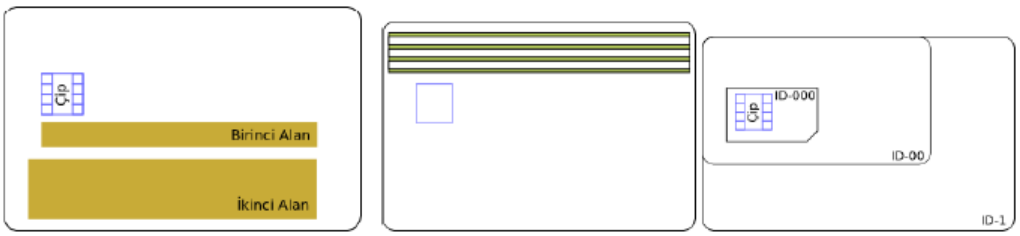
• ISO 10536 Kontaksız Tümleşik Devre Kartları

• ISO 11693 Optik Bellekli Kartlar-Genel Karakteristikleri

• ISO 11694 Optik Bellekli Kartlar- Doğrusal Kayıt Metodu Bellek alanları ise büyük miktarda veri saklamak için kullanılır ve büyüklüğü 1K ile 64K arasında değişir.

3.3. Fiziksel Yapı

Bağlantı biçimi, içindeki birimler, çalışma şekli, boyutu gibi bir çok parametreye göre akıllı kartları sınıflandırmak mümkün. Temelde hepsi ISO 'nun bu konuda getirdiği biçimsel ve iletişimsel standartları desteklemektedir, böylece farklı kartlar ve okuyucular bir arada kullanılabilmektedir. Temel kart biçimi ve boyutu ISO 7810 standardında tanımlanan ID-1 dir. Bu manyetik ve çipli tüm kredi kartlarının uyduğu ortak boyut olup, aşağıdaki özellikleri taşımaktadır. Şekil (3.3.1.)'de Akıllı Kart Fiziksel Yapısı gösterilmiştir.



Şekil 3.3.1. Akıllı Kart Fiziksel Yapısı

Kartın ön yüzündeki birinci alan kabartma olarak kart numarası için ayrılmıştır. İkinci alan ise gene kabartma olarak kart sahibine ilişkin isim ve adres gibi bilgiler içindir. Arka yüzdeki manyetik şerit, üç ayrı iz halinde ayrılmıştır. İlk iki iz okunabilir, üçüncü iz ise hem okunabilir hem yazılabilir bilgi taşır. Manyetik şeritin kapasitesi 1000 bit civarında olmakla birlikte, kabartmalardaki bilgileri taşımak için fazlasıyla yeterlidir. Kart üzerindeki çip gene sabit bir konumda bulunmakta ve belirli noktalardaki temas yüzeyleri aracılığıyla iletişim kurmaktadır. Bu kart boyutunun cep telefonları için büyük kalması nedeniyle GSM kartları için ID-000 adlı daha ufak bir biçim de standartlaştırılmıştır. Kartın sık değişmediği ortamlar için tasarlanan bu boyut dışında bir de iki boyut arasında

ID-00 mini-card standardı vardır. ID-1 boyutundaki temaslı çip kartları kesilerek mini boyuttaki kartlar elde edilebilir.

3.4. NFC

MasterKart, ISIS (Ortaklık,Verizon, Barclaykart ve Discover), ve Google gibi dünya devleri mobil cüzdan duyurularını yaptılar. 2000 yılından bu yana ödeme dünyasındaki en önemli rollere sahip olan mobil operatörler, finansal hizmet sağlayan firmalar ve satıcılar mobil ödemenin uygulanabilirliğini değerlendirmektedir ve bu rollera sahip oyuncuların son gelişmelerde mobil ödemeye teşvik oluşturduğu ortadadır.

Yeni geliştirilen NFC teknolojisi, yakın alan haberleşmesi demektir ve mobil cihazlarda temassız haberleşmeyi mümkün hale getirmektedir.

Temassız haberleşme teknolojilerin başında RFID, NFC yer almaktadır. NFC teknolojisinin mobil cihazlarda temassız ödeme sağlaması ile mobil ödeme uygulama çeşitliliği, kuponlar, biletler ve promosyonlar gibi sektörlerde sıçrama yaşandı. NFC tabanlı mobil ödemelerde giderek artış yaşanmaktadır. Şekil (3.4.1.)' de iki telefon arasında NFC ile veri aktarımı gösterilmiştir.

Şekil 3.4.1. İki Telefon Arasında NFC İle Veri Aktarımı

NFC teknolojisinin otopark sektöründe mobil bilet, akıllı posterler, temassız okuyucu gibi birçok alanda kullanılması ile toplu taşıma operatörlerine ve kullanıcılarına birçok faydasının olacağı beklenmektedir.

Temassız ödeme sistemlerinde müşteri ile POS cihazı arasında fiziksel temas gerektirmeden ödeme işlemi gerçekleşir.

Temassız ödeme işleminde müşteri POS terminaline temassız ödeme kartını, cep telefonunu veya temassız ödeme yapacağı cihazını yaklaştırır ve Radio Frekans (RF) dalgaları ile ödeme bilgileri iletilir. Şekil (3.4.2.)' de temassız POS ödemesi gösterilmiştir.

Şekil 3.4.2 Temassız Pos Ödemesi

Temassız ödeme sistemleri dünyada artık birçok ödeme alanında yer almaktadır ve NFC teknolojisi ile mobil ödemenin hızlı bir giriş yapması ve temassız ödeme trendini artırması beklenmektedir.

Tüketicinin mobil ödeme uygulamasından hesaplarını kontrol edebiliyor olması ve ürün pazarlamaya yönelik NFC teknolojisinin sunduğu teşvikler mobil ödemeye yönelmeyi hızlandırmaktadır.

Radyo frekansı tanımlama (RFID) tabanlı temassız cihazlar kullanarak ve yakın alan iletişimi (NFC) konsepti ile birlikte müşterilere güvenli bir şekilde ödeme yapmaları sağlanmaktadır.

NFC'li toplu ulaşım bileti ve diğer ödeme sistemlerinde NFC'nin hızla tercih edilmesi ile temassız ödeme sistemleri giderek büyümektedir.

2008 yılı başında, MasterKart PayPass, Visa payWave veya American Express ExpressPay markalı 35 milyondan fazla temassız finansal ödeme kartları yayınlanmıştır ve 80.000 şirket 400.000 'den fazla okuyucunun temassız ödeme sistemlerine ve NFC haberleşmeye uyumlu şekilde çalıştığı görülmüştür. Temassız ödeme sistemleri ile NFC özellikli cihazlara geçiş kolaylaşmıştır [2].

Elektronik ödeme sistemlerinin en çok kullanıldığı alanlardan birisi olan otoparklarda mobil bilet uygulamaları gelecekte yaygın bir şekilde kullanılacaktır. Mevcut temassız ödeme sağlayan RFID özellikli sisteme NFC özellikli okuyucuların entegre edilmesi ve NFC özellikli cep telefonlarının mobil bilet olarak kullanılması mümkün olacaktır. NFC'li okuyucu ile NFC özellikli cep telefonu arasında iki yönlü iletişim ile haberleşme gerçekleştirilir. Ayrıca NFC özellikli cep telefonunun okuyucu olarak kullanılması ile akıllı bilete kontör yükleme bakiye bilgilerini görüntüleme uygulamaları geliştirilebilmektedir. Şekil (3.4.3.)' de Visa ve Master kart uyumlu NFC okuyucu ve cep telefonu uygulaması gösterilmiştir.

Şekil 3.4.3 Visa ve Master Kart uyumlu NFC Okuyucu

Bu yükleme uygulamaları ile kullanıcılar sahip oldukları akıllı kartlara kontör yükleme işlemi için bir satış gişesine gitmeye gerek duymadan kendi cep telefonlarını bir pos cihazı gibi kullanabilmektedir.

Ayrıca Akıllı posterlerdeki NFC etiketleri okuyabilen NFC cep telefonu uygulamaları ile posterdeki bilgiyi kendi telefonuna indirebilmekte ve böylece dijital bilgiye hızlı bir şekilde ulaşmaktadır. Şekil (3.4.4.)' de NFC Cüzdan uygulaması gösterilmiştir.

Şekil 3.4.4. NFC Cüzdan

NFC hakkında uluslararası yapılan çalışmalar ve mobil ödeme yönetimi konusunda geliştirilen uygulamalar incelendiğinde inovatif uygulamalar ile NFC'nin yeni kullanım alanları her geçen gün artmaktadır. Mobil ödeme ve NFC alanında interaktif yeni uygulamalar ile farklı sektörlerin NFC teknolojisinin kullanımına ilgisi olduğu gözlemlenmiştir. NFC birçok görüşe göre, cep telefonlarının verdiği hizmetler olan konuşma ve kamera'dan sonra dokunma yoluyla bilgiye erişmede bir devrim olarak görülmektedir.

NFC hız, güvenlik ve kolaylık sunan yeni bir teknolojidir. Yaklaşık 10 yıllık bir geçmişi olmasına rağmen kısmen yeni bir teknolojidir. Uzak doğu ülkeleri bu teknolojiyi daha aktif kullanırken, Avrupa bu konuda biraz geride kalmıştır.

Ülkemizde de bu teknolojiyi GSM şirketleri ve bankalar aktif kullanmakta ve değişik projeler üzerinde çalışmalar yapılmaktadır.

Mobil ödeme, e-bilet ve e-cüzdan gibi alanlarda uygulamalar geliştirilmektedir. Geliştirilen projelerin arka bağlantısında ya bir banka ya da bir GSM şirketi bulunmakta iken Avrupa'da ilk kez geliştirilen MicroSD kart tabanlı NFC uygulaması ile bu kısıtlamanın da ortadan kalkacağa benziyor.

NFC teknolojisinin güvenirliğini, kullanım kolaylığını ve popülerliğini teşvik etmek için 2004 yılında NFC Forum sitesi kurulmuştur. Böylece standartları oluşturma belli bir çatı altında toplanmıştır. NFC ile ilgili tüm organizasyonlar bu site üzerinden yapılmakta ve geniş bir katılım sağlanmaktadır.

2006 yılında ise NFC etiketlerinin standartları belirlenmiş ve akıllı posterler geliştirilmeye başlanmıştır. NFC'nin kullanım alanlarının çok geniş olmasından dolayı şimdiden çok kullanılacak ve rağbet görecek bir teknolojisi olacağı düşünülmekte ve bu alandaki yatırımlar artmaktadır.

"NFC World Asia 2010" konferansında yapılan "The Foundation for Progress with NFC" sunumuna göre Türkiye, NFC projesinin başarılı olduğu ve büyüdüğü 100 ülke arasında ilk 15 ülke arasında yer almaktadır.

Aynı zamanda 2015 yılında İstanbul'daki 6 üniversitede öğrenci kartı ve İstanbul kartlar birbirine entegre edildi. Kartların ön yüzü üniversite kimlik kartının görseli, arkası ise standart İstanbul kart görseli ile kaplandı. Böylece bu üniversitelerde öğrenciler iki ayrı kart taşımak yerine tek kart taşıması hedeflendi. Şekil (3.4.5.)' de NFC özellikli İstanbul-Öğrenci Kart gösterilmiştir.

Şekil 3.4.5. NFC Özellikli İstanbul-Öğrenci Kart

3.4.1. NFC önemi

Yaşadığımız bu zamanda insanların bir çoğu mobil bir cihaza sahip. Bu cihazlarla ilk çıktığı zamanlarda sadece ses ve kısa mesaj iletimi yapılırken günümüzde multimedya servisleri, TV, internet ve hayatı kolaylaştıracak birçok uygulamalar ve donanıma sahip cihazlar geliştirilmektedir. Bunların yanı sıra SIM kart üreticileri, NFC ödeme uygulamasını güvenli olarak hafızasında tutabilen SIM kartları üreterek MNO'lar aracılığıyla kullanıcılara ulaştırmaktadır [3].

Son zamanlarda özellikle ulaşım alanında akıllı kartların kullanımının artması ile bu alandaki çalışmalara ağırlık verilmiştir. İlk zamanlar basit hafıza kartları kullanılmıştır. Sonrasında akıllı temaslı ve temassız kartların kullanımı ile bu alandaki gelişmeler hız kazanmıştır. Şekil (3.4.1.1.)' de NFC kullanım alanları gösterilmiştir.

Şekil 3.4.1.1. NFC Kullanım Alanları [8]

Bu gelişmeler olumlu yönde olurken, en büyük problem kullanıcıların her bir servis için farklı farklı kartları kullanması gerekiyordu.

Ulaşım, kütüphane, sinema, alış-veriş ve akıllı elektronik sistemler için ayrı kartları üzerlerinde taşımaları gerekiyordu. 90'lı yıllarda elektronik cüzdan ve çoklu uygulamalı akıllı kart alanındaki çalışmalar bu sınırlılığında ortadan kaldırılabileceğini 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. Şekil (3.4.1.2.) de NFC özellikli akıllı telefon gösterilmiştir.

Şekil 3.4.1.2. NFC Özellikli Akıllı Telefon

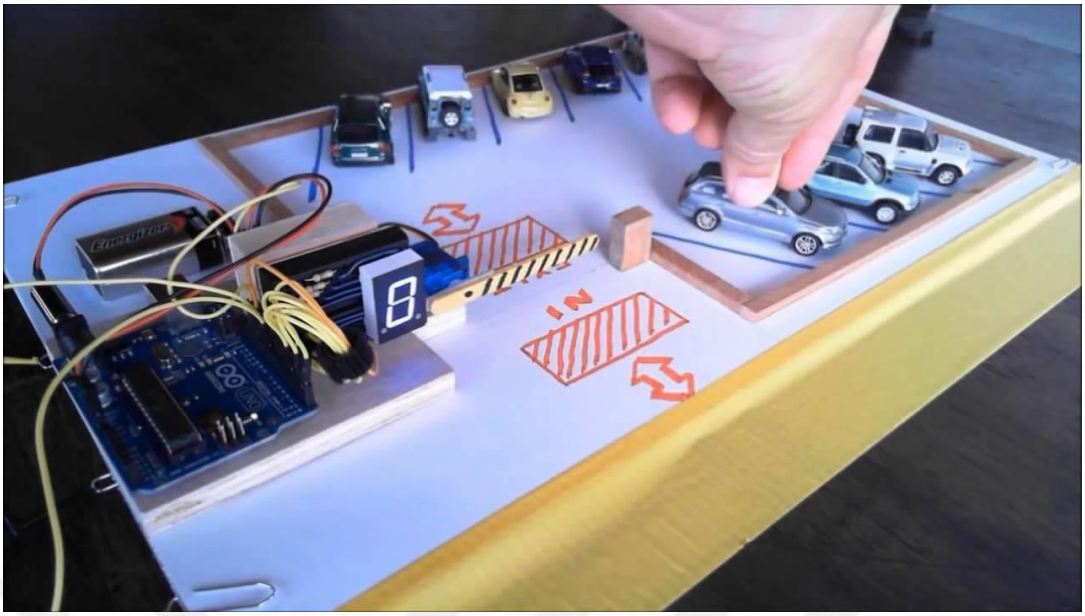
3.4.2. NFC teknolojisi ve akıllı kart sistemleri

NFC teknolojisinin otoparklarda ödeme aracı olarak kullanılabilmesi için teknik ve iş modelinde yaşanan sıkıntılardan dolayı NFC teknolojisinin otoparklarda ödeme aracı olarak kullanılabilmesi ve NFC'li inovatif projelerin hayata geçmesi gecikmiştir.

Bu çalışmada NFC uygulamalarının parklanma sektöründe kullanılabilmesi için akıllı şehir uygulamalarına farklı bir bakış sunulmaktadır.

NFC teknolojisinin daha iyi anlaşılması ve parklanmada kullanımının yaygınlaştırılması için en ideal iş modelinin kurulması amaçlanmıştır.

Çalışmanın amacı otopark kullanan insanların hayatını kolaylaştıracak, geliştirilmiş NFC'li ödeme Uygulaması ile kolay geçiş imkânı sunan kullanıcı ile interaktif bir yapı hazırlamaktır. Şekil (3.4.2.1.)' de NFC kart ödeme özellikli otopark prototipi gösterilmiştir.



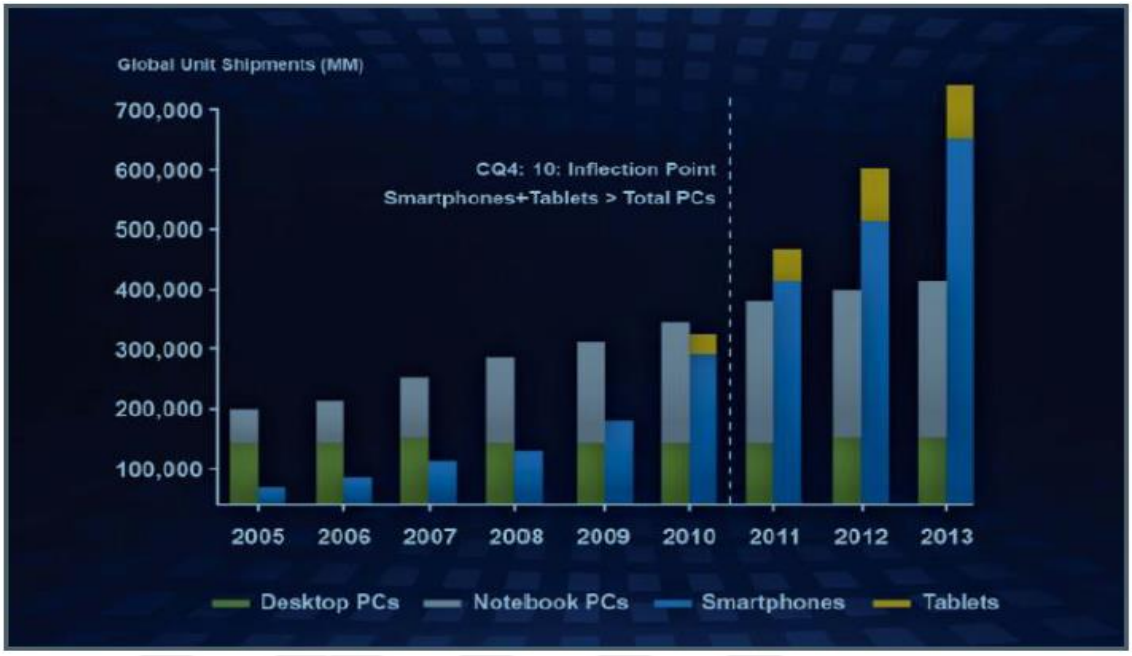
Şekil 3.4.2.1. NFC Kart Ödeme Özellikli Otopark Prototipi

3.4.3. NFC teknolojisine genel bakış ve NFC'nin geleceği

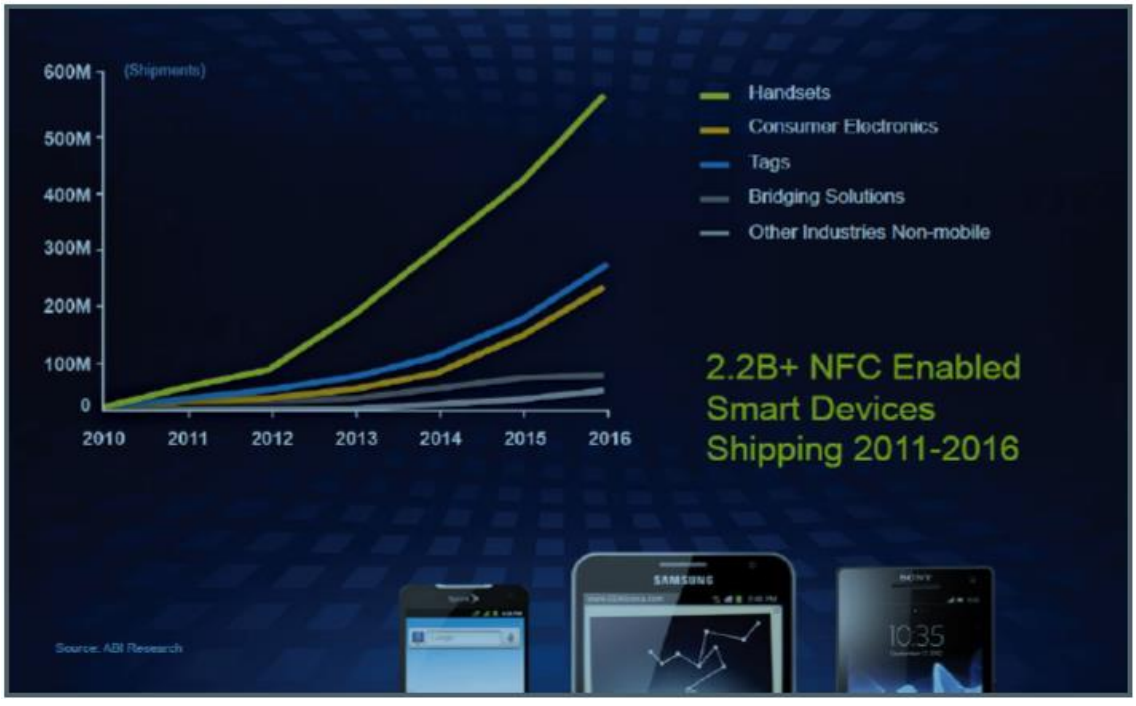
NFC hakkında uluslararası yapılan çalışmalar ve mobil ödeme yönetimi konusunda geliştirilen uygulamalar incelendiğinde, NFC'li cep telefonlarının sayısının artması, temassız ödeme sisteminde yer alan firmaların NFC'li ödemeye destek vermesi ve inovatif uygulamaların sunumu ile NFC'nin yeni kullanım alanları her geçen gün artmaktadır.

2020 yılında cep telefonlarının yarıdan fazlasının NFC destekleyeceği beklenmektedir ve NFC'nin görünen amacı temassız ödeme olsada geliştirilen interaktif uygulamaların birçok sisteme uygulanabilirliği gözlenmektedir. Tablo (3.4.3.1) ve Tablo (3.4.3.2)' de NFC cihazların yıllara göre üretim oranları araştırma sonuçlarına göre verilmektedir.

Tablo 3.4.3.1. NFC Cihaz Üretim Oranları 2005-2013 [4]



Tablo 3.4.3.2. NFC Cihaz Üretim Oranları 2010-2016 [4]



Operatörler, bankalar, kart üreticileri ve diğer servis sağlayıcı şirketlerin NFC'nin yaygınlaşmasına yönelik yapmış oldukları çalışmalar NFC'nin gelişimini ve gelecekte yaygın bir şekilde kullanılacağını göstermektedir.

Bu çalışmalara örnek verecek olursak;

 Ödeme sistemlerinde çözümler sunan Dünyanın önde gelen firmalarından Mastercard NFC'li Paypas uygulamasını duyurdu. NFC telefonunuzda Paypas hesabınızı aktifleştirdikten sonra paypas kabul eden terminale tek bir dokunuşla alışverişinizi rahat ve eğlenceli tamamlayabilmektesiniz. Yine NFC'li temassız ödeme sistemi çözümlerini sunan visa kart, PayWave desteği ile NFC'li temassız ödemenin önünü açmaktadır.

 Temassız ödeme sistemlerinde önemli bir role sahip olan NXP, Dünyada Toplu ulaşımda ve otoparklarda ödemenin hızlı bir şekilde temassız ödemeye geçtiğini ve NXP ürünlerinin kullanımı ile NFC'li temassız ödemeye geçişin hızlı olacağını belirtmektedir. Şekil (3.4.3.1.)' de Hollanda' da bulunan NXP merkez binası gösterilmiştir.

Şekil 3.4.3.1 Hollanda'da Bulunan NXP Merkez Binası

 İstanbul, Londra ve Nice'de otopark bileti için NFC çalışmaları yapılmıştır.

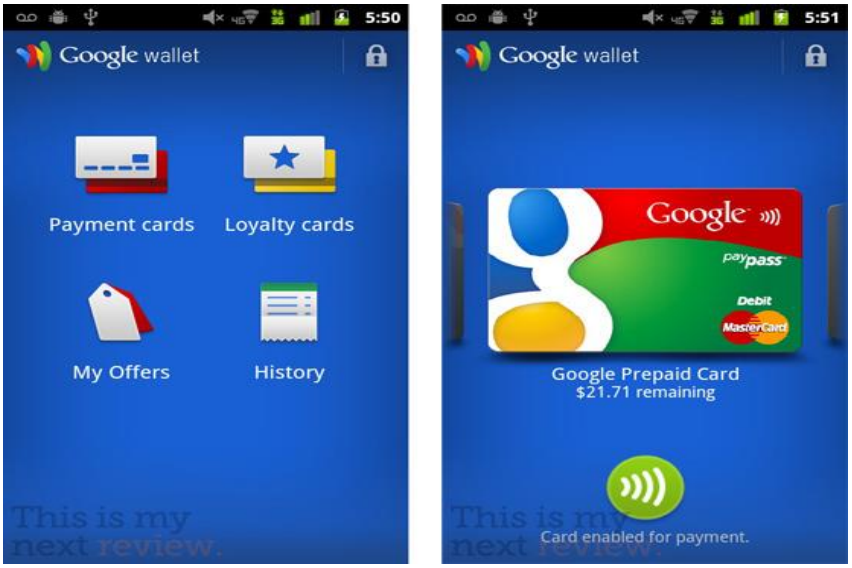
 Dubai'de otopark bileti olarak artık NFC'li cep telefonu kullanılmaktadır.

 Türkiye'de Banksoft, NFC Mobil ödeme sistemlerinde tüm operatörlerden ve bankalardan bağımsız bir TSM çözümü geliştirmiştir.

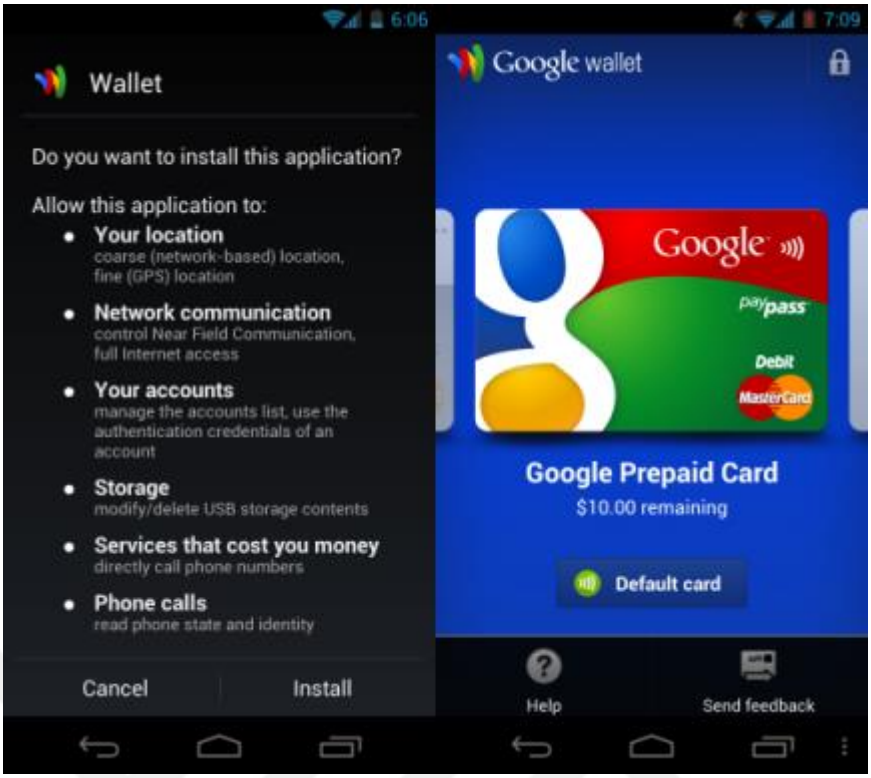
 ABD genelinde yaygın bir şekilde kullanılan ISIS Mobile Wallet, NFC uyumlu Android telefonlarda ve NFC destekli SIM kartlarda çalışan Mobil cüzdan uygulamasıdır. Şekil (3.4.3.2.)' de ISIS mobile wallet uygulaması gösterilmiştir.

Şekil 3.4.3.2. ISIS Mobile Wallet Uygulaması

Google'un duyurmuş olduğu Google Wallet projesi ile temassız ödeme olanağı sunulmaktadır ve birçok ülkede kullanılmaya başlanmıştır. Şekil (3.4.3.3.) ve Şekil (3.4.3.4.)' de Google Wallet uygulaması gösterilmiştir.



Şekil 3.4.3.3. Google Wallet Uygulaması



Şekil 3.4.3.4. Google Wallet Uygulaması

 Sony, elektronik ürünlerinde NFC özelliği taşıyan cihazlar(Laptop, cep telefonu, tablet) ve kullanımları için gerekli spesifikasyonları tanıtarak NFC cihazlar ile NFC Etiketler arasında tek bir dokunuşla haberleşmeyi (paylaşım, yükleme, dinleme, görüntüleme) sağlamaktadır. Şekil (3.4.3.5.)' de Sony NFC tablet gösterilmiştir.

Şekil 3.4.3.5. Sony NFC Tablet

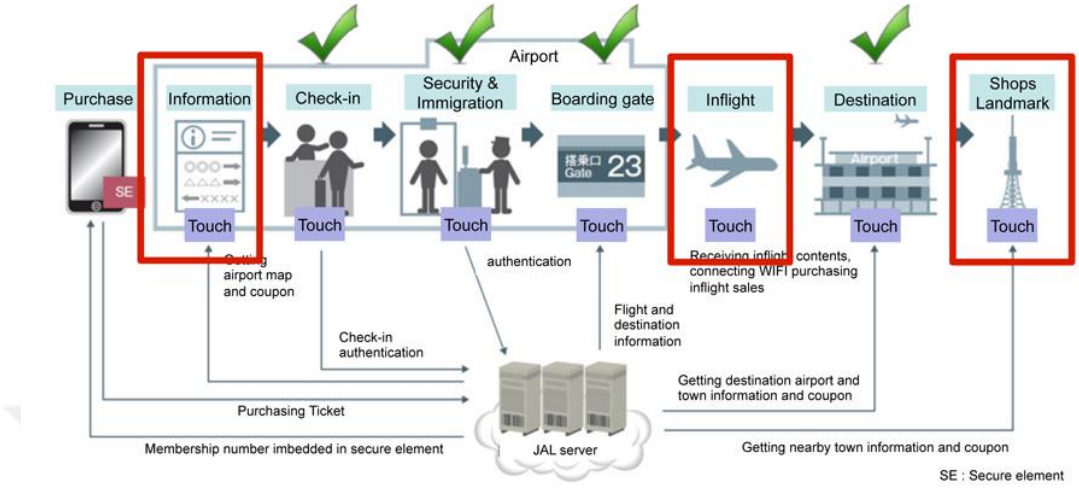
 Otomotiv sektöründen Almanya'dan PLDS firması, cep telefonu, tabletler aracılığıyla nfc teknolojisinin kullanım alanlarını(anahtar, cd/dvd, usb.) tanıtmıştır [5]. Nfc teknolojisine dayalı projelerle sürücüler araçlarda bulunacak olan kablosuz şarj cihazına telefonunu yerleştirerek cep telefonu ile araba arasında NFC'li haberleşme sağlanmakta cep telefonundan aracın hız, ışık, koltuk, ayna ayarlarının kontrollerini yapabilmektedir. Şekil (3.4.3.6.)' de PLDS firmasının ürettiği NFC özellikli araba, Şekil (3.4.3.7.)' de NFC'li otomotiv çözüm modelleri gösterilmiştir.

Şekil 3.4.3.6. PLDS Firmasının Ürettiği NFC Özellikli Araba [5]

Şekil 3.4.3.7. NFC'li Otomotiv Çözüm Modelleri [5]

Japon hava yolları, yeni uygulaması olan NFC'li boarding, geçişin nasıl kullanılacağı tanıttı ve havalimanlarında NFC'li Boarding, yolcuların check in ve geçiş işlemlerini

kolaylaştırarak vakit kazancı sağlamaktadır. Şekil (3.4.3.8)' de Japonya hava yolları NFC check in ve geçiş sistem şeması gösterilmiştir.



Şekil 3.4.3.8. Japonya Hava Yolları NFC Check İn ve Geçiş Sistem Şeması

 Otopark sekötürnde Dünya'nın bilinen büyük şehirlerine akıllı ve güvenli çözümler sunan firmalardan olan Thales'in NFC Mobil Bilet projesi ile otopark kullananların akıllı kart bilet taşımaktansa cep telefonlarını bilet olarak kullanabileceklerdir. Buna benzer olarak Fransa'da Cityzi firmasının Nice şehrinde uygulanan mobil bilet uygulaması dinlenildi. Uygulama tüm Fransız operatörler tarafından desteklenmektedir.

 Avusturya'dan Evva firmasının cep telefonlarının elektronik anahtar olarak kullanılmasını amaçlayan AirKey uygulaması ile kapıda bulunan NFC'li uç ile haberleşen cep telefonu anahtar görevi görmektedir. Şekil (3.4.3.9)' da kablosuz anahtar uygulama örneği gösterilmiştir.

Şekil 3.4.3.9. Kablosuz Anahtar Uygulama Örneği

 Canon, PowerShot SX700 HS kamerasına NFC özelliğini ekleyerek kullanıcıların android telefon veya tabletlerine dokunarak görüntü paylaşabileceklerini duyurdu. Şekil (3.4.3.10) da PowerShot SX700 NFC özellikli Canon kamera gösterilmiştir.

Şekil 3.4.3.10. PowerShot SX700 NFC Özellikli Canon

3.4.4. NFC iletişim modları

Ulaslar arası NFC standartlarına göre NFC iletişim modları aktif mod ve pasif mod olarak 2 grupta sıralanmıştır.

3.4.4.1 Aktif mod

Bu modda iki cihaz güç kaynağına sahiptir ve ürettikleri sinyal üzerinden birbiriyle iletişim kurabilirler. NFC okuyucu cihazlar aktif modda çalışır. NFC'li cep telefonu, aktif 15 modda çalışan bir NFC cihaz olduğundan NFC etiketlerden bilgi toplamanın yanısıra, diğer NFC cihazlar ile de bilgi alışverişinde bulunabilmektedir. Örneğin Akıllı posterden bilgi okuyan bir cep telefonu aktif modda çalışır. Ancak NFC'li ödeme yapan bir uygulama sırasında cep telefonu pasif modda uygulamayı kabul eden NFC okuyucu aktif modda çalışır.

3.4.4.2 Pasif mod

Bu modda, başlatıcı cihaz radyo sinyalleri üretir ve hedef cihaz bu elektromanyetik alan tarafından oluşturulan gücü alır. Hedef cihaz, mevcut elektromanyetik alan ile başlatıcı cihaza yanıt verir. Manyetik alan tarafından desteklenerek çalışan NFC Etiket'ler pasif modda çalışır.

3.4.5. NFC çalışma modları

NFC Linkte her iki cihaz, veri taşıyan bir RF sinyali üretmek için bir aktif mod vardır bir de sadece tek bir NFC cihazının RF sinyali ürettiği pasif mod çalışmaktadır. NFC standardının parçası olan iki bağlantı için farklı çalışma modları tanımlanmıştır. Pasif cihaz geri RF sinyali (başlatıcı cihaza) üreten cihaza veri aktarmak için düzenli bir yükleme modülasyonu kullanır.

İki çalışma modu da NFC tabanlı cihaz için en uygun olacak uygulamaları tanımlamaya yardımcı olmak için NFC Forum tarafından belirtilen iletişim modları kullanırlar. NFC Forum tarafından belirlenen 3 farklı çalışma modu vardır. Bunlar; Kart Emulasyon modu, Uçtan uca modu ve Okuyucu/Yazıcı modudur.

Kart Emulasyon modu kullanılarak güvenli bir veri aktarımı ile cep telefonu akıllı kart gibi davranır. Okuma Yazma iletişim modu uygulamaları, NFC Forum tarafından belirtilen ileti biçimini kullanarak veri transferi sağlayan bir okuma / yazma modunu içerir ve üçüncü bir uçtan uca modu ile bir cihazdan başka bir cihaza cihaza bağlantı sağlanarak iletişim desteklenir.

3.4.5.1. Kart emulasyon mod

Bu modda NFC cihazı sanki bir akıllı kart gibi davranır. Akıllı kart okuyucu cep telefonunu akıllı kartı okuduğu şekilde okuyabilir. Bu modda özellikle Ödeme ve bilet uygulamaları çalışmaktadır. Temassız ödemenin cep telefonundan yapılabildiği elektronik ödeme sistemi için oluşturulmuştur. Toplu ulaşım biletleri, park ödeme uygulamaları bu modda çalışan uygulamalara örnektir. Bu modda cep telefonunuz, bir banka kartı, kredi kartı, toplu taşıma bileti, sadakat kartı, kimlik ve anahtar olarak kullanılabilmektedir.” Dokun ve Öde” sloganıyla duyrulur.

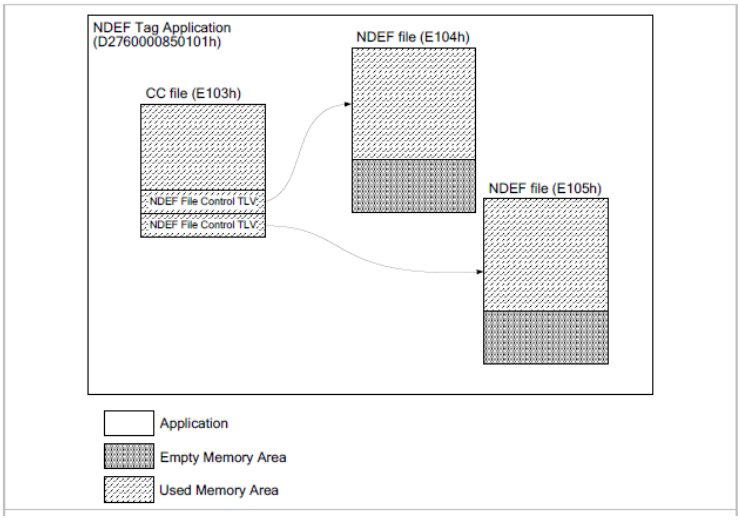
3.4.5.2. Okuyucu/yazıcı mod

NFC cihazı başka bir akıllı karta okuyucu gibi erişecek moddadır. Bu modda NFC cihazı pasif NFC etiketindeki bilgileri okuyup, NFC etikete yazabilecek şekilde çalışmaktadır. NFC cihaz NFC etikete dokundurulduğunda haberleşme başlar ve NFC etikette yer alan bilgi NFC cihaza aktarılır. Akıllı posterler ve ürünler hakkında bilgi veren NFC etiketler bu modda çalışan uygulamalara en iyi örneklerdendir. Şekil (3.4.5.2.1.)’ de NFC telefon NFC etiket okuma yazma modu gösterilmiştir.

Şekil 3.4.5.2.1. NFC Telefon NFC Etiket Okuma Yazma Modu

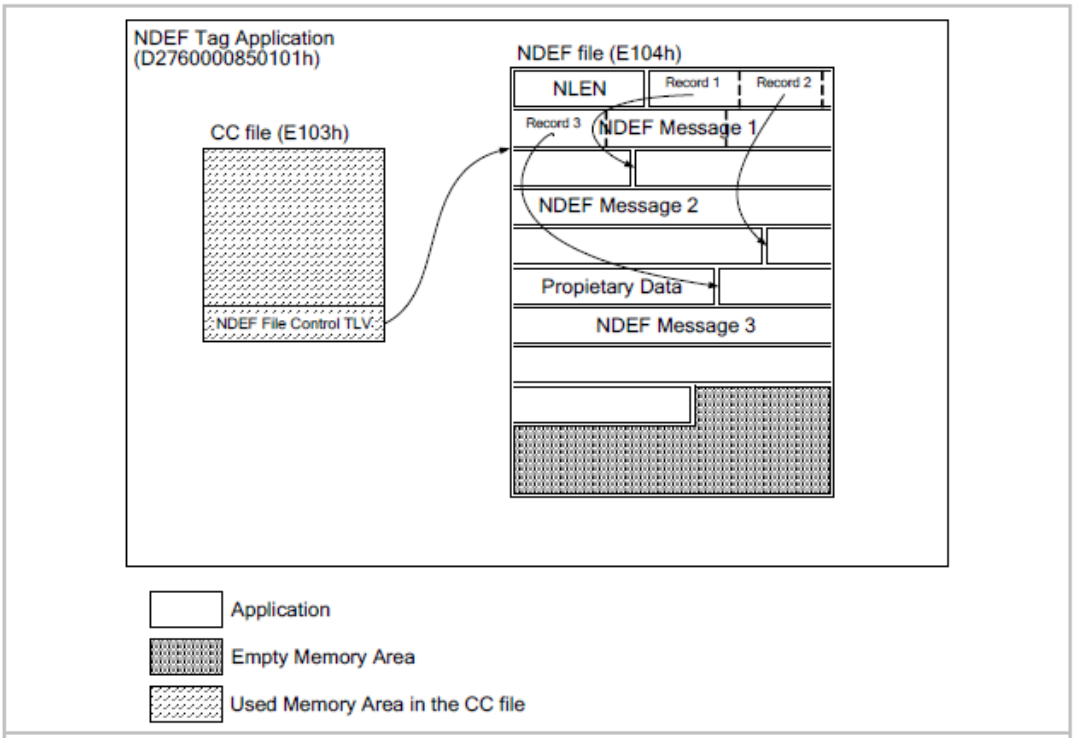
3.4.5.3. Uçtan uca mod

Bu modda iki NFC cihazı birbiriyle haberleşerek bilgi alışverişinde bulunabilir. Bu modda bir cihaz aktif durumda iken diğer cihaz pasif durumdadır. Bu modda iki cihaz arasında yapılan paylaşıma en iyi örnek bluetooth eşleştirme bilgisidir. NFC teknolojisi ile veri alışverişi gerçekleştirilmektedir ancak çok büyük boyutlu verilerin taşınmasında Bluetooth, Wifi gibi diğer iletişim kanallarına ihtiyaç duymaktadır. Şekil (3.4.5.3.1.)' de birkaç NDEF dosyasının NDEF tag uygulamasındaki örneği gösterilmiştir.



Şekil 3.4.5.3.1. Birkaç NDEF Dosyasının NDEF Tag Uygulamasındaki Örneği [7]

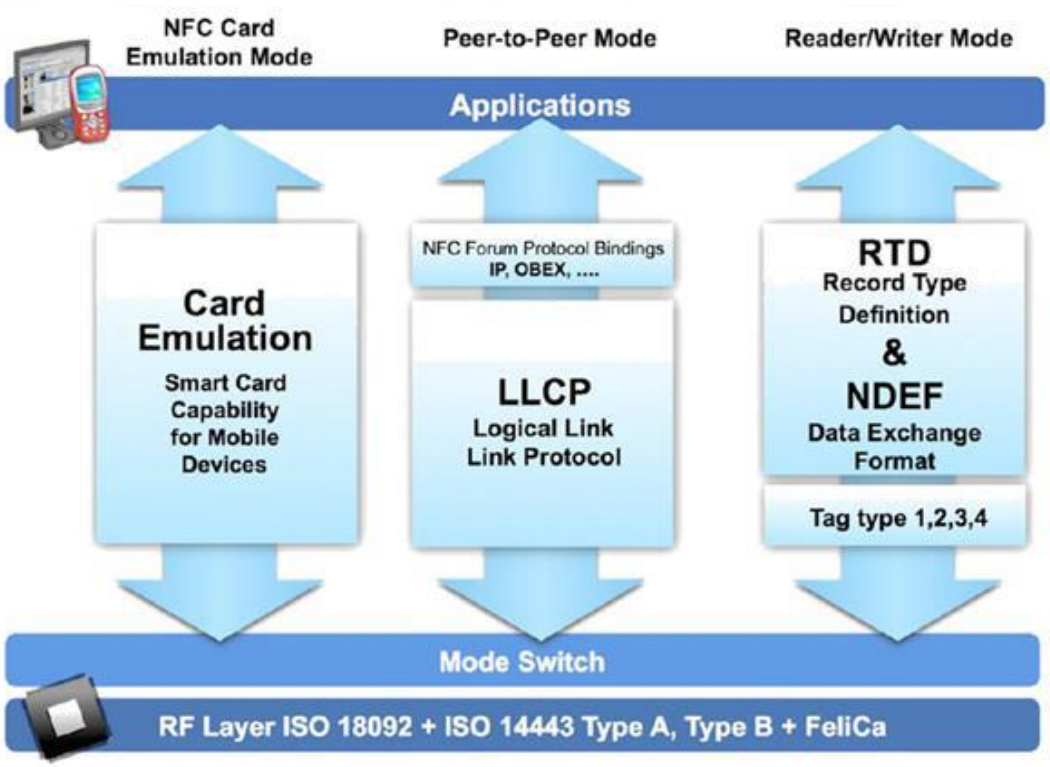
İki cihaz arasında NFC ile eşleştirme kolayca gerçekleştirildikten sonra veri büyük boyutta ise Wifi bağlantısı ile birlikte taşınır. Bu modda NFC cihazları iletişim kurarken NFC Forum'un Logical Link Control Protocol, Mantıksal Bağlantı Kontrol Protokol (LLCP)'nü kullanırken Simple NDEF Exchange Protocol, Basit NDEF Veri Taşıma Protokol (SNEP) ile iki cihaz arasında NDEF mesajlaşma sağlanır. Şekil (3.4.5.3.2.)' de aynı NDEF dosyasında üç NDEF mesajı örneği ve patentli veri bloğu örneği gösterilmiştir.



Şekil 3.4.5.3.2. Aynı NDEF Dosyasında Üç NDEF Mesajı Örneği Ve Bir Patentli Veri Bloğu Örneği [7]

NFC cihazlar arasında kolayca Bluetooth eşleştirme, fotoğraf, müzik, URL paylaşımları örnek verileceği gibi sosyal ağların kullanımında ve oyunlarda etkin kullanımı olan bir moddur. Bu modda çalışan uygulamalar "Dokun ve Paylaş", "Dokun ve Eşleştir" sloganlarıyla duyulur. Şekil (3.4.5.3.3.)' de NFC Bluetooth kulaklık eşleştirme gösterilmiştir. Şekil (3.4.5.3.4.)' de NFC standart arabirimi üç çalışma modu gösterilmiştir.

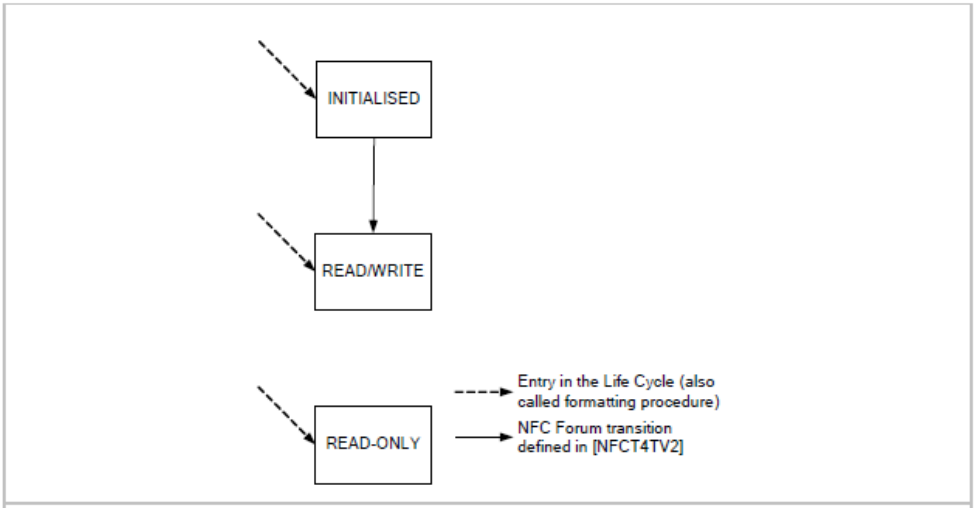
Şekil 3.4.5.3.3. NFC Bluetooth Kulaklık Eşleştirme [6]



Şekil 3.4.5.3.4. NFC Standart Arabirimi Üç Çalışma Modu [7]

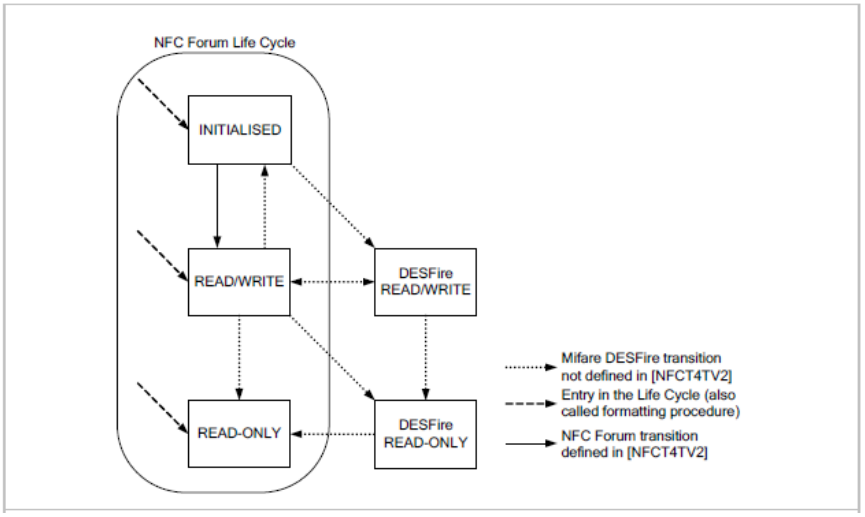
3.4.5.4. NFC yaşam döngüsü

NFC yaşam döngüsü [NFCT4TV2] tarafından belirlenen yaşam döngüsü gösterir. Yaşam döngüsünde geçişler 4 tip etiket yönetmek için NFC Forum cihazda uygulanır. MIFARE DESFire NFC Forum yaşam döngüsü ile tam uyumludur. Şekil (3.4.5.4.1.)' de NFC forum yaşam döngüsü gösterilmiştir.



Şekil 3.4.5.4.1. NFC Forum Yaşam Döngüsü [7]

MIFARE DESFire yaşam döngüsü ise ek bileşenler, girişler ve spesifik MIFARE DESFire özelliklerinden faydalanmak geçişler ile birlikte NFC Forum tarafından belirlenen yaşam döngüsü gösterir. Şekil (3.4.5.4.2.) de Mifare Desfire yaşam döngüsü gösterilmiştir.



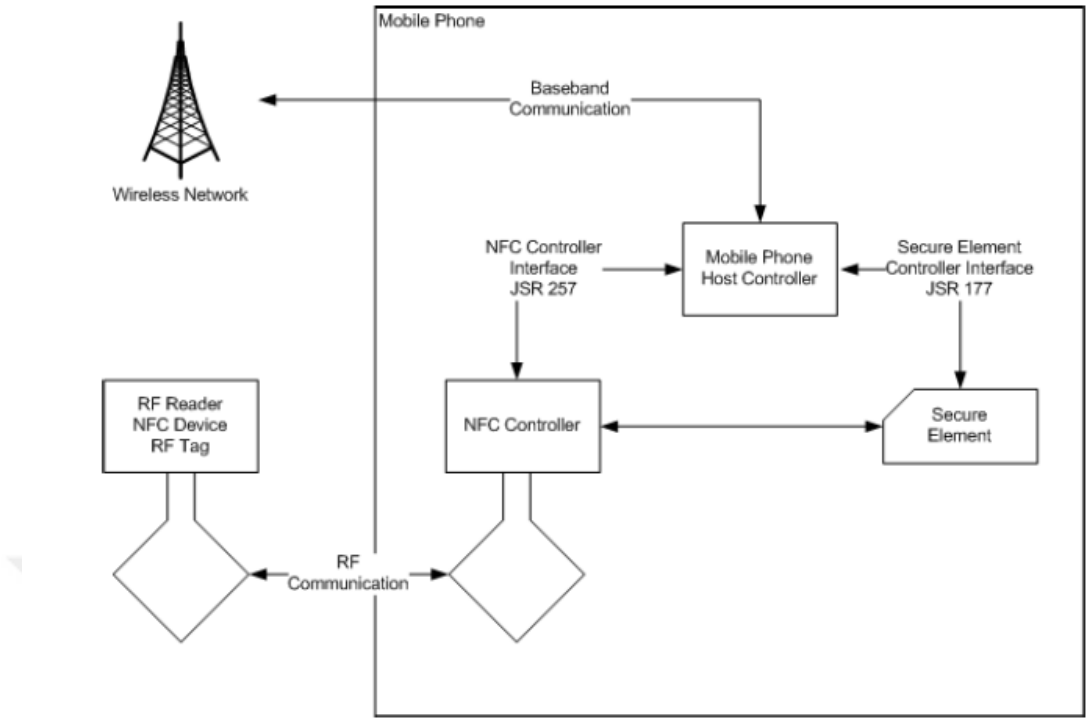
Şekil 3.4.5.4.2. Mifare Desfire Yaşam Döngüsü [7]

3.4.6. Güvenli/secure element

Ödeme uygulamalarında key, hesap bilgileri gibi önemli verilerin depolandığı ve yönetildiği dış müdahalelere dayanıklı güvenli alandır. Birçok NFC uygulaması korunması gereken gizli veriler kullanmaktadır. Bu gizli bilgilerin saklandığı yer Secure element olarak adlandırılır ve NFC teknolojisinin olmazsa olmaz bir parçasıdır. Secure element, işletim sistemi üzerinde akıllı kart uygulamalarının bulunduğu mobil cihazlarda yer alan güvenli alandır. Ödeme uygulamalarında gizli bilgilerin saklanmasını sağlayan ve güvenliği kolaylaştırmak için yapılan şifreleme işlemlerine destek veren güvenli bellektir.

Yeni üretilen secure elementlerde yer alan ödeme uygulamalarına örnek olarak American Express ExpressPay, Discover Zip, MasterKart PayPass, Visa payWave gösterilebilir [8]. Ayrıca otoparklarda ödemenin yapıldığı bilet ile kapı anahtarı gibi güvenli erişim gerektiren uygulamalarıda destekler. (Şekil 3.4.6.1.)'de belirtilen iletişim kanallarına göre Secure elementte Global platform standartları geçerlidir ve Java kart işletim sistemine göre düzenlenmiştir. Secure element üreten firmalar, secure elementi sahibi olacak MNO, banka gibi diğer firmalara istenilen özelliklerde secure element üretimi sağlarlar. Secure elementin sahibi olan firma secure elementin yönetiminden ve korunmasından sorumlu olur. NFC ekosisteminde yer alan aktörler arasındaki ilişki secure elementin rolüne göre değişiklik gösterebilmektedir. NFC Secure Element, içerisindeki akıllı kart yonga güvenliğini sağlayarak gizli bilgileri hafızasında tutar.

Telefonun anakartı üzerinde gömülü parçası veya sonradan eklenen güvenli bir yonga şeklinde ve SIM kart üzerinde güvenli öğe olmak üzere 3 çeşit NFC Secure element bulunmaktadır [9].



Şekil 3.4.6.1. Secure Element İletişim Şekli [9]

3.4.6.1. Gömülü yonga

Cep telefonu üreticileri tarafından telefondaki NFC Kontrolör içerisine Secure element yerleştirebilmektedir. Güvenli bellek doğrudan anakarta lehimlenmiştir. Cep telefonunda gömülü bir güvenli alan için telefon üreticileri ve diğer aktörler arasında iş birliğine varılıp ortak bir standart getirilmesi gerekmektedir. MNO'lar bağımsız bir model olacağından ve OTA yönetiminin maliyetinin daha düşük olması nedeniyle Bankalar ve diğer servis sağlayıcılar tarafından desteklenen bir model olmuştur. Ancak telefon içerinde güvenli alan için elverişli bir alan olması gerektiğinden ve üreticilerin maliyetini artıracağından, secure elementin yönetiminde telefon üreticilerine ayrıca bir sorumluluk yükleyeceğinden dolayı SIM kart daha alternatif görünmektedir.

Mobil ödeme uygulaması telefonda gömülü olarak bulunan secure elementde yer alacağı için kullanıcı telefonunu değiştirdiğinde yeniden uygulamayı yüklemesi gerekmektedir.

Telefon değişikliği veya kullanıcı değişikliği birtakım güvenlik sorunlarınıda ortaya çıkaracağından birçok kullanıcı tarafından tercih edilmeyecektir bu model. Teknik olarak SWP protokol ile haberleşme sağlanmaktadır.

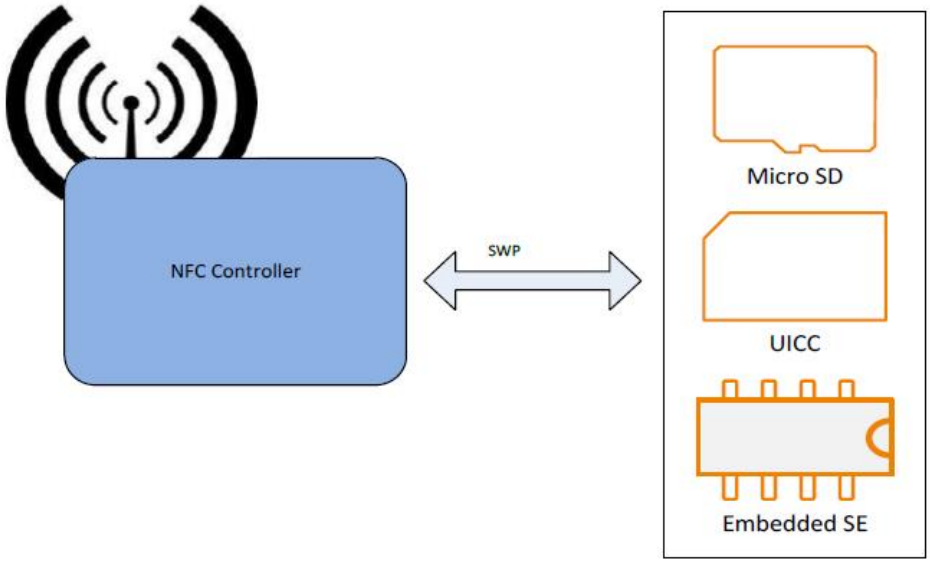
3.4.6.2. SIM (UICC)

SIM kart, cep telefonlarının GSM servisinden yararlanmasını sağlayan akıllı karttır. UICC, GSM ağlarındaki mobil cihazlarda kullanılan akıllı kart olduğu gibi aynı zamanda ETSI Akıllı kart platformu tarafından tanımlanan UMTS şebekelerinde de kullanılmaktadır. Mobil ödemelerde güvenli elementin SIM kart üzerinde olduğu bir iş modelinde ödeme uygulaması SIM kart üzerine yüklenir. Mobil ödeme uygulamasının UICC üzerinde yer alabilmesi için birtakım işlemlerden geçmesi gerekmektedir. SIM kartın ömrü cep telefonu ve diğer harici hafıza kartlarına göre daha uzun olduğu için güvenli elementin SIM kart üzerinde olması daha avantajlıdır. Her Servis sağlayıcı yalnızca kendisinin erişebileceği özel güvenli alanlara sahip olabilmektedir. SIM kart üzerinde. OTA uygulamaları ile güvenli alana uygulama yüklenebilir, güncellenebilir, kişiselleştirebilmektedir. Böylece kullanıcılara daha hızlı hizmet verilecektir. Cep telefonunuzun imha olduğu durumlarda özellikle uzaktan SIM karta erişim yapılarak güvenli bir şekilde uygulamalar kaldırabilmektedir. Kullanıcı telefonunu değiştirmek istediğinde ise SIM kartında bulunan mobil ödeme uygulaması SIM kart aracılığıyla kullanıcıyı tanımasından sonra yeni telefonunda aktif hale gelir. SIM kartın NFC Kontrolör ile ve uygulamalarla haberleşebilmesi için birtakım standartlara sahip olması gerekmektedir. ETSI ve Global Platform spesifikasyonlarına göre standartlaştırılmıştır. Single Wire Protokol (SWP) kullanılarak SIM kart ile NFC Kontrolör arasında iletişim sağlanmaktadır [10]. Şekil (3.4.6.2.1.)' de SIM (UICC) örneği gösterilmiştir.

Şekil 3.4.6.2.1. SIM(UICC) Örneği

3.4.6.3 Hafıza kart (SD Kart)

Cep telefonu ve diğer mobil cihazlar ile entegre etmek için tasarlanmış bir bellek kartıdır. NFC özelliği bulunmayan cep telefonlarında NFC Kontrolör ve Secure Elementin bir arada bulunduğu özel yongalardır. SD kartın kullanıldığı Mobil ödeme uygulaması modelinde Service Provider'lar MNO'lara mobil hizmet ücreti ödemek zorunda kalmadan uygulamarını secure elementte saklayabilmekteler. Ödeme uygulamalarının SD kart üzerinde yer alması ve yönetilmesi için standartların oluşturulması gerekmektedir. SD kartın ödeme uygulamalarının yönetiminde SIM kart modeline benzerlik göstermesi, veri depolama yerinin SIM karttan ve telefondan ayrı olması avantajlarındandır. Yani kullanıcı mobil aboneliğini nereden aldığından etkilenmeden SIM kartından bağımsız bir şekilde ödeme uygulamalarının bulunduğu SD kartını kullanabilecektir. Ayrıca daha fazla depolama hafızası sunabileceğinden kullanıcının özel kullanım ihtiyacını karşılayabilecektir ve SIM kart gibi sınırlı olmayarak kullanıcıya bellek boyutu seçimi sunabilecektir. SD kart teknik olarak NFC Kontrolör ile SWP üzerinden iletişime geçmektedir. Şekil (3.4.6.3.1)' de NFC kontrolör ve Secure Element iletişim kanalı gösterilmiştir.



Şekil 3.4.6.3.1. NFC Kontrolör ve Secure Element İletişim Kanalı [11]

3.4.7. NFC ve güvenlik yapısı

NFC teknolojisi yakın mesafe haberleşmeyi desteklediğinden iki cihazın dokundurulacak kadar yaklaştırılması aradaki haberleşmeyi güvenli hale getirir. Böylece telefondaki veriler ve SE içerisindeki veriler çalınmaya karşı korunmuş olur.

Gelişen teknolojiler her zaman güvenlikle ilgili bazı endişeleri de beraberinde getirmektedir. Örneğin iki cihaz arasındaki iletişim esnasında üçüncü bir tarafın hattı dinlemesi şeklinde olabilir. Bu dinlemede aradaki şifrelemenin kırılması ile bilgilere 3. Şahısların da erişebilmesi demektir. Diğer bir endişe ise gönderilen bilginin değiştirilmesi ya da bozulmasıdır. Bir diğeri ise işletim sistemi üzerinden bulaşan virüslerdir.

Güvenlik risklerine karşı kartlı ödeme sektöründe çeşitli önlemler alınmaktadır. Örneğin Visa ve MasterCard geliştirdikleri güvenlik yöntemleri ve koydukları kurallarla saldırılara maruz kalınmasını, kart bilgilerinin kopyalanması ve şüpheli işlemlerin kontrol edilerek engellenmesini sağlamışlardır.

NFC özellikli iki cihaz arasında verilerin gizlenmesi amacıyla şifrelenmesi gerektiğinde AES (Advanced Encryption Standart-Gelişmiş Şifreleme Standardı) kullanılmaktadır.

NFC teknolojisinin geleceği hakkında ABI araştırmalarına göre önümüzdeki 5 yıl içerisinde Dünya'da 32 milyar bilet mobil olacaktır ve bunların % 30'u NFC cep telefonlarından temassız gerçekleştirilecektir [12].

3.4.7.1. Güvenlik yapısı

NFC uygulaması ve veriler NFC cihaz bilgilerin gizlilik durumuna göre üzerinde şifreli veya şifresiz olarak saklanabilir. Otopark biletinde kullanıcıların bilgilerin, bakiyelerini ve diğer bilet bilgilerini içeren bu hassas bilgilerin NFC cihaz üzerinde güvenli bir şekilde saklanması ve yönetilmesi gerekmektedir.

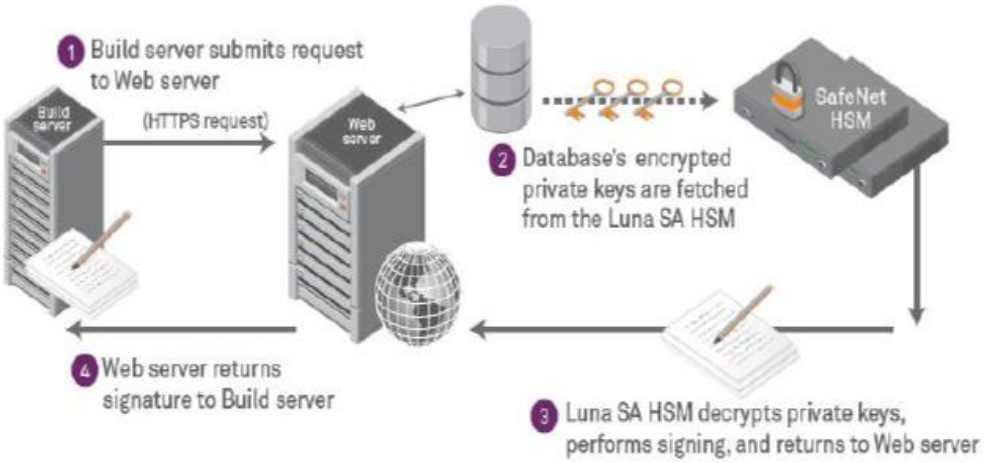
Cep telefonlarında veriler için en güvenli ortamı sunan SIM kartlardır [10.]. Oluşturulan Global Platform standartları ile SIM kartların MNO, SP ve cep telefonu üreticileri ile NFC'li ödeme sisteminde haberleşmeleri güvenli bir şekilde gerçekleştirilmektedir

NFC Mobil Bilet Ekosistemindeki tüm paydaşlar, güvenli bir ödeme için sahteciliğe karşı standartlara uygun bir şekilde güvenliği sağlamalıdır. Kullanıcıların bilgileri ve ödeme bilgileri şifreli bir şekilde güvenli bir kanal üzerinde iletilerek SP TSM, MNO TSM ve Telefon arasında güvenli kanal oluşturulur. Bilet Uygulamasının personalizasyonu ve yönetiminde kullanılan anahtarların oluşturulması ve saklanması HSM tarafından gerçekleştirilerek 3. Kişilerin bu anahtarlara erişmesi engellenmektedir. Akıllı kart sistemlerinde anahtarları yüklemek için kart basım merkezine ve güvenli oda ile personele ihtiyaç duyulurken NFC Mobil Bilet sisteminde fiziksel bir ortama gerek kalmadan OTA üzerinden yüklenebilmektedir.

Secure Channel Protocol olarak bilinen SCP'ler ile uygulamaların güvenli dağıtımı OTA üzerinden gerçekleştirilir. Global Platform spesifikasyonlarında belirtilen SCP'ler şifreleme hizmetleridir.

3.4.7.2.HSM ile şifre yapısı

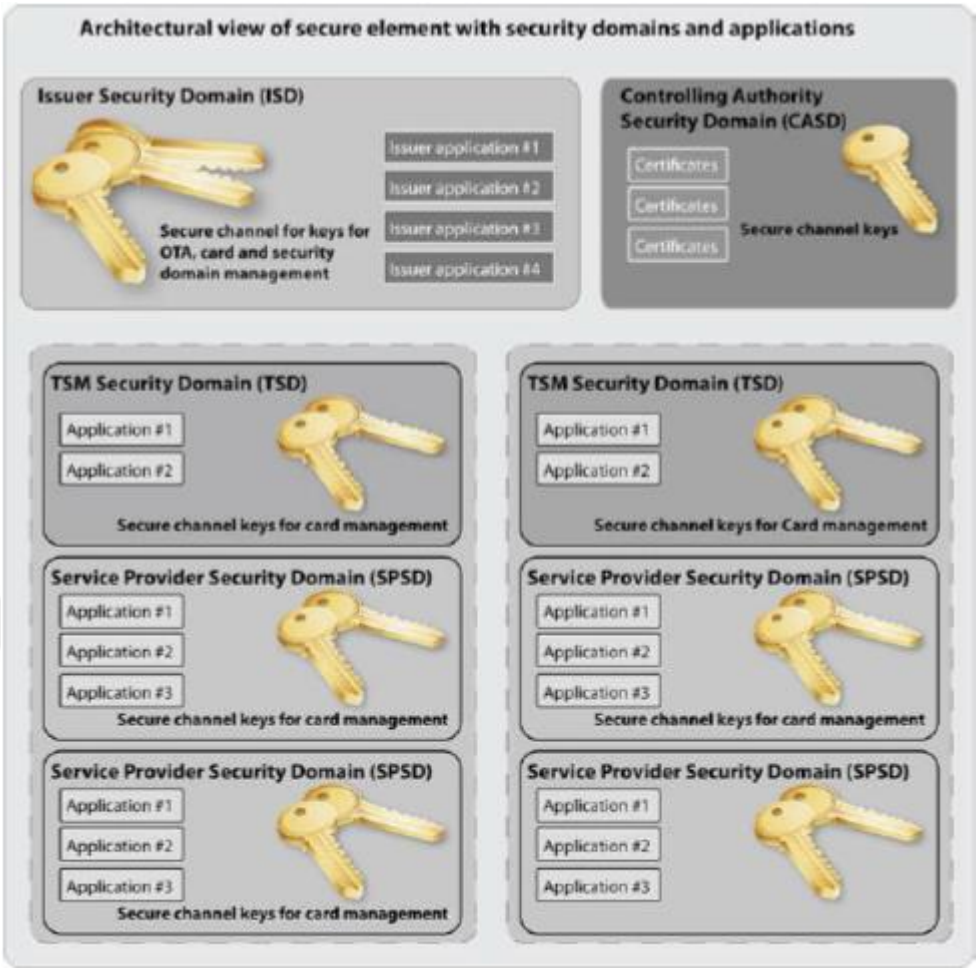
HSM, Hardware Security Module; hassas kriptografik anahtarları fiziksel ortamlarda saklamak ve kriptografik işlemleri en güvenli şekilde gerçekleştirmek için üretilmiş özel güvenlik donanımlarıdır. Bu donanım uygulamanın güvenli bir şekilde çalışmasını sağlar. Kritik güvenlik seviyesine sahip uygulamaların key yönetimi ve şifrelenmesini sağlayan donanım tabanlı çalışan parçadır. PIN yönetimi, Kök anahtar korunumu, online bankacılık, veritabanı şifreleme, kod imzalama gibi işlemler HSM ile çalışan uygulamalara örnektir [13]. HSM'ler saldırılara karşı savunma sistemleri ile donatılmışlardır. Veri güvenliğinin sağlanması gereken durumlarda HSM, güvenli internet kanalı üzerinden verilerin dağıtımını gerçekleştirir. NFC'li Ödeme uygulamalarında anahtar yönetimi ve kriptografik işlemlerde HSM önemli rol oynamaktadır. NFC Mobil Bilet uygulamasının personalizasyonu ile uzaktan yönetiminde gerekli anahtarlar HSM aracılığıyla güvenli bir şekilde üretilmekte ve HSM üzerinde saklanabilmektedir [14]. Şekil (3.4.7.2.1.)' de HSM ile şifreleme yapısı gösterilmiştir.



Şekil 3.4.7.2.1. HSM ile Şifreleme Yapısı [13]

3.4.7.3. Güvenli kanal protokolleri/secure channel protocols

Secure Channel güvenli kanal olarak bilinen protokoller, SIM karta gönderilen verilerin Global Platform uyumlu APDU komutlarıyla güvenli kanal üzerinden şifreli olarak gönderilmesini sağlar. NFC Cep telefonu ile TSM arasında HTTP üzerinden iletişim kurulur ve Mobil Uygulama arayüzünden SIM karta erişim sağlanır. Global Platform spesifikasyonlarına göre birden fazla uygulamanın yönetimi tek bir simkart üzerinde olabilmektedir. Her bir güvenli alanın yönetimi güvenli kanal üzerinden gerçekleşmektedir [15]. Şekil (3.4.7.3.1.)' de Secure Elementin mimarisi ile güvenli alan ve uygulamaları gösterilmiştir.



Şekil 3.4.7.3.1. Secure Elementin Mimarisi ile Güvenli Alan ve Uygulamalar [16]

3.4.7.4. SCP 02

SCP 02 protokolü SIM kart üzerinde güvenli alanla dışardan ISO arayüzünden direk erişim salayan protokoldür. Güvenlik gerektiren ödeme uygulamalarında kullanılmak için oluşturulan güvenli kanaldır. SIM kart ile SP TSM arasındaki veriler SCP 02 anahlarları ile şifrelenerek iletilir.

3.4.7.5. SCP 80

SCP80, Global Platform ETSI TS 102 225 standardı ile tanımlanan güvenli OTA bir protokolüdür.

3.4.7.6. SCP 81

SCP81 Global Platfrom 2. 2 tarafından ETSI TS 102 226 standardı ile tanımlanan TLS güvenli protokolü temsil eder. HTTPS üzerinden uzaktan güvenli uygulama işlemlerinde kullanılır. SCP80/81 üzerinden SCP 02 protokolleri, SP ve MNO'ların uygulama yönetimindeki rollerini ayırmada kullanılır. SE'e gönderilecek olan her bir uygulama bilgisinin (script) güvenli iletimi için SCP 02 oluşturulur. SCP 02 ile şifrelenmiş bilginin güvenli iletimi için SCP 80 veya SCP 81 oluşturulur.

SCP kullanmak aşağıdaki nedenlerden dolayı gereklidir:

- Uygulama yöneticisi olan SP ve MNO tarafından çift taraflı onaylanma gerektirir. İki taraf onaylamadan erişime izin verilmez.
- SP'lerin mevcut kişiselleştirme (personalizasyon) sistemleri SCP 02'ye dayalıdır ancak OTA üzerinden yeniden şifrelenerek taşınması gerçekleştirilir.
- Oluşturulan iki protokolün yönetimi (Şekil 3.4.7.3.3.1.)'de ki gibidir. Her bir SCP protokolü farklı SD'ler için kullanılır.

Şekil 3.4.7.3.3.1. SCP Protokolü

3.4.7.7.Ödeme bilgilerine erişme

Ödeme Bilgileri olan, miktar, geçiş zamanı, otopark yeri (bariyer bilgisi), bilgilerine ödemeyi kabul eden cihaz, otopark merkez operatörü ve müşteri görebilir.

3.4.7.8.Standartlar

NFC Kart Emülasyon Modda çalışan bariyer sistemleri ve el terminalleri ile Temassız okuyucu, ISO 14443 Tip A veya ISO 14443 Tip B uyumludur.

ETSI, Mifare4Mobile ve Global Platform spesifikasyonları gereklidir.

Anahtar Yönetimi; Mobil NFC servisi için geliştirilen GPS services 1.0 mesajlaşma spesifikasyonuna göre yapılmaktadır [16].

Ayrıca kullanıcının kredi kartı veya banka kartı bilgileri alınacaksa PCI standartına sahip olunmalıdır.

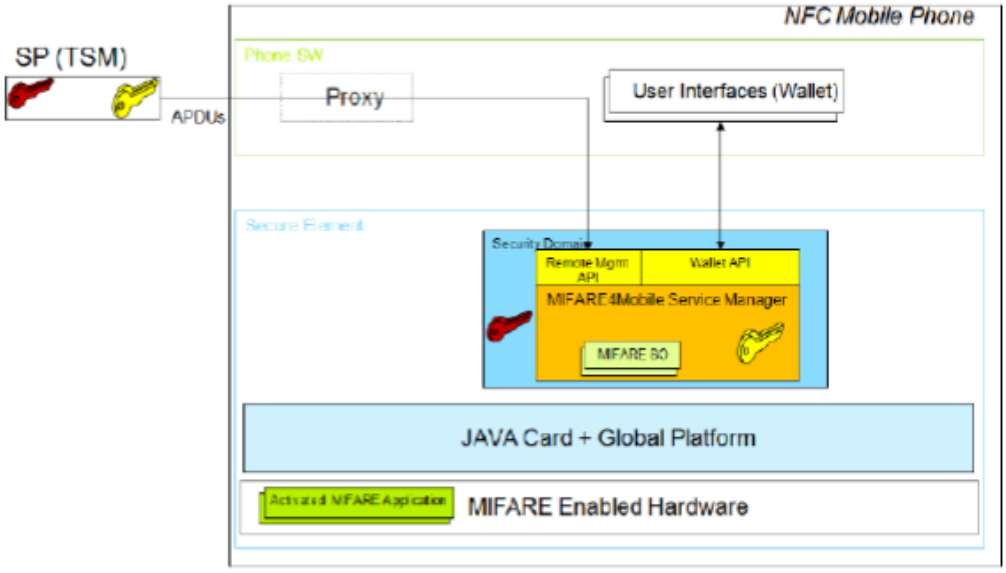
3.5. Temassız Akıllı Kart Teknolojisi ve Mifare4Mobile

Temassız akıllı kartlar, içinde bir mikro işlemcili yonga ve anten bulunan plastik kartlardır. RFID teknolojisini kullanarak kart okuyucular ile haberleşir. Temassız haberleşme karttaki antenin kart okuyucuya yaklaştırılması ile sağlanır. Temassız teknoloji, ISO / IEC 14443 ve ISO / IEC 15693 olmak üzere iki ana standarda dayalıdır. ISO / IEC 15693, 1 metre mesafeye kadar haberleşme olanağı sunarken, ISO / IEC 14443 standardı an fazla 10 santimetreden yakın haberleşmeyi sağlayarak bankacılık gibi temassız ödeme sistemlerinde güvenlik gerektiren uygulamalarda kullanılmakta, temassız kartlar ISO / IEC 14443 standardına dayalıdır.

Dünya'da 1,2 milyar insanın kullandığı Mifare Temassız teknolojisi Toplu ulaşımda kullanılan biletlerin % 74'ünü oluşturmaktadır. Mifare ürünleri, ISO / IEC 14443 standardına dayalıdır ve uluslararası güvenlik sertifikalarına sahiptir.

Mifare4Mobile 2008'de NXP tarafından mobil cihazlarda Mifare tabanlı uygulamaları yönetmek için oluşturulmuş bir spesifikasyondur.

Şekil 3.5.1.'de gösterilen Mifare4Mobile teknolojisi, mevcut ISO / IEC 14443 standardı ile uyumlu ve NFC'li mobil cihazlarda mifare uygulamaların yönetimini standardize etmektedir.



Şekil 3.5.1. Mifare4Mobile Servis Yönetiminde TSM ve Cüzdan Arayüzleri [17]

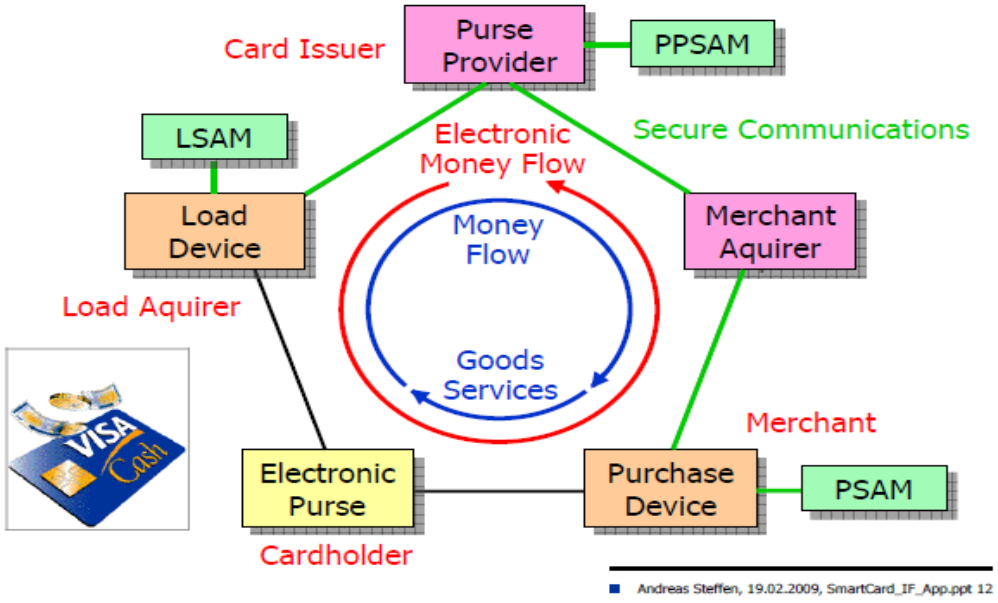
MIFARE4Mobile V2.0 spesifikasyonu, MIFARE DESFire, MIFARE DESFire EV1 ve MIFARE Classic bilet yapılarını mobil yapmak için geliştirilmiştir. Mifare4Mobile farklı platformlar(UICC, Gömülü Güvenli Eleman, Mikro SD kart, Servis sağlayıcılar, MNO, diğerleri) arasında birlikte çalışılabilirliği sağlamaktadır [17]. Mifare4Mobile Spesifikasyonu;

- Aynı anda birden fazla TSM servisi ile çalışmaya uyumludur.
- Bir Secure Element üzerinde birden fazla Mifare uygulamasının bulunmasını destekler. Global Platform 2. 2 kart spesifikasyonlarına uygundur.
- Servis Sağlayıcı ile Mifare uygulama arasında uçtan uca güvenlik sağlar.

Mifare4Mobile NFC özellikli cihazlarda bilet yönetimi için mevcut akıllı kartlardaki hafıza, uygulama yapısının, fonksiyonlarının aynı olması gibi gerekli temel gereksinimleri karşılamalıdır. MIFARE4Mobile V2.0 ile Secure Element üzerinde mevcut akıllı kartların fonksiyonlarını yerine getirebilen birden fazla sanal kart vardır. Şekil (3.5.2.)' de elektronik cüzdan çalışma şeması verilmiştir. MIFARE4Mobile V2.0 sanal kartların özellikleri:

- Aynı anda birden fazla akıllı kart çalıştırır.

- Temassız okuyucular, ISO / IEC 14443 tarafından tanımlanan anti-collision(çakışmayı önleme)'yi desteklemeye ihtiyaç duymaz.
- Sanal kartlar tek bir UID(kartın seri numarası)'yi ortak kullanabilirler.
- Aynı UID'ye sahip ve çakışmayan sanal kartlar(birden fazla desfire uygulaması) aynı anda aktif edilebilir.
- Sanal kartın yetkilendirilmesi daima Secure Elementin sahibi tarafından(SEI TSM veya SEI adına görevli TSM) yapılır.
- Birden fazla servis sağlayıcı TSM'le çalışmaya uyumludur.
- Sanal kart yalnızca bir Servis Sağlayıcı ya da servis sağlayıcılar adına hizmet veren ortak TSM tarafından yönetilebilir [18].



Şekil 3.5.2. Elektronik Cüzdan Çalışma Şeması [18]

3.5.1. Mifare - desfire

MIFARE Desfire (MF3ICD40) MIFARE Classic'e göre daha fazla donanım ve yazılım güvenlik özelliklerine sahip olup, SmartMX benzeri bir çekirdeğine dayalı şekilde 2002 yılında tanıtılmıştır. Basit bir dizin yapısı ve dosyaları sunan genel amaçlı Mifare Desfire

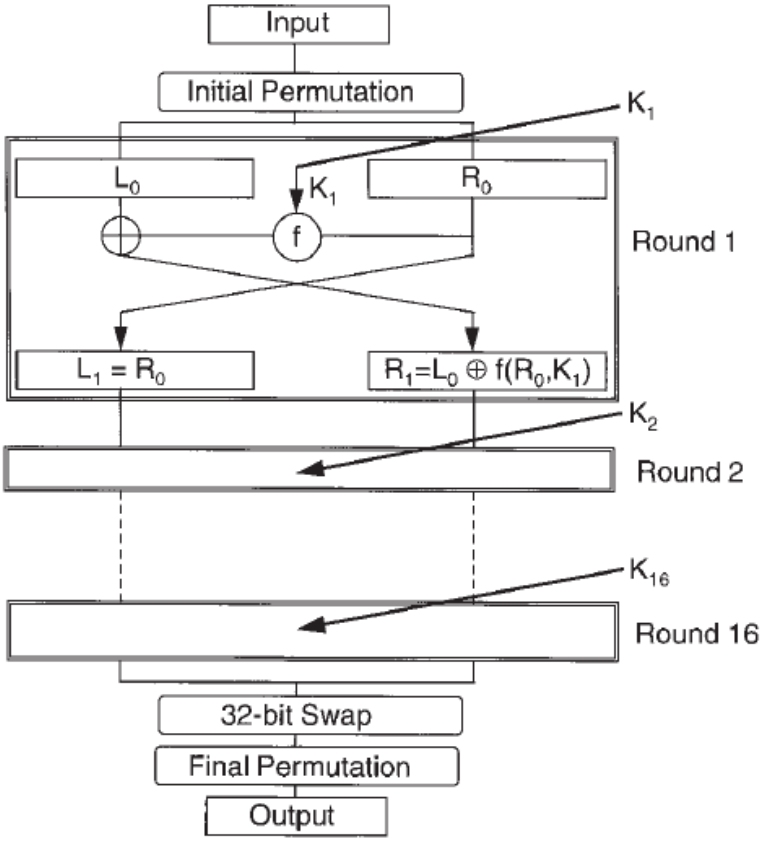
işletim sistemi ile önceden programlanmış olarak gelir. 4 tür halinde satılmaktadır. Bir tanesi sadece Triple-DESli ve 4 Kb depolamaya sahip, diğer üçü AESlidir (2, 4 veya 8 Kb). (AES: Advanced Encryption Standard).

AES varyantları CMAC gibi ek güvenlik özelliklerine sahiptir. MIFARE DESFire ISO / IEC 14443-4 ile uyumlu bir protokol kullanmaktadır. Kart çok hızlı işlemi mümkün kılan, 3DES/AES kripto hızlandırıcılı 8051 işlemcisine dayanmaktadır.

Kart ve kart okuyucu desfire terminal arasındaki maksimum okuma/yazma mesafesi 10 cmdir. Fakat gerçek mesafe okuyucu tarafından oluşturulan alan gücüne ve anten boyutuna bağlıdır.

3.5.1.1.Desfire kart uygulaması

NXP firmasının üretmiş olduğu Mifare Desfire EV1 kartlar, ISO 14443-4 uyumlu 4 KB hafıza büyüklüğüne sahip, yüksek güvenlikli akıllı kartlardır. 28 tane farklı uygulamaya destek verebilmesi, hızlı ve güvenli veri iletimi, esnek hafıza yapısı ve bağımız çalışabilmesi açısından otopark kullanımında ideal bir bilet uygulaması olarak görünmektedir. Tip 4 NFC Etiket ini kullanan Mifare Desfire kart, ISO14443-4, 7Byte UID, 2k or 4kByte, 3DES, encryption, MACing, Enciphering desteklemesi ve Java tabanlı olması ile uygulamaya yüksek güvenlik kazandırmaktadır. Şekil (3.5.1.1.1.)' de DES algoritması gösterilmiştir.

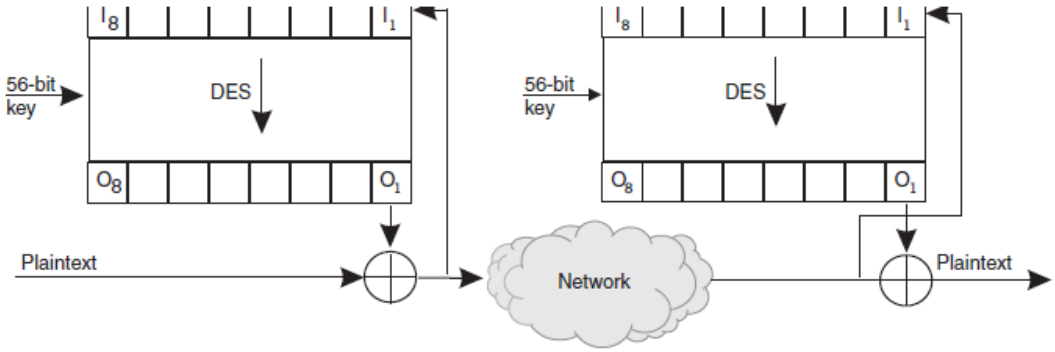


Şekil 3.5.1.1.1. Des Algoritması

Otoparklarda kullanılması düşünülen desfire kart uygulamasını NFC telefondaki SIM karta koymak mümkündür. SIM kart tabanlı yapılan NFC Mobil Bilet Projesinde desfire kart uygulaması kullanılmıştır. SP TSM ve MNO TSM tarafından nasıl yönetileceği, SIM kartın üzerinde nasıl yer alacağı ve haberleşme standartları Mifare4Mobile spesifikasyonlarına göre belirlenmektedir.

3.5.1.2.Blok şifre sistemi / algoritma

Desfire blok şifre yapısında N-bit açık metin bloğunu n-bit kapalı metin bloğuna taşır. Burada n, bloğun uzunluğudur. Klasik bir DES şifreleme metodu aşağıdaki (Şekil 3.5.1.2.1.)'de belirtilmiştir.



Şekil 3.5.1.2.1. DES Şifreleme Metodu

Bu algoritma (fonksiyon), k-bit vektörler anahtar uzayı 𝕂 dan seçilen gizli anahtar K ile parametrize edilir.

Burada genel varsayım; gizli anahtar rastgele seçilir.

P ve C kümelerinin her birinin eleman sayısı 2 ise

Toplamda P $\xrightarrow{yields}$C ye $C^p = 2^{n2^n}$ fonksiyonu vardır. Fakat 1-1 fonksiyon sayısı $2^n!'\, dir.$

Her bir gizli anahtar K ϵ 𝕂, bütün 1-1 fonksiyonların K=2^k tane arasından birini seçmek için kullanılır. Tablo (3.5.1.2.1.)' de DES simetrik ve Asimetrik anahtar tablosu gösterilmiştir.

Tablo 3.5.1.2.1. DES Simetrik Ve Asimetrik Anahtar Tablosu [18]

Açık Metin (P)		$X=P^3$	Şifreli Metin (C)	$Y=C^7$	Şifre Çözme İşleminden Sonra	
Sembol	Sayı		X (mod 33)		Y (mod 33)	Sembol
K	11	1331	11	19487171	11	K
R	18	5832	24	4586471424	18	R
I	9	729	3	2187	9	I
P	16	4096	4	16384	16	P
T	20	8000	14	105413504	20	T
O	15	3375	9	4782969	15	O

DES algoritması bir Block Cipher algoritmasıdır. Yani şifrelenecek metin bloklar halinde şifreleme işleminden geçirilir. Ayrıca DES algoritması simetrik şifreleme prensibine dayanmaktadır. Yani DES, veri bloklarını şifrelemek ve deşifrelemek için aynı anahtarları kullanmaktadır. DES 64 Bitlik düz metin blokları üzerinde işlem yapmaktadır. 64 bitlik veri blokları, 56 bitlik bir anahtarın kontrolünde şifrelenerek yine 64 bitlik şifrelenmiş metin bloklarına dönüştürülür. Deşifrelenirken de 64 bitlik şifrelenmiş veri blokları, 56 bitlik bir anahtarın kontrolünde deşifrelenerek yine 64 bitlik deşifrelenmiş metinlere(düz metne) dönüştürülür.

DES' de şifreleme ve deşifreleme için yer değiştirme, permütasyon gibi bir dizi işlem yürütülerek gerçeklenmektedir. Bu işlemlerin sırası şifreleme ve deşifreleme için birbirlerinin tam tersi şeklindedir. Şimdi DES algoritmasını basit olarak inceleyelim;

IP(Initial Permutation) şifreleme işleminde kullanılacak ilk permütasyondur.

Verilen bir düz metin(x) üzerine ilk permütasyon uygulanarak x0 elde edilir.

x0= IP(x)=L0R 0

L0= x"in ilk 32 biti

R0=x"in son 32 biti

Ardından 16 defa tekrarlanan bir fonksiyonla yeni değerler hesaplanır.

LiRi(1<=i<=16) aşağıdaki kurala göre hesaplanır:

Li=Ri-1

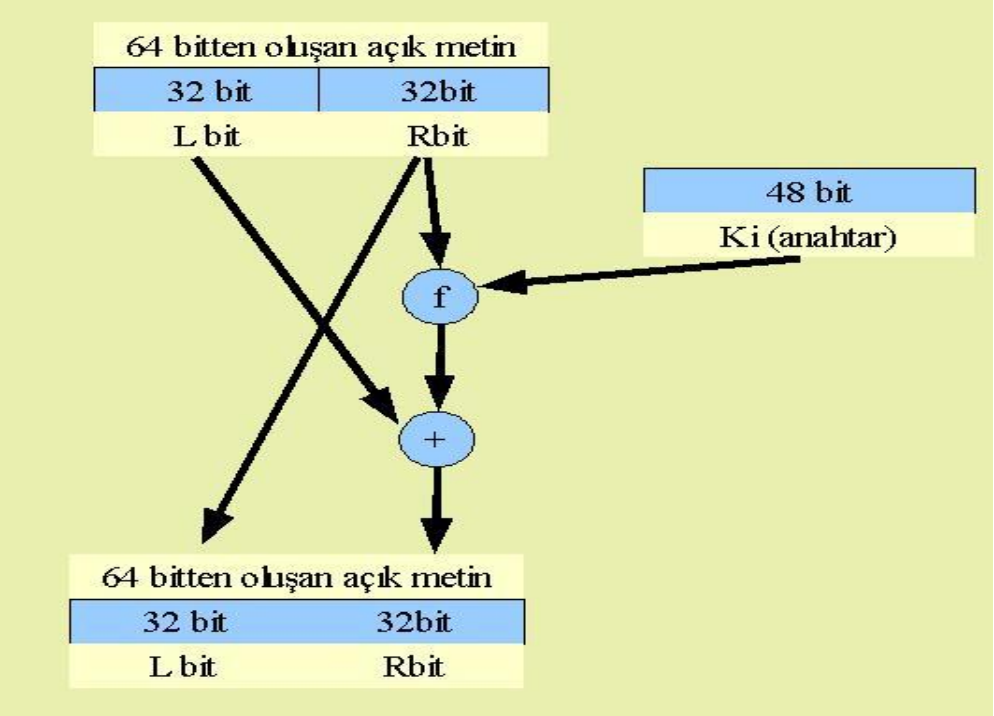
Ri=Li-1 f(Ri-1,Ki)

iki bit stringinin Exclusive-or işlemine tabi tutulacağını gösterir.

En son olarak da R16L16"ya IP -1 uygulanarak şifreli metin elde edilir.

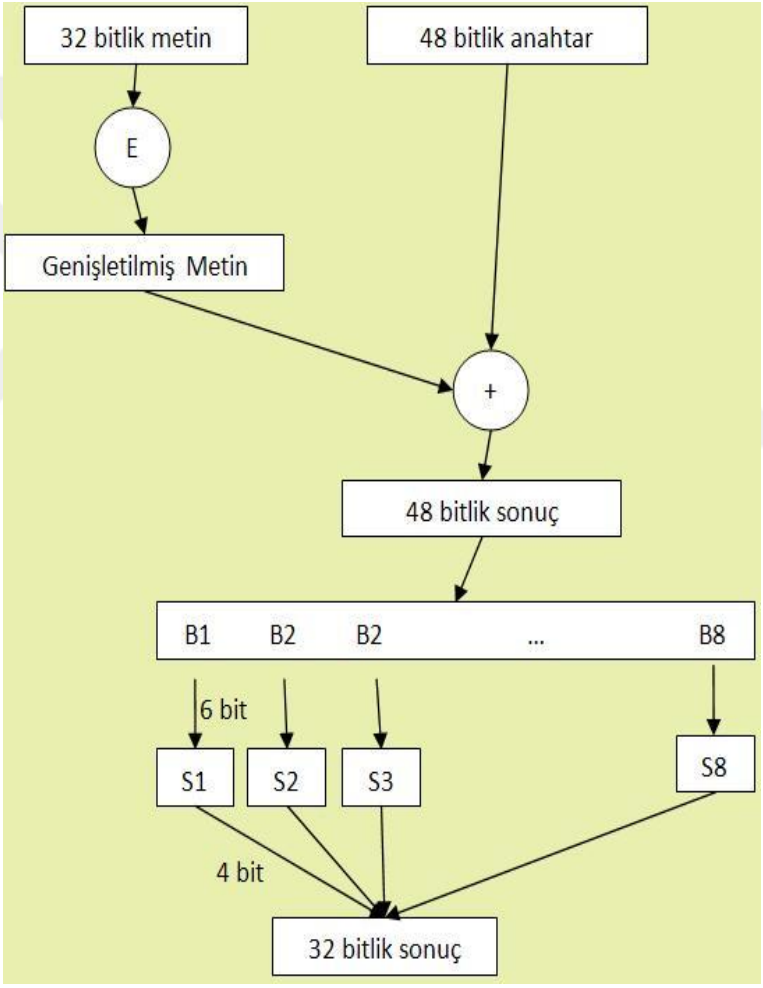
Şekil 3.5.1.2.2.'de görüldüğü gibi 64 bitten oluşan bir metnin öncelikle 2 parçaya ayrılması gerekir, soldaki ve sağdaki parça ayrı ayrı işlenmektedir. Bu işleme sağdaki 32 bitlik parçanın f fonksiyonuna anahtar ile birlikte girmesi ve parçaların yer değiştirmesi şeklinde yapılmaktadır. Aşağıdaki şekilde (+) işlemi yahut işlemidir (xor (exclusive or, özel veya))

Şekilde DES için yapılan bir geçiş çizilmiştir, DES şifrelemesinde bu işlem 16 defa tekrar edilmektedir.



Şekil 3.5.1.2.2. DES Açık Metin Yapısı

Şekil 3.5.1.2.3.'de gösterildiği gibi S1, ... S8 ile gösterilen kısma SBox denir. Bu kısımda 48 bitlik bir bitstringinden 32 bitlik bir bitstringi oluşturulur. DES"te 8 tane SBox vardır. SBoxlar 6 bitlik bir bitstringten 4 bitlik bitstringler elde ederler. Şekil 3.5.1.2.2.'de bir DES geçişi (pass) içindeki f fonksiyonunun nasıl çalıştığı gösterilmiştir. Bu fonksiyon bir 32bit'lik parçayı alarak 48 bit'lik anahtar ile 32 bit'lik sonuç üretmektedir. Bu üretme işlemi sırasında en kritik işlem yukarıdaki şekilde E olarak görüntülenmiş expansion işlemidir. Bu işlem basitçe aynı bit için birden fazla sonuç üretilebilmesini ön görür. Aşağıda detaylıca anlatılacaktır ancak yukarıdaki resmin detaylarına devam edilecek olursa genişletilmiş (expanded) bili, anahtar ile xor işlemine tabî tutulur. Sonuçta 48 bitlik olarak üretilen metin 8 bloğa bölünür. Her blok 6 bitlik bir parçadan oluşmaktadır. Her 6 bitlik parça bu sefer expansion işleminin tersi olarak küçültülmekte ve 4 bit'e indirilmektedir. Sonuçta 4 bitlik 8 blok yani toplam 32 bitlik veri üretilmiştir.



Şekil 3.5.1.2.3. DES Şifreleme Geçişi

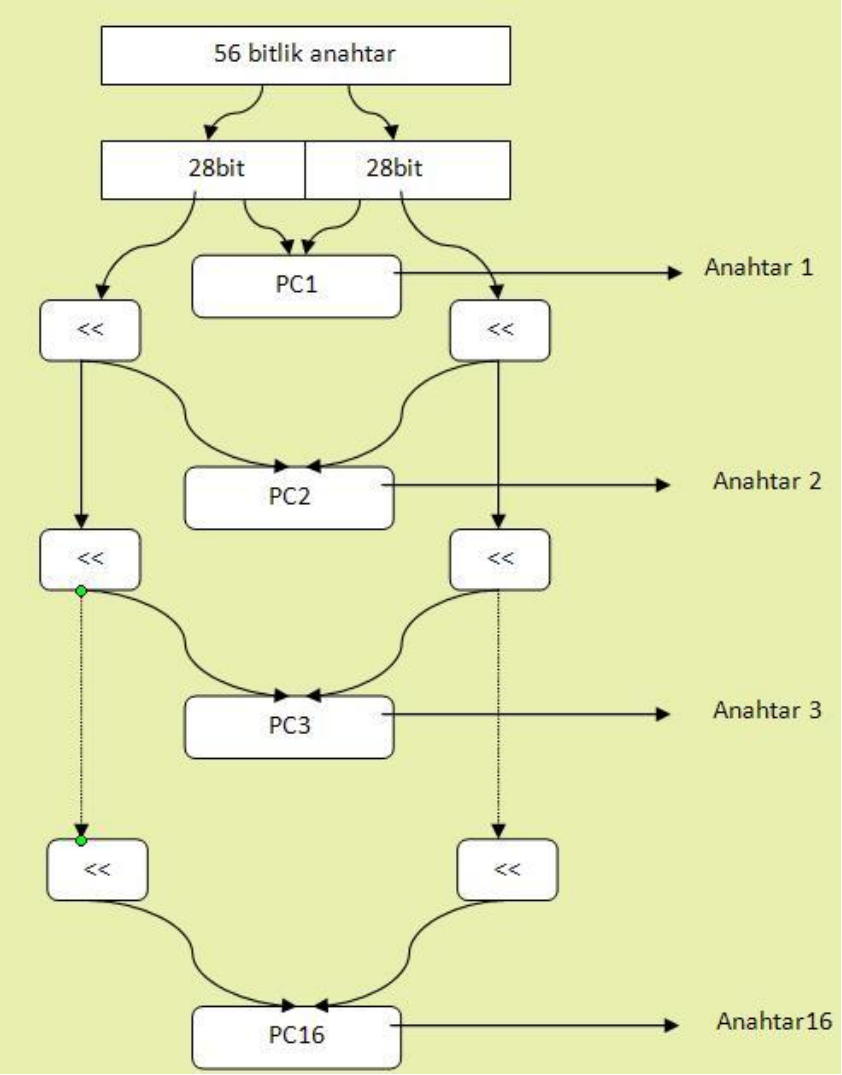
Tablo 3.5.1.2.2.'de mantık basitçe bir sayının birden fazla pozisyonda bulunmasıdır. Bu durumda örneğin 1 sayısı için hem 2. hem de 4. konumda karşılık bulunmaktadır. DES ile ilgili diğer bir ayrıntı da anahtar üretilmesidir. Dikkat edilirse DES'in 64 bitlik bir

anahtar ile çalıştığı ve 8 bitlik parity kontrolü çıkarılacak olursa bu anahtarın 56 bitlik olduğu yukarıda anlatılmıştı. Ancak f fonksiyonuna giren her geçişteki anahtar boyutu yukarıda 48 bit olarak verilmiştir. Dolayısıyla aslında her geçiş (pass) için farklı bir anahtar üretilmektedir. Bu anahtarlar 56 bitlik esas anahtardan üretilen anahtarlardır.

32	1	3	1	2	4	3	6
4	5	5	7	28	30	7	9
9	7	10	8	22	11	11	15
29	12	14	17	15	16	12	18
13	23	19	21	15	17	14	18
31	20	21	20	24	25	26	27

Tablo 3.5.1.2.2. Expansion Tablosu

Şekil 3.5.1.2.4.'de gösterildiği gibi 56 bitlik giriş anahtarından her geçiş için gereken anahtarların üretilmesi gösterilmiştir. Bu işlem 16 adımda yapılmaktadır ve her adımda o adım için üretilmiş olan tablo kullanılmaktadır. Her adım öncelikle 2 adet 28 bitlik parçaya bölünmüştür. Tablolara PC1′den PC16′ya kadar isimler verilmiştir. Ayrıca her tablo girişinden önce bir kaydırma işlemi kullanılarak üretilen anahtar değiştirilmektedir. Buna göre örneğin 10. adımda orijinal verinin her iki parçası da 10 bit kaydırılmış olacaktır. DES ile şifrelenmiş bir metni açmak için aynı algoritmaya şifreli metni (cipher text) aynı anahtar ile vermek yeterlidir.



Şekil 3.5.1.2.4. DES Cipher Text Yapısı

DES için zaman içinde bilgisayarların işlem hızının gelişmesi ile saldırılar kolay hale gelmiştir. DES'in daha zor saldırılır hale gelmesi için 128 bit anahtar uzunluğu kullanan üçlü DES uygulaması geliştirilmiştir.

3.5.2. Mifare – desfire EV1

Daha önceden DESFire8 olarak isimlendirilen MIFARE Desfire EV1 MIFARE DESFire kartının gelişmiş versiyonu olup genel olarak geriye doğru uyumludur. 2 KB, 4 KB ve 8 KB NV-Bellek ile kullanılabilir.

Diğer Özellikler Şunlardır:

- Rastgele ID desteği
- 128-bit AES desteği
- Donanım ve işletim sistemi EAL 4+ düzeyinde Common Criteria onaylıdır.

MIFARE DESFire EV1 kamuya Kasım 2006 yılında ilan edildi.

Mifare Desfire EV1 temassız akıllı kart, birkaç dönüşlü bobine bağlı ve standard ISO akıllı kartına gömülü olup NXP MF3 IC D41 tabanlıdır.

Aktarım protokolü ISO 14443-4 ile uyumludur. Desfire ISO7816-4 uyumlu APDU mesaj yapısını da destekler. Bu bir temassız data ve enerji iletimidir. Pile ihtiyaç bulunmamaktadır. Desfire'ın bir üst versiyonu olan Mifare Desfire EV1 daha yüksek bir güvenlik seviyesine sahiptir. Mifare Desfire EV1 veri iletimini şifrelemek için 3DES donanım şifreleme motorunu kullanır. Kart, 28 farklı uygulama ve uygulama başına 32 dosya tutabilir. Her dosyanın boyutu Mifare Desfire EV1 gerçekten esnek ve uygun bir ürün olacak şekilde, oluşturulma anında tanımlanır. Kart sahipleri temassız uygulama tecrübesini rahatça yaşarken, aynı zamanda aynı cihazı otomatlarda, erişim kontrol sistemlerinde ve benzeri uygulamalarda kullanma imkanına sahiptirler.

- Model : MIFARE DESFire™ Ev1
- Frekans : 13.56MHz
- Protokol : ISO14443A
- EEPROM Boyutu : 4096 Byte
- Materyal : PVC
- Çalışma Isı Aralığı : -20 - +50
- Boyut : 85.6 × 54 × 0.86 (mm)

Gelişen teknoloji ile birlikte mifare desfire yapısıda hızla gelişmektedir. İlk olarak Amerikan Savunma Sanayisi'nde kullanılan ve EV2 yapısı ortaya çıkmıştır. EV2 henüz kullanımı EV1 kadar yaygın olmasa da dünya genelinde kullanılmaya başlanmıştır.

3.5.2.1 Çalışma şekli

Mifare Desfire EV1 temassız akıllı kart, birkaç dönüşlü bobine bağlı ve standard ISO akıllı kartına gömülü olup NXP MF3 IC D41 tabanlıdır. Aktarım protokolü ISO 14443-4 ile uyumludur [19]. Desfire ISO7816-4 uyumlu APDU mesaj yapısını da destekler. Bu bir temassız data ve enerji iletimidir. Pile ihtiyaç bulunmamaktadır.

Mifare, haberleşme gibi bilgi gönderim ve alımını sağlayan anten ve bilgi depolamasını sağlayan, antene entegre çip (IC internal circut) olmak üzere iki parçadan oluşmaktadır.

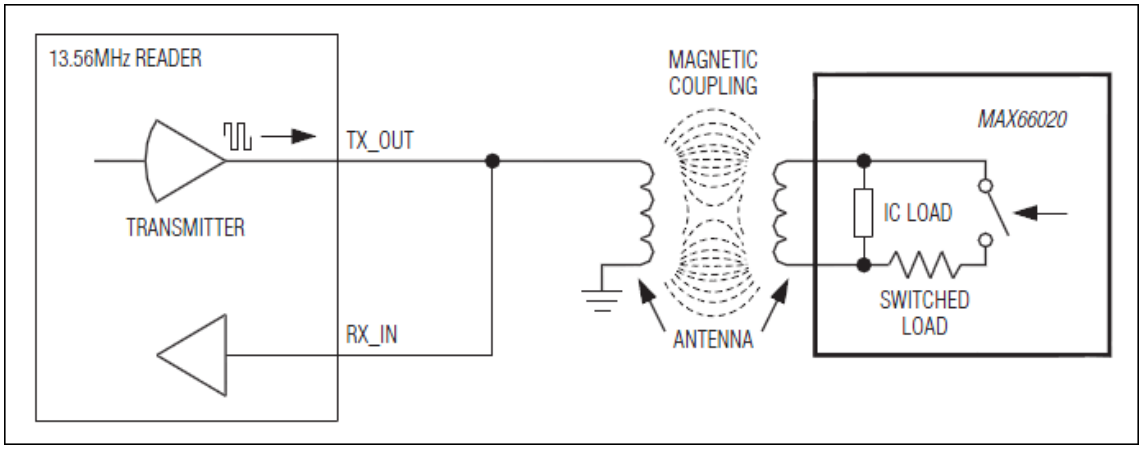
IC; Segmentlere bölünmüş ve güvenlik mekanizmasınca korumalı bir hafızaya sahip olup Access kontrol sistemlerinde kullanılmaktadır.

Mifare kartlar esnek, yüksek güvenliğe haiz, sitilist temassız plastik kartlardır. Bu kartların özelliği, mifare okuyuculara sinyal gönderen bir çipin kartın içine gömülü olmasıdır.

Mifare kartların bir çok kişi tarafından özellikle bilet ve düşük miktarlardaki finansal işlemlerde tercih etmesi bu tip kartların popüleritesini arttırmıştır.

Mifare kartlar ISO/IEC 14443 norm ve standartları doğrultusunda 13.56 Mhz iletişim frekansına sahiptir. Diğer proximity kartlar gibi mifare kartta yaklaşık 10 cm lik okuyucu mesafesi sınırları içerisinde aktivasyon sağlamaktadır. Kart tarafından gönderilen kod okuyucu tarafından tanımlanır. Kart ve okuyucu arasında kurulan iletişim şifreli olması sebebiyle yüksek güvenlik özelliğine sahiptir.

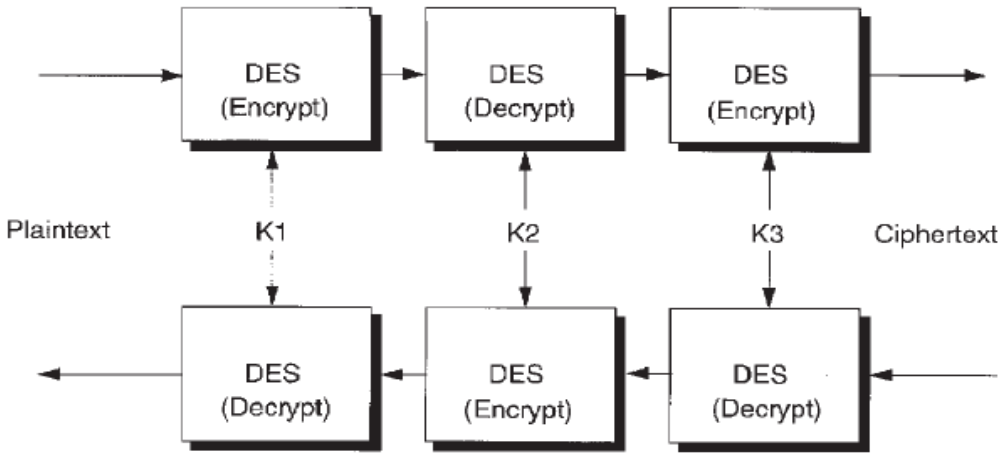
MIFARE DESFire EV1 hem hava arayüzü hem de şifreleme yöntemleri için açık küresel standartlara dayalıdır. ISO / IEC 14443A nın tüm 4 düzeyi ile uyumludur ve opsiyonel ISO / IEC 7816-4 komutlarını kullanır. Şekil (3.5.2.1.1.)' de ISO / IEC 14443A yapısına uygun bir RFID iletişim şeması gösterilmiştir.



Şekil 3.5.2.1.1. ISO / IEC 14443A Yapısına Uygun Bir RFID İletişim Şeması

Bir on-chip yedekleme yönetim sistemi ve karşılıklı üç geçişli kimlik doğrulama ile birlikte, bir MIFARE DESFire EV1 kartı 28 farklı uygulama ve uygulama başına 32 dosyaya kadar tutabilir. Her dosyanın boyutu Mifare Desfire EV1 gerçekten esnek ve uygun bir ürün olacak şekilde, oluşturulma anında tanımlanır.

Buna ek olarak, işlem odaklı veri bütünlüğünü garanti altına alan, her dosya tipleri için bir anti-tear mekanizması mevcuttur. Mifare Desfire EV1 ile 848 Kbit/s ile veri transfer hızına erişilebilir. Bu cihazın temel özellikleri DESFire EV1 adıyla gösterilir: DES, veri iletimini şifrelemek için 3DES donanımlı şifreleme motorunu kullanarak yüksek düzeyli güvenliği gösterir. Şekil (3.5.2.1.2.)' de 3DES donanımlı şifreleme algoritması gösterilmiştir.



Şekil 3.5.2.1.2. 3DES Donanımlı Şifreleme Algoritması

FIRE ise onun temassız proximity işlem piyasasında hızlı, yenilikçi, güvenilir ve güvenli bir IC olarak üstün konumunu gösterir. Bu yüzden, MIFARE DESFire EV1 son kullanıcılar için birçok fayda getirir. Kart sahipleri temassız uygulama tecrübesini rahatça yaşarken, aynı zamanda aynı cihazı otomatlarda, erişim kontrol sistemlerinde ve benzeri uygulamalarda kullanma imkanına sahiptirler. Diğer bir deyişle, MIFARE DESFire EV1 silikon çözümü güvenlik ve güvenilirlik ile birlikte geliştirilmiş tüketici dostu sistem tasarımı sunmaktadır.

3.5.2.2 Mifare kart tipleri

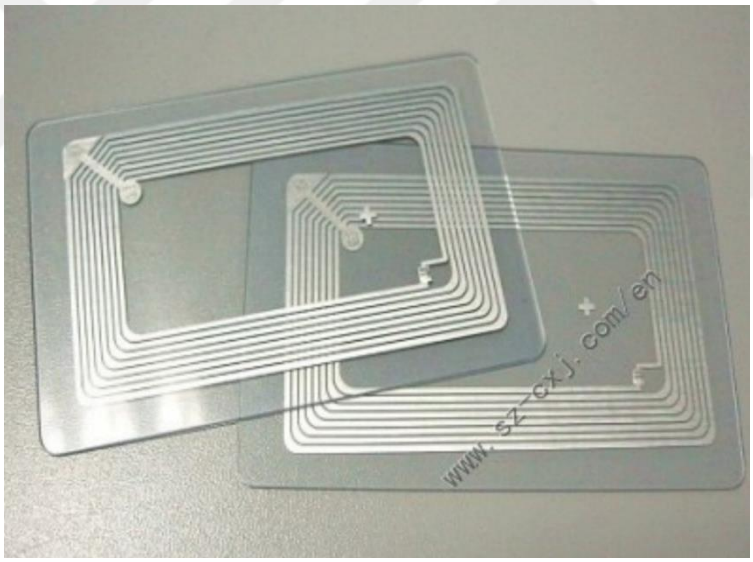
Mifare Classic – 1024 bytes bilgi depolama kapasitesine sahiptir (Mifare 1K). NXP NFC controller chiplere sahip Samsung smart mobil telefon gibi diğer cihazlar arasında da kullanılabilirler. Şekil (3.5.2.2.1)' de Klasik Mifare kart gösterilmiştir.

Şekil 3.5.2.2.1. Klasik Mifare Kart

Mifare Ultralight ve Mifare Ultralight EV1 – Yalnızca 512 byte hafızaya sahiptir. Güvenlik özelliği yoktur, genellikle tek kullanımlık bilet olarak kullanılmaktadır. Şekil (3.5.2.2.2.)' de Mifare Ultralight kart gösterilmiştir.

Şekil 3.5.2.2.2. Mifare Ultralight Kart

Mifare Ultralight C – Düşük maliyetlidir, tek kullanımlık bilet için uygundur. Belli bir dereceye kadar güvenlik özelliklerine sahiptir. Şekil (3.5.2.2.3.)' de Mifare Ultralight C kart gösterilmiştir.



Şekil 3.5.2.2.3. Mifare Ultralight C Kart

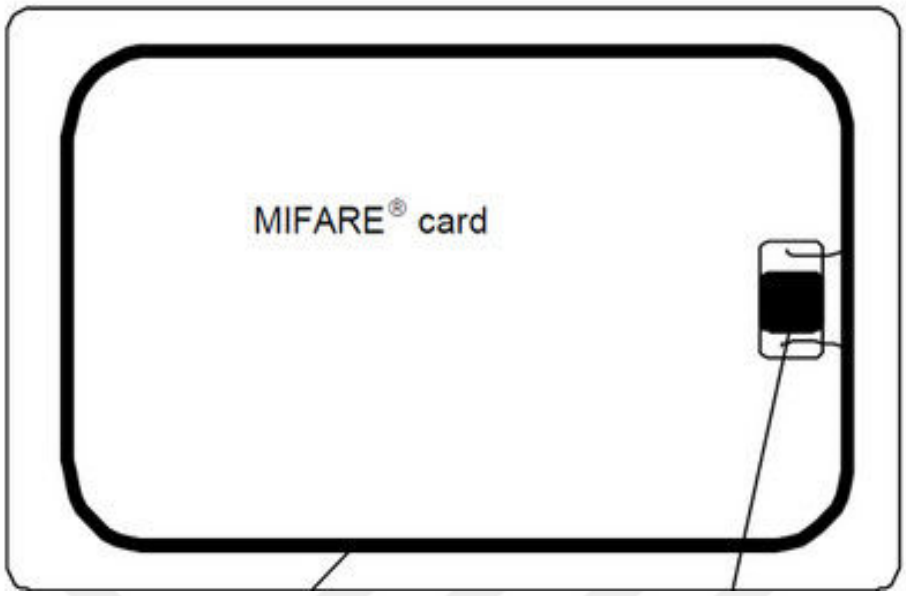
Mifare DESFire – Mifare Classic den daha fazla güvenlik özelliklerine sahiptir. Hızlı işlem kabiliyeti için şifre hızlandırıcı özelliği vardır. Şekil (3.5.2.2.4.)' de Mifare DESFire kart gösterilmiştir.

Şekil 3.5.2.2.4. Mifare DESFire Kart

Mifare DESFire EV1 – 2006 yılında piyasaya sürülmüştür. Karışık ID yi destekleyen 128 bit şifreleme standartlarına sahiptir. Şekil (3.5.2.2.5.)'de Mifare DESFire EV1 kart gösterilmiştir.

Şekil 3.5.2.2.5. Mifare DESFire EV1 Kart

Mifare Plus – Mifare classic in değişenidir. Daha fazla güvenlik özelliklerine sahiptir ve kolayca Mifare plus x'e yükseltilebilir. Şekil (3.5.2.2.6)'da Mifare Plus kart gösterilmiştir.



Şekil 3.5.2.2.6. Mifare Plus Kart

3.5.2.3 Temel özellikleri ve faydaları

- MIFARE temassız akıllı kart işlemleri için önde gelen endüstri standardıdır.
- 10 milyondan fazla mifare okuyucu çekirdek bileşenleri ile dünya çapında geniş bir kullanıcı tabanına satılmıştır ve 1 milyardan fazla da temassız ve ikili arayüz IC satılmıştır.
- ISO 14443A ile tam uyumlu.
- Geleceğe dönük evrim yolu ve yol haritası – Standart arayüzü bugünün altyapısının kolaylıkla gelecekteki kart ICleri için yükseltilmesini temin eder.
- Tutarlı ürün portföyü ve çoklu değer zincirinin her düzeyinde kaynağa sahip olma.
- Hızlı programlama ile 2/4/8-Kbyte EEPROM.
- Güvenli, yüksek hızda komut seti.
- ISO / IEC 14443-4 uyarınca yüksek veri oranları: 848 Kbit /s'ye kadar.

- Esnek dosya yapısı.
- Donanımda açık DES/2K3DES/3K3DES/AES kripto algoritması seçeneği.
- Gizlilik koruması.
- Benzersiz 7 baytlık seri numarası (ISO kademeli düzey 2).
- Veri bütünlüğü: CRC ve fiziksel katmanda bit sayımı.

3.5.2.4 Başlıca uygulama alanları

- Toplu taşımada elektronik bilet sistemi
- Yol geçiş ödeme sistemleri.
- Havayolu biletleri
- Erişim (Access) kontrol
- Çoklu uygulamalar
- Sadakat programları
- Sosyal hizmetleri içeren e-devlet uygulamaları
- Kapalı döngüsel mikro ödeme
- Kartlı ödeme sistemleri
- E-kimlik
- Otopark ödeme sistemlerinde

Mifare Desfire EV1 bir temassız kart üzerinde birden fazla uygulamayı birleştirmek ve desteklemek isteyen çözüm geliştiriciler ve sağlayıcılar için idealdir.

Hızlı ve güvenli veri iletimi, esnek bellek organizasyonu ve mevcut altyapı ile çalışabilirlik gereksinimleri ile tamamen uyumludur.

Mifare Desfire EV1 hava arabirimleri ve şifreleme yöntemlerinin her ikisi için açık küresel standartları temel almıştır. ISO / IEC 14443 A'nın tüm dört düzeyiyle uyumludur ve isteğe bağlı olarak ISO / IEC 7816-4 komutlarını kullanır.

On-chip yedekleme yönetim sistemi ve üç geçişli kimlik doğrulama özelliğiyle Mifare Desfire EV1 kartı 28 farklı uygulamayı ve kişi başına 32 dosyayı tutabilir. Her dosyanın boyutu ve erişim koşulları Mifare Desfire EV1 gerçekten esnek ve uygun bir ürün olacak şekilde, oluşturulma anında tanımlanır.

Buna ek olarak, işlem odaklı veri bütünlüğünü garanti altına alan, her dosya tipleri için bir anti-tear mekanizması mevcuttur. Mifare Desfire EV1 ile 848 Kbit/s ile veri transfer hızına erişilebilir. Çipin ana özellikleri Mifare Desfire'ın ilk evrimi olan Desfire EV1 isminde belirtilmiştir: DES yüksek güvenlik seviyesinin taahhütünü belirtir.

Mifare Desfire EV1 iletim veri güvenliğini sağlamak için bir DES, 2K3DES, 3K3DES ve AES donanım şifreleme motoru kullanır.

Mifare Desfire EV1 son kullanıcılar için birçok fayda getirir. Kart sahipleri temassız uygulama tecrübesini rahatça yaşarken, aynı zamanda aynı cihazı otomatlarda, erişim kontrol sistemlerinde ve benzeri uygulamalarda kullanma imkanına sahiptirler. Diğer bir deyişle Mifare Desfire EV1 silikon çözümü, güvenli ve güvenilir tüketici dostu sistem tasarımı sunar. 70 pF seçeneği küçük anten form faktörlerinin okuma mesafesi iyileştirmesini sağlar.

Mifare Desfire EV1 mükemmel hız dengesi, performans ve maliyet verimliliği sunar. Onun açık konsepti Yakın Alan İletişimine (NFC) dayalı akıllı kağıt bilet, anahtar fobları, mobil bilet gibi diğer medyanın gelecekteki sorunsuz entegrasyonunu sağlar. Ayrıca mevcut mifare okuyucu donanım platformu ile tam uyumludur.

MIFARE DESFire EV1 taşımacılıkta, eDevlet veya kimlik uygulamalarda çoklu uygulamalı akıllı kart kullanmak isteyen servis sağlayıcılar için idealdir.

Hızlı ve son derece güvenli veri iletimi, esnek hafıza organizasyonu ve mevcut altyapısıyla birlikte çalışabilirlik gereksinimleri için tam uyumludur.

4. İSPARK VE NFC ÖZELLİKLİ İSTANBUL KART ENTEGRASYONU

İSPARK, mevcutta bulunan tüm otopark bilet verme makinelerini değiştirerek, İstanbul Kart yapısına uygun Mifare Desfire uyumlu kart okuyuculara sahip yeni nesil bilet verme makineleri (Parkmatik) ile değiştirmiştir. Toplamda 500 ün üzerinde otoparkda revizyona giden İSPARK tüm otoparklarında bu parkmatikleri kullanmıştır. Aynı zamanda merkezi yazılımı sıfırdan itibaren değiştirerek NFC, debit kartlar, finans teknolojileri ile ödeme sistemleri, internet ile ödeme, mobil ödeme ve akıllı kart destekli yapı tasarlamıştır. Bunlardan en güveilir olan Mifare Desfire V1yapısına sahip olan akıllı karttır.

4.1. İstanbul Kart Nedir?

İstanbul kart Mifare Desfire yapısına sahip bir akıllı karttır. İlk olarak seyahat amaçlı çıkarılan bu kart, günümüzde B2B ve B2C deki mobil ödeme sistemlerinin gelişimi, NFC teknolojilerinin etkin kullanımı sonucu rolünü arttırmıştır. Şekil (4.1.1)' de İstanbul Kart gösterilmiştir.

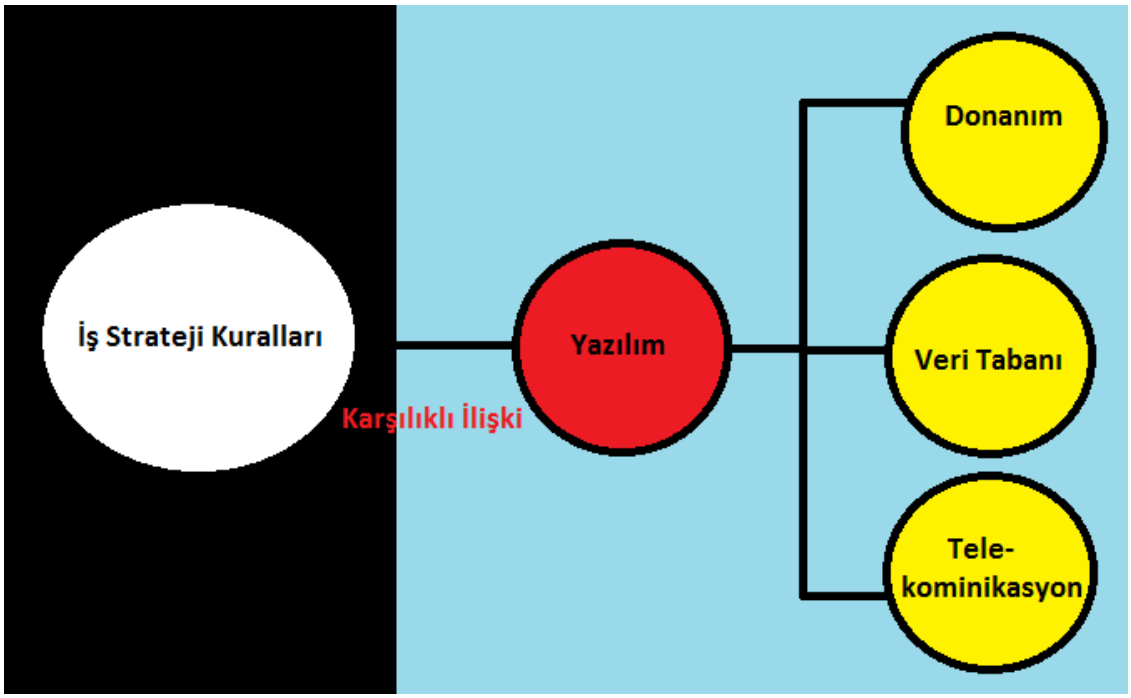
Şekil 4.1.1. İstanbul Kart

4.2. Otopark Sistemlerinin Sayısal Firmaya Dönüşümü ve ERP Yapısının Oluşturulması

Birikim ve belediye enformasyon tabanlı şehir ekonomileri, akıllı şehircilik kapsamında vatandaşa sunulan ve sunulması gereken yeni ürün ve hizmetler, üretken ve stratejik bir mal varlığı olarak bilgi birikimi, zaman üzerine kurulu şehir bazında kültürel teknolojik rekabet, daha kısa ürün döngü ömrü, kaotik ortam, çalışanların kısıtlı bilgi birikim havuzu, klasik otopark sistemlerinin sayısal bir firmaya dönüşmesinin başlıca etmenleridir. Bunlardan en önemlisi İSPARK'ın akıllı şehircilik kapsamında büyük rol üstlenmiş olması veya üstlenecek olmasıdır.

Peki İSPARK'ın sayısal bir firmaya dönüşebilmesi ve İstanbul Kart uygulaması için nereden başlanması gerekti?

Tabiki donanımsal olarak alt yapıyı değiştirmek, sonrasında bu donanımları besleyecek günümüzde ki kurumsal sistemlerin diline uygun bir yazılımla beslemek ve bu sistemleri etkin kullanacak nitelikli personel yetiştirmekti. Şekil (4.2.1.)' de organizasyonlar ve enformasyon sistemleri arasındaki karşılıklı bağımlılık gösterilmiştir.



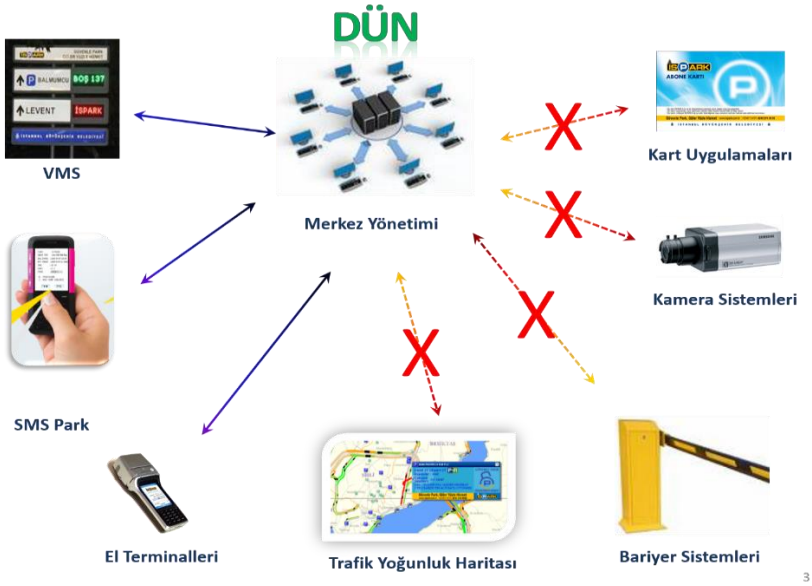
Şekil 4.2.1. Organizasyonlar ve Enformasyon Sistemleri Arasındaki Karşılıklı Bağımlılık

4.3. Otopark Sistemlerinin Değişim Öncesi Sistemsel Yapısı

Aslında herhangi bir kurumsal proje için İSPARK'ın sistemsel yapısı oldukça uygunsuzdu. Veriler dağınık, birden fazla veri tabanın da tutuluyordu. Bir birimin veya işkolunun diğer paralel çalıştığı işkolu veya birimle sistemsel bağı yoktu. Donanımları günü kurtarmaya yeten, kombinasyon olarak birbiriyle çokta uyuşmayan ürünlerdi.

İSPARK birçok lokasyonun dan anlık olarak veri alamıyordu. Buda İSPARK'ın kurumsal mimarisinin olmadığının en büyük kanıtıydı. Kamera sistemleri, bariyer sistemleri, el terminali sistemleri gibi başlıca iş kollarının veri tabanları dağınık ve oldukça karışıktı. Saha da elde edilen veriler local olarak saklanıyor, gerektiğinde SQL server lar ile alınabiliyordu. Bu sistemde bir yöneticiye detaylı bir rapor bile sunmak imkânsızdı.

Enformasyon sistemleri yalnızca teknolojiden ibaret değildir. İşletmeler, değer yaratmak ve karlılığı arttırmak için BS'ne yatırım yaparlar. İSPARK gibi kamu iştiraki firmalar ise kaliteli hizmet ve akıllı Enformasyon sistemlerine yatırım yaparlar. Fakat her iki kuruluş içinde bilgi teknolojileri iş ortamından kaynaklanan zorluklara karşı geliştirilmiş örgütsel ve yönetimsel bir çözümdür. İSPARK'da bu çözüm için başta İstanbul kart uygulamasını hayat sokması için BT çözümlerini tercih etmiştir. Şekil (4.3.1.)' de İspark otopark sistemlerinin değişim öncesi sistemsel yapısı gösterilmiştir.



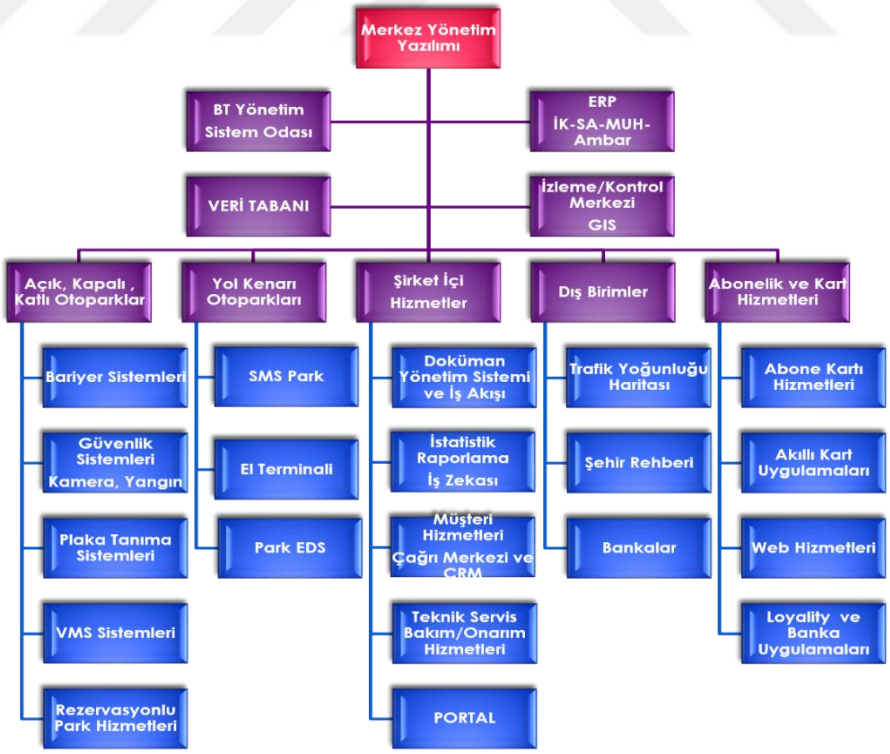
Şekil 4.3.1. Otopark Sistemleri İSPARK Değişim Öncesi Sistemsel Yapısı

4.4. Otopark Sistemlerinin Yeni ERP Yapısı ve Kurumsal Entegrasyon Sistemlerine Uyum Stratejisi

İlk zamanlarda geleneksel kurum örneği sergileyen İSPARK mevcut yapısını tamamen değiştirerek günümüze uygun modern bir hale getirmiştir.

Öncelikle sistem tarafındaki donanımları IBM ve CİSCO ürünleri ile değiştiren İSPARK, firewallda sürüm yükseltime gitmiş, birimleri ve iş kollarını yeniden tanımlayarak iş süreçlerini belirlemiştir. Her bir iş süreçlerine ileride kurulacak bir çok kurumsal sistemlere frekans değerleri atanacak şekilde tasarlanmıştır.

Dağınık halde bulunan veri tabanını implementasyon işleminden sonra tek bir veri tabanı haline getirerek BigData ve veri madenciliği gibi süreçlerin önünü açmıştır. İstanbul Kart ve diğer uygulamalar için düşünülen BI ve CRM gibi iş kollarının altını beslemiştir. Tüm bu değişikleri Belbim ile birlikte yürüttüğü kurumsal ERP yazılımı ile desteklemiştir. Şekil (4.4.1.) de İspark' ın yeni ERP yapısı gösterilmiştir.



Şekil 4.4.1. İSPARK yeni ERP Yapısı

4.5. İstanbul Kart Entegrasyonu İçin Altyapı Ve Donanım Değişiklikleri

Bir otopark sisteminin akıllı şehircilik kavramına katkı sağlayabilmesi ve kendi içinde veri madenciliği yaparak eksik ve negatif süreçlerini geliştirmesi için kullandığı donanımları akıllı şehir yapısına uygun olarak güncellemelidir. Örnek verdiğimiz İSPARK bu bağlamdaki değişimlerini alt başlıklar halinde inceleyelim.

4.5.1. Merkezi sistemlerde yapılan değişiklikler

İSPARK merkezde kullandığı eski sunucuları yeni nesil sunucular ile değiştirdi. Tüm donanımlarda ve ana çatı sunucularda Cisco ürünlerini tercih etti. Kullanılan Firewall güvenlik sistemini ABD'de top 5 de olan bir Firewall ile değiştirdi. Yeni nesil sanal sunucu serverları kuruldu. Önem derecesine göre bazı sistemleri bu sanal sunuculara taşındı. Böylece hem güvenlik anlamında hem de bakım maliyeti anlamında önemli ölçüde ilerleme sağladı.

Donanım değişikliklerinden sonra İSPARK bu donanımları çalıştıracak bir yazılıma ihtiyaç duydu. Staratejik planlamadan sonra ileride kullanılacak olan her türlü teknoloji düşünülerek yeni bir kurumsal yazılım tasarlandı. Bu yazılımın içinde NFC'li ödeme sistemleri de yer almaktadır.

4.5.2. Saha genelinde yapılan donanımsal değişikler

İSPARK, mevcutta bulunan tüm otopark bilet verme makinelerini değiştirerek, İstanbul Kart yapısına uygun Mifare Desfire uyumlu kart okuyuculara sahip yeni nesil bilet verme makineleri (Parkmatik) ile değiştirmiştir. Toplamda 500 ün üzerinde otoparkta revizyona giden İSPARK tüm otoparklarında bu parkmatikleri kullanmıştır.

5. OTOPARK SİSTEMLERİ VE İSTANBUL KART UYGULAMASI

İSPARK gerekli alt yapı, donanım ve yazılımsal değişikleri yaptıktan sonra İstanbul genelinde ulaşım başta olmak üzere birçok alanda kullanılan İstanbul akıllı kart uygulamasını bariyerli ve bariyersiz otoparklar bazında iki şekilde tasarlamıştır.

5.1. Sistem Tasarımı ve İşleyiş

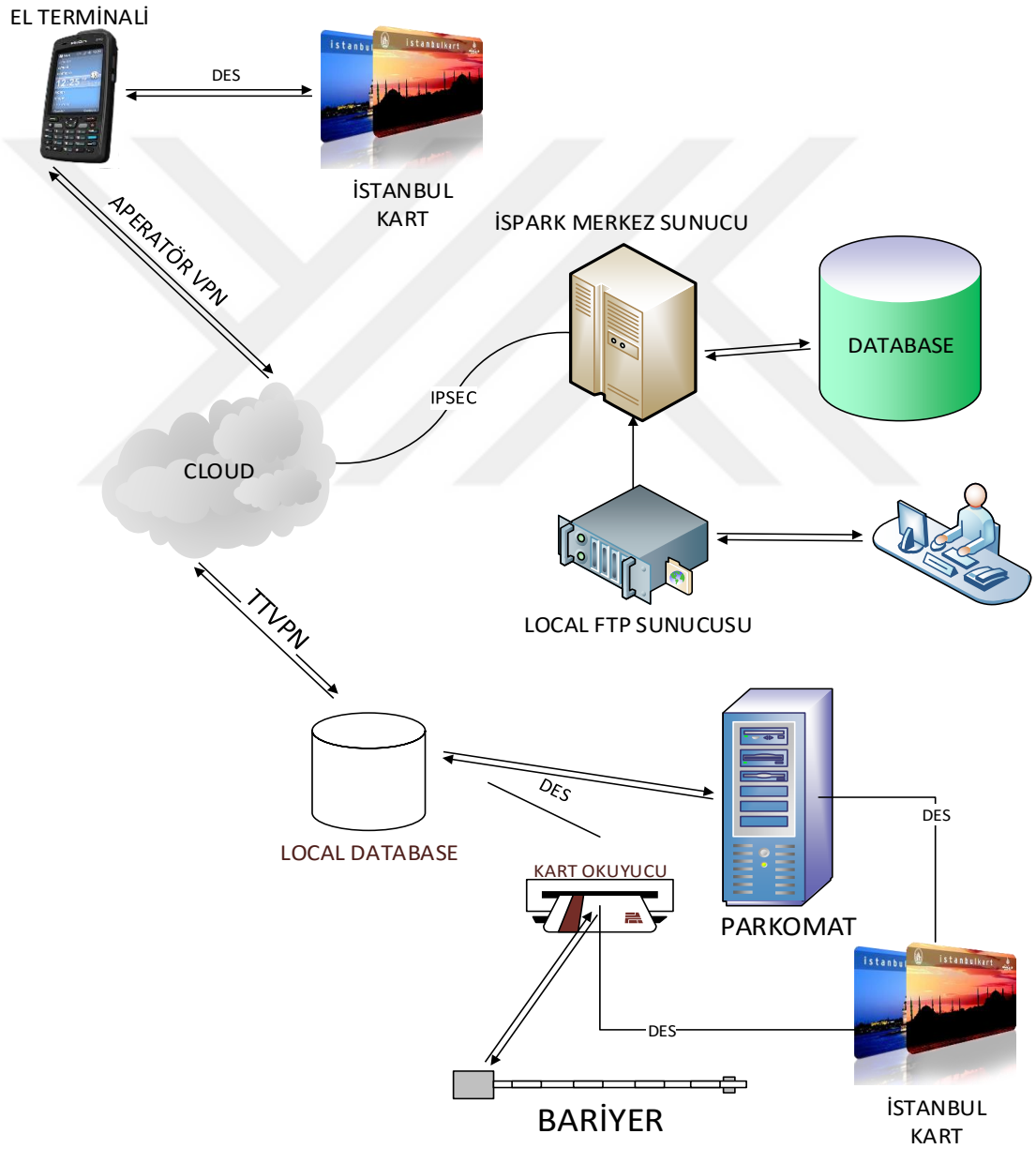
İSPARK donanımsal olarak bütün sistemlerini HyperConverged sistemler ile değiştirdi. HyperConverged, sanal platform için geliştirilmiş bir altyapıdır. Hypervisor altında birbirinden bağımsız tüm BT bileşenlerini başarılı bir şekilde birleştiren ve yöneten bir mimaridir. HyperConverged, BT işlemlerini daha verimli hale getirerek altyapı kullanımını büyük ölçüde kolaylaştırır. Sanal platform kullanımını hızlandırır, kaynak kullanımını etkili bir şekilde yönetmeyi sağlar ve en önemlisi HyperConverged, maliyetleri büyük ölçüde azaltır.

Yazılımlar ve birleştirici uygulamalar bu sistemlere kurulmuştur. Sistemler genel merkezde tutulmaktadır. Bulut imkanı sunabilen bir yapıya sahiptir. Bariyerli ve bariyersiz tüm otoparklar merkezle bağlantılıdır ve düzenli olarak veri alışverişinde bulunurlar. Bariyerli otoparklar TTVPN üzerinden merkezle haberleşir. Burada kullanılan protokol IPSEC dir.

Bariyersiz; yani el terminali kullanılan otoparklar ise mobil operatörler üzerinden oluşturulan APN kanalları üzerinden IPSEC-VPN protokolü ile merkezle bağlantı kurar. Böylece yapılan her işlem ve hareket merkezi olarak takip edilebilmektedir.

Şifrelemeler local olarak yapılır. Çözümleme ise merkezde yapılır. Yani otoparklarda NFC kart ile yapılan işlemler local olarak şifrelenir fakat çözümleme merkezde yapılır. Sıradan NFC okuyucularının olduğu sistemlerde ise çözümleme genelde aynı yerde gerçekleşir.

Burada diğer sistemlerden farklı olarak şifreleme local şekilde yapılır ve TTVPN boyunca iletilen veriler kriptolu olarak gönderilir. Kriptolu olarak merkeze gelen işlem verisi çözülür ve karşı cevabı tekrar kriptolu olacak şekilde kriptolayarak local otoparka gönderir. Otoparklarda ise şifreleme ve çözme işlemini sam-modül yapar. Bu modül bariyerli otoparkların bilet alma-verme makinalarında ve ödeme işleminin yapıldığı otomatik parkomat sistemlerinin içinde bulunmaktadır. Şekil (5.1.1)' de İspark otomasyon sistem tasarımı gösterilmiştir.



Şekil 5.1.1. İspark Otomasyon Sistem Tasarımı

Tasarlanan bu sistemin kırılması ve bir işlem bitinin çözümlenmesi için öncelikle IPSEC yapısını kırmak, sonrasında ise DES şiflerini çözümlemek gerekir. Ancak bu şekilde yapılan işlemin içeriği görüntülenebilir. Bu işlem Amerikan Savunma Sanayisi'nin Süpernova bilgisayarlarına erişmek ve sisteme sızmak kadar zordur ama imkânsız değildir.

5.2. Bariyerli Otoparkların Entegrasyonu (Açık ve Kapalı)

İSPARK toplamda 118 adet bariyerli otoparka sahiptir. Bu otoparkların tamamında İstanbul kart uyumlu donanımlar kullanmıştır. Otoparkların çalışma prensibinden bahsedecek olursak;

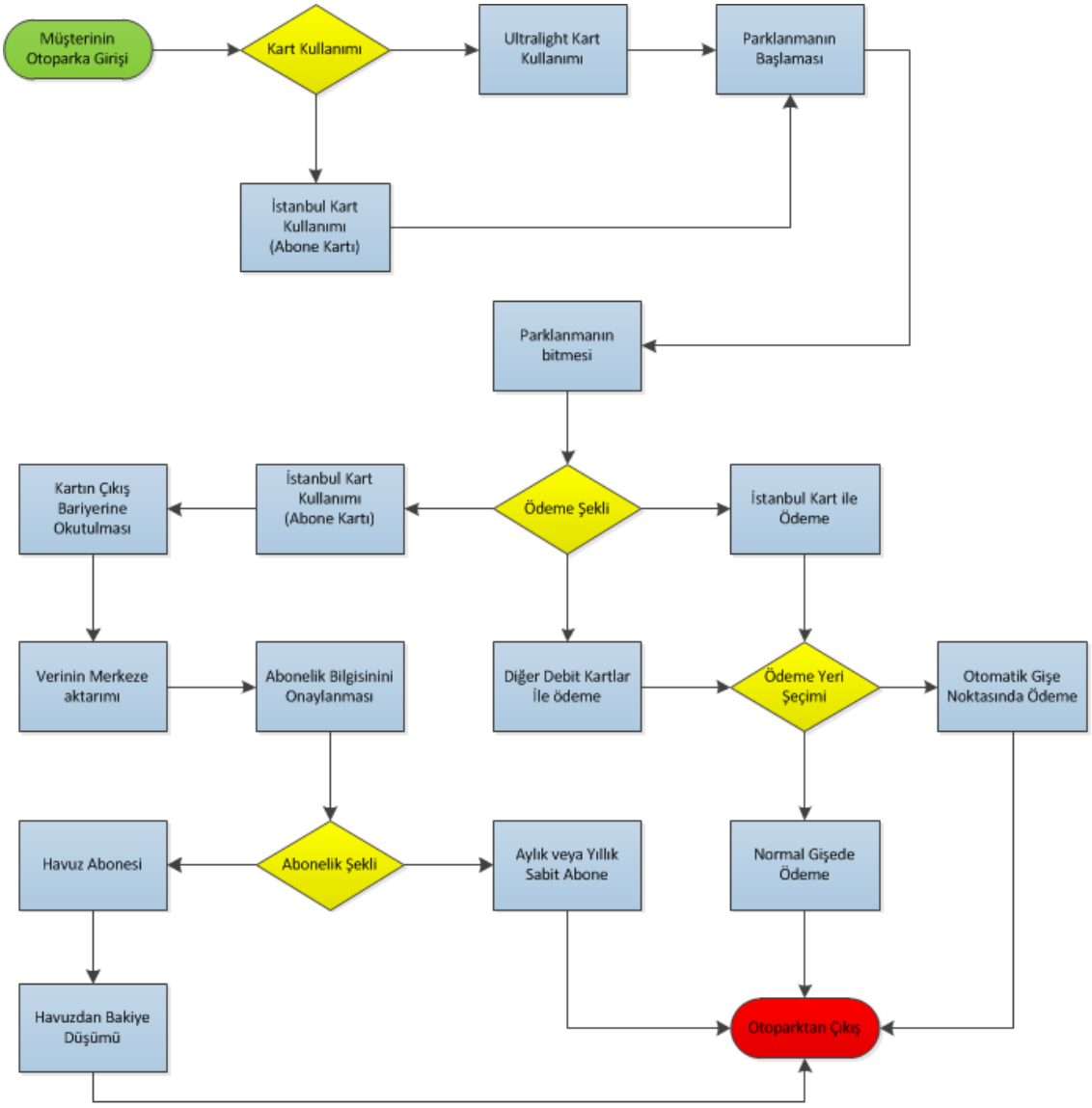
- Müşteri otoparka giriş yaptığında bir bilet verme makinası ile karşılaşır. Bu makinada İstanbul Kart okuyucusuda yer almaktadır. Abone olan müşteriler bilet almadan direkt olarak İstanbul kartını okutup otoparka giriş yapabilirler. Yine çıkışta da İstanbul kartını okutarak çıkış yapabilecekler.

Abone olmayan bireysel müşteriler ise İstanbul kartını ödeme aracı olarak kullanacaktır. Senaryo şu şekildedir;

- Müşteri giriş bilet verme makinasından bilet aldıktan otoparka giriş yapar.
- Parklanmayı tamamladıktan sonra otomatik gişeye gelir.
- Otomatik gişeye, giriş biletmatikten aldığı bileti verir.
- Müşteri karşısına çıkan ödeme tiplerinden İstanbul kartı seçer. Kartını otomatik gişede bulunan okuyucuya okutur ve ücret karttan alınır.
- Gişe, ödemesi İstanbul kart ile yapılan bileti müşteriye geri verir. Müşteri arabasına binip çıkış bariyer gişesine gelir.
- Ödemesini yaptığı bileti çıkış bilet yutmatiğe verir. Yutmatik bileti yutar ve ödemesi yapılan biletin bariyerini açarak müşterinin çıkışını sağlar.

Otomatik gişelerde aynı zamanda İstanbul kart satılabilecek ve dolumuda yapılabilecektir.

Şekil (5.2.1.)' de Bariyerli Otoparkların EPC Diyagramına Göre İş Akış Şeması gösterilmiştir.



Şekil 5.2.1. Bariyerli Otoparkların EPC Diyagramına Göre İş Akış Şeması

5.3. Bariyersiz Otoparkların Entegrasyonu (Yol Üstü-Single Park)

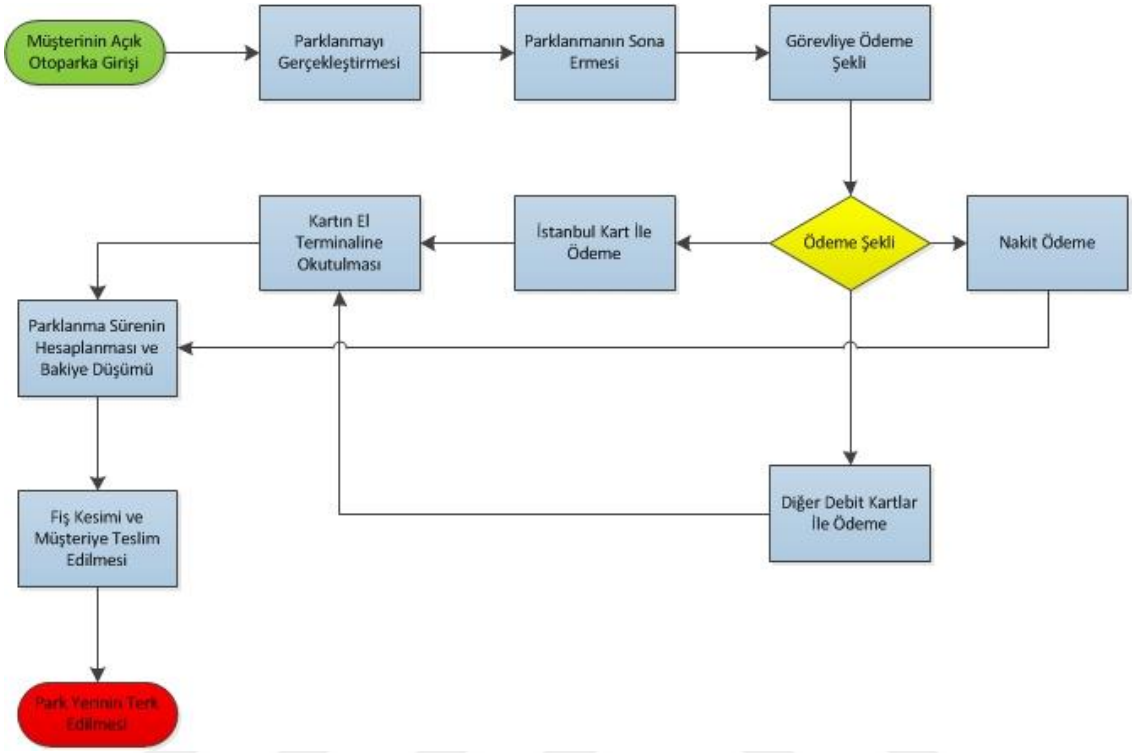
İSPARK hali hazırda bünyesinde 250 den fazla yol üstü otopark işletmektedir. Bu otoparklarda bulunan el terminalleri sayesinde sayısal işlemleri yürüten İspark, İstanbul kart entegrasyonunu bu cihazlar ile de sağlamıştır. İSPARK yol üstü otoparklarında NFC uyumlu el terminalleri kullanmaktadır. Şekil (5.2.1)' de NFC uyumlu bir el terminali gösterilmiştir.

Şekil 5.3.1. NFC Uyumlu Bir El Terminali

Bu cihazların üzerinde bulunan okuyucular İstanbul kart yapısını desteklemektedir. Dolayısıyla merkezi yazılım üzerinden çalışan el terminallerine İstanbul kart projesi birkaç yazılımsal müdahale ile entegre edilmiştir. Şu anda aktif olarak tüm cihazlarda denemeler devam etmektedir. Kullanım senaryosuna bakacak olursak;

- Müşteriler yol üstü bir otopark kullandıklarında, parklanma öncesinde veya sonrasında İstanbul kart ile ödeme yapabileceklerdir. Bakiyesi yetersiz gelmeleri durumunda yine el terminalleri üzerinden ücret yüklemesi yapılabilecektir.

Şekil (5.3.2.)' de Bariyersiz Otoparkların EPC Diyagramına Göre İş Akış Şeması gösterilmiştir.



Şekil 5.3.2. Bariyersiz Otoparkların EPC Diyagramına Göre İş Akış Şeması

6. SONUÇ

Mifare kartlar sağladıkları minimum işlem zamanı, dolandırıcılığın minimize edilmesi gibi sunmuş olduğu avantajlar sayesinde toplu taşımacılık, kartlı geçiş sistemleri ve elektronik cüzdan gibi uygulamaların yanı sıra otopark sektöründe de dünyada en fazla tercih edilen ve büyümeye devam eden sistem olmaktadır. Bu bağlamda İSPARK gibi otopark firmaları, İstanbul'un smart city olması için en önemli iştiraklerinden biri haline gelmiştir ve gelecektir.

Akıllı kartların ulaşım sektörü ve diğer ödeme sistemlerinden sonra otoparklarda kullanılması, hem müşteri hem de kurum açısından kazan-kazan modeli oluşturmaktadır. Kullanımı basit, riski az, güvenliği yüksek, temini kolay olan bu kartların otoparklarda kullanımı şüphesiz İstanbul'da parklanmayı daha basit hale getirecek, parklanma süresini düşürecek ve trafiği olumlu yönde etkileyebilecektir.

Aynı zamanda güvenlik alt yapısı sayesinde vatandaşların kullandıkları diğer debit kartlara göre bir üst seviyede olacaktır. NFC kartların kullandığı AES şifre yapısı buna paralel olarak 56bit'lik DES algoritması bu kartların güvenlik altyapısını seviyesini yükselten temel unsurlardır.

Akıllı kartların dolum limitine sınırlama getirildiği takdirde kayıp, çalıntı gibi durumlarda diğer debit kartlar gibi yüksek meblağlarla kullanıcıyı zarara uğratmayacak veya vatandaşın işin hukuki boyutları ile uğraşmasına gerek kalmayacaktır.

Akıllı kartlar kişiye özel tanımlandığı takdirde E-Devlet uygulamasından anında kayıp veya çalıntı halinde pasif hale getirebilir. Yine aynı uygulamada vatandaş tanımlı kredi kartından akıllı kartına anında bakiye yükleyebilir veya eskiyen kartın yenisi E-Devlet deki ikamet adresine talep edebilir.

Akıllı kartların Smart City tanımı kapsamında tüm şehrin alışveriş noktalarına veya diğer ihtiyaçlar konusunda kullanıldığı dünya örneklerinde görülmektedir. Dolayısıyla tek bir kart ile şehirde ki her olanaktan faydalanmanın ve riski yok denecek kadar az olan bir akıllı kartın otopark sektöründe de kullanımının yaygınlaştırılması gerekmektedir.

KAYNAKLAR

[1] S. C. Alliance, (2013). “Near Field Communication (NFC) and Transit:Applications, Technology and Implementation Considerations”.

[2] First Data, (2010). “Transit Payment Systems: A Case for Open Payments”.

[3] NFC Forum, (2011). “NFC in Public Transport, Wakefield: NFC Forum”.

[4] C. Lackner-NXP, (2013). “The power of NFC”, Wima NFC Monaco, 22-24 Nisan 2016.

[5] PLDS, (2013). "NFC in the Automotive World", Wima NFC Monaco, Monaco, 2013.

[6] Tagawa, K., (2013). "The Four Essential Keys to a Winning NFC Solution", Wima Monaco, 22-24 Nisan 2013.

[7] N. Forum, NFC Forum Specification Architecture, http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/, 8 Şubat 2017.

[8] Smart Card Alliance, (2011). “The Mobile Payments and NFC Landscape: A U.S. Perspective”.

[9] Langer, A. ve Josef, O., “Secure Element Development”.

[10] SIMAlliance, (2013). “NFC Secure Element Stepping Stones v1.0”, 2013.

[11] Langer, G., (2008). “Near Field Communication based Mobile Payment System”, Proceedings der 3. Konferenz Mobilität und Mobile Informations systeme, 2008.

[12] Clark, S., NFC to account for 30% of mobile tickets, http://www.nfcworld.com/2014/02/17/327868/nfc-account-30-mobile-tickets/ , 15 Nisan 2014.

[13] Oruç, Y., Hardware Security Module (HSM) nedir?, http://www.cozumpark.com/blogs/gvenlik/archive/2012/02/12/hardware-security-module-hsm-nedir.aspx. , 7 Mart 2016.

[14] First Data, (2009). “Trusted Service Manager: The Key to Accelerating Mobile Commerce”.

[15] Smartcard Alliance, (2009). “Security of Proximity Mobile Payments, A Smart Card Alliance Contactless and Mobile Payments”.

[16] Kaasinen, E., (2005). "User acceptance of mobile services value, ease of use, trust and ease of", Tampere University of Technology, 2005.

[17] C. GmbH, (2013). “Integrated best in class NFC Solutions for your business” Wima NFC Monaco, 22-24 Nisan 2013.

[18] MIFARE4Mobile Industry Group, (2012), “enabling electronic ticketing and access management applications on mobile devices”.

[19] Pereira A., (2011). “Consumer Adoption of NFC Lineer CommMode”, NORGES HANDELSHØYSKOLE .

ÖZGEÇMİŞ

Adı Soyadı : Ali GÜNGÖR

Doğum Yeri ve Yılı : Manisa 08.12.1978

Medeni Hali : Evli

Yabancı Dili : İngilizce

E-posta : ali.gungor@ispark.istanbul

Eğitim Durumu

Lise : Turgutlu Endüstri Meslek Lisesi, 1994

Lisans : Marmara Üniversitesi, Elektrik Öğretmenliği, 1997

Yüksek Lisans : İstanbul Ticaret Üniversitesi, Siber Güvenlik, 2015

Mesleki Deneyim

BELBİM A.Ş.
Elektronik ve PC Atölye Şefi 2001-2011

İSPARK A.Ş.
Bilgi Sistemleri Müdürü 2015-(devam ediyor)

Yayınları