T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AKILLI KİMLİK KARTI UYGULAMASI

YÜKSEK LİSANS TEZİ

Ahmet ŞANSLI

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜH.

Tez Danışmanı : Yrd. Doç. Dr. Hayrettin EVİRGEN

Ağustos 2007

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AKILLI KİMLİK KARTI UYGULAMASI

YÜKSEK LİSANS TEZİ

Ahmet ŞANSLI

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜH.

Bu tez 02 / 08 /2007 tarihinde aşağıdaki jüri tarafından oybirliği/oyçokluğu ile kabul edilmiştir.

Yrd. Doç. Dr. Hayrettin EVİRGEN	Prof. Dr. Ümit KOCABIÇAK	Yrd. Doç. Dr. Mustafa TURAN
Jüri Başkanı	**Üye**	**Üye**

TEŞEKKÜR

Bu tez çalışmasının hazırlanışında bana yol gösteren tüm hocalarıma özellikle danışman hocam Yrd.Doç.Dr Hayrettin EVİRGEN'e, tezin düzenlenmesinde Arş.Gör.Burhan BARAKLI, Arş.Gör.Melih Göksel, Arş.Gör.Ahmet KÜÇÜKER, Arş.Gör.Tuğba TUNACAN ve de beni hiçbir zaman yalnız bırakmayan Endüstri Mühendisi Dilek ORMANCI'ya, her zaman yanımda oldukları için teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

ISO : International organization for standardization

VCC : Power supply input – besleme gerilimi

RST : Reset – yeniden başlatma sinyali

CLK : Clock signal – saat sinyali

RFU : Reserved for future use – İleride kullanılmak üzere ayrılmış

GND : Ground – toprak

VPP : Programming voltage input – programlama gerilimi

I/O : Input/output – giriş/çıkış

ATR : Answer to reset – başlatma cevabı

TS : Başlangıç karakteri

TO : Format karakteri

TA_i : Arayüz karakteri

TB_i : Arayüz karakteri

TQ_i : Arayüz karakteri

TD_i : Arayüz karakteri

T_i : Hatırlatma karakteri

TC_k : Kontrol karakteri

RAM : Random access memory – rastgele erişilebilir bellek

EDC : Blok hata yakalama kodu

CLA : Komut sınıfı

INS : Komut

P1 : Komut için paramatre

P2 : Komut için paramatre

Lc : Verinin boyutu

Le : Cevap uzunluğu

SW1 : Durum baytı

SW2 : Durum baytı

DF : Dedicated file

EF : Elementary file

MF : Master file

PIN : Personal identification number – kişisel tanımlama numarası

CPU : Central processing unit

ROM : Read only memory

RFID : Radio frequency identification – temassız akıllı kart

OGS : Otomatik geçiş sistemi

KGS : Kartlı geçiş sistemi

GSM : Global system for mobile communications – mobil iletişim sistemi

SIM : Subscriber identity module – kişisel kimlik modülü

MAC : Message authentication code – mesaj doğrulama kodu

DES : Data encryption standart – veri şifreleme standartı

RSA : Rivest shamir algorithm – açık anahatarlı şifreleme

AB : Avrupa birliği

POS : Point of sale – satış cihazı

ŞEKİLLER LİSTESİ

TABLO LİSTESİ

ÖZET

Anahtar kelimeler: Akıllı kart, rsa, des, şifreleme

Akıllı kartlar, bünyesinde bulundurduğu mikroişlemciler ve bellekler sayesinde küçük bir bilgisayara benzetilebilir. Yarıiletken teknolojilerindeki gelişmelere bağlı olarak, mikroişlemci teknolojisi çok küçük ve hızlı bir yapıya kavuşmaktadır[1]. Bu özelliklere bağlı olarak, mikroişlemciler çok kısa sürede kod yapılarını işletebilmektedir. Akıllı kartlarda mikroişlemcilere yazılan işletim kodları yardımıyla bellek bölgelerine erişilip veri okuma ve yazma işlemleri gerçekleştirilmektedir.

Bu tez çalışmasında, kişinin özlük bilgilerinin bir kartta tutulması, çeşitli uygulama alanlarında da yalnızca bu kartı kullanarak işlem yapmak üzere bir uygulaması tasarlanmıştır. Tasarlanan bu uygulama neticesinde, kişiler tüm kimlik ya da özlük bilgilerini gerektiren herhangi bir yerde bu kartı kullanabilecektir. Aynı zamanda bankamatik kartları, kimlik bilgisi kartları vb. kartların yerine bu kartın kullanılması amaçlanmıştır.

SMART IDENTITY CARD APPLICATION DEVELOPMENT

SUMMARY

Key Words: Smart card, RSA, DES

A smart card is a card that is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. The microprocessor card can add, delete, and otherwise manipulate information on the card. Smart cards, unlike magnetic stripe cards, can carry all necessary functions and information on the card. Smart cards, as a result of including microprocessors, and memories act as a mini computer. Semi conductor devices technologies are grooving so fast, by the fact that microprocessor technology is becoming so little and fast. By all of these, microprocessors are able to execute code structures in effective times. Smart cards uses this codes to access memory ranges for read and write processes.

In this study, person's identity datas stored on a smart card. And that smart identity card will be used for all daily processes that requires authentication and identification of person. As a fact that card will be used in systems as debit, credit cards, driver licence and health card.

BÖLÜM 1. GİRİŞ

Sürekli gelişen teknolojilerle birlikte artık kişilerin ihtiyaçları da değişmektedir. Eskiden kullanılmakta olan sistemlerin yenilenme ihtiyacı da bu değişimlere bağlı olarak gelişmektedir. Günümüzde her dakika kullanmakta olduğumuz teknolojilerin yerini daha gelişmiş bir üst sürümleri almaktadır. Bu değişim ve gelişmelerin yaşandığı alanlardan biri de kişiyi tanımlayan; kimlik kartı, banka kartı, ehliyet gibi kartlar üzerinde yaşanmaktadır.

Getirdiği kolaylıklar, dayanıklılığı, yüksek güvenlik unsurları ve daha fazla veri depolayabilme gibi özellikleri sebebiyle akıllı kartların günümüzde kullanılmakta olan manyetik şeritli bankamatik kartlarının yerini alması kaçınılmaz olacaktır. Bu kartlara kimlik bilgileri gibi kişinin özlük bilgileri yüklenmesiyle; trafik denetimi, sağlık sistemi, alışveriş gibi kimlik belgesi gerektiren yerlerde işlemlerin daha hızlı, güvenli ve etkin bir şekilde yapılmasını sağlayacaktır.

Akıllı kartlar günümüzde birçok ülkede çeşitli yüksek güvenlik ve kimlik doğrulama gerektiren uygulamalarda etkin bir şekilde kullanılmaktadır[2]. Bu tezin amacı, kimlik, ehliyet, banka kartı, kredi kartı gibi gereksinimlerin tek bir akıllı kart kullanarak sağlamaktır.

Tek kart üzerinden bu işlemlerin sağlanması amacıyla kişinin, kimlik, ehliyet, sağlık, banka hesap bilgilerinin ilgili kurumlarca sağlanacak olan veritabanlarında kayıt altında olması gerekmektedir. Günümüzde kişiye ait bilgiler farklı farklı kurumlarda dağınık ve birbirinden bağımsız bir şekilde yer almaktadır. Bu da bilgiye erişimi kısıtlamaktadır. Gerek veri girişi gerekse bu bilgilerin değiştirilmesi sırasında insan kaynaklı hatalı kayıtların girilmesine bağlı olarak tutarsızlıklar meydana gelmektedir.

Tasarlanan sistemde kişinin özlük bilgileri bir merkezde tutulacaktır. Diğer uygulamlar da bu merkezden, kişi herhangi bir hizmet aldığı sırada ya da gerekli bir

kontrol sırasında kişinin kartını kullanarak sisteme güvenli, hızlı ve etkin bir şekilde erişebilecektir. Buna bağlı olarak da günümüzde sorun teşkil eden kimlik sahteciliği, sahte evrak düzenlenmesi gibi girişimler engellenmiş olacaktır. Aynı zamanda her kurumun, diğer kurumlarla koordineli çalışan bireylerle ilgili verileri içeren kendine ait bir veritabanı oluşacaktır. Bu veritabanlarında saklanan verilerden elde edilen bilgiler doğrultusunda ülke ekonomisinin gelişimine katkıda bulunulacak yatırımlar, oluşturulabilecek, yeni pazarlama ve pazar oluşturma stratejileri geliştirilebilecektir.

BÖLÜM 2. KİMLİK KARTLARI

Kimlik kartları; kişinin kim olduğunun tanımlanmasıyla ilgili bilgileri içerecek şekilde tasarlanmış kartlardır. Kartın içermesi gereken bilgiler genellikle kişinin ismi, fotoğrafı, doğum tarihi, anne adı, baba adı, vatandaşlık numarası gibi kişiye özgü tanımlayıcı bilgilerdir.

Dünya üzerinde kullanılan kimlik kartlarının türleri uluslararası standart belirleme örgütü (ISO) tarafından ISO 7810 standartında belirtilmiştir[3]. Bu standartın içerisinde; kullanılacak olan kartların hangi alanlarda, nasıl kullanılacağı, nelere dikkat edilmesi gerektiği, boyutları gibi bilgiler yer almaktadır.

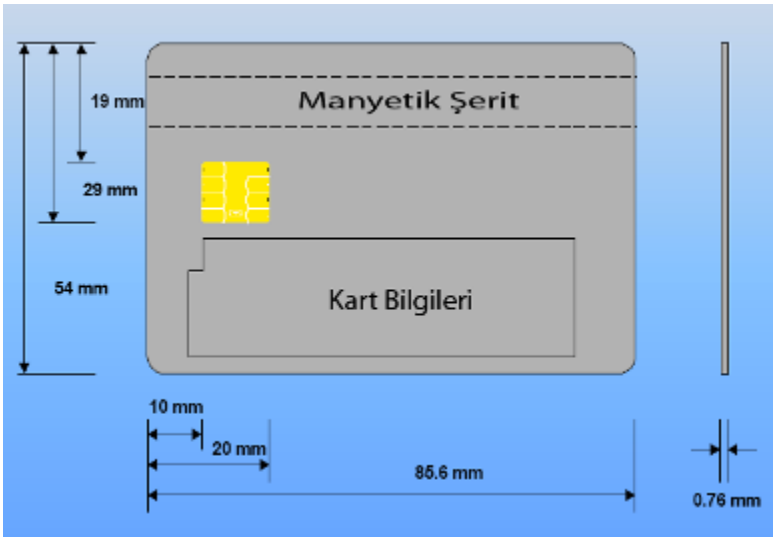
Bu standartta yer alan kartlar günlük hayatta; kimlik dışında bankamatik kartı, kredi kartı, kartvizit, pasaport gibi bir çok yer de kullanılmaktadır. Ayrıca Avrupa Birliği kapsamında yer alan Fransa, Almanya, İtalya gibi ülkelerde karta gömülen mikroişlemci aracılığıyla e-Devlet projeleri kapsamında tüm işlemlerde ID-1 tipindeki akıllı kimlik kartları kullanılmaktadır[2]. Bu tez çalışmasında akıllı olarak adlandırılan kartları inceleyerek tüm kimlik bilgisinin gerektiği vatandaşlık işlemlerinde sahip olunan kartların hepsinin yerine kullanılabilecek bir kimlik kartı sistemi tasarlamaktır.

2.1. Kimlik Kartı Tipleri

ISO 7810 standartında ID-1, ID-2, ID-3 olmak üzere üç tip kart tanımlıdır[3]. Ayrıca standartta kartın imal malzemesi, boyutları, kişiye ait bilgilerin bulunacağı alan, dayanacağı ısı aralıkları gibi sabit bilgiler yer almaktadır. Tanımlanan kart tipleri şu şekildedir:

ID-1 tipindeki kartların boyutları 85.60 × 54.00 mm boyutundadır[3]. Bu tip kartlar çoğunlukla bankacılıkta kullanılır. Bankacılık dışında ehliyet, kredi kartı olarak da kullanılmaktadır. Ülkemizde ehliyet, bankamatik ve kredi kartı olarak kullanımları

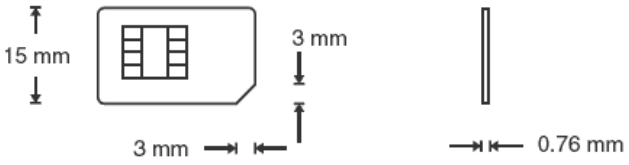
mevcuttur. Bu kart kimlik kartı olarak tanımlanan kartlar arasında en çok tercih edilen kart çeşididir. Şekil 2.1. ID-1 kart'ın ISO 7810 standartında tanımlanan özelliklerinden görünümüyle ilgili bilgileri göstermektedir[3].



Şekil 2.1. ID-1 kart görünümü

Temel özelliklerinin ISO 7810 standartında tanımlanmış olan kart; bankacılık sektöründe kullanılmak üzere, bu sektöre özel tanımlamalar ve standartlar ISO 7813 standartında belirtilmiştir[3]. Kredi, bankamatik kartları temel özellikler dışında kartın kenarlarının 3.18mm yarıçapında yuvarlatılmış olması, kartın kalınlığının 0.76 mm olması gibi bir kaç ek özellik içermektedir. Yine ID-1 kartlar ve tanımlandığı standart baz alınarak ID-1 karta bir mikroişlemci gömmek suretiyle akıllı kartlar olarak adlandırılan ISO 7816 standartı geliştirilmiştir[3].

ID-1 kartların temel özellikleri baz alınarak ID-000 kartlar geliştirilmiştir. ID-000 tipindeki kartların boyutları ilk çıkıtğı zaman kredi kartı boyutu olan 85.60 × 54.00 mm boyutunda idi. Şimdi kullanılan boyutları ise 25 × 15 mm'dir[3]. Bu tip kartlar dünyanın her yerinde yaygın olarak cep telefonlarında kişinin kimliğinin şebekeye tanıtılmasında kullanılmakta ve SIM (Subscriber Identity Module) kart olarak bilinmektedirler. SIM kartlar kullanıcının kimliğini belirleyen bir anahtar içerirler ve bu anahtar aracılığıyla kendisini şebekeye tanıtır. ID-1 kartlardan türetilen bu kartlar sadece boyut olarak farklılıklar içermektedir. Şekil 2.2'de ID-000 kartın boyutları gösterilmektedir.



Şekil 2.2. ID-000 kart görünümü

ID-2 tipindeki kartların boyutları 105 × 74 mm boyutundadır[3]. Bu tip kartlar birçok ülkede kimlik kartı olarak kullanılmaktadır. ID-1'den daha büyük boyutlarda olması kartın yüzeyi üzerinde kişiyi tanımak üzere kullanılabilecek büyüklükte bir fotoğraf sığmasına rağmen yine de cüzdanda taşınacak boyutlardadır.

ID-3 tipindeki kartların boyutları 125 × 88 mm boyutundadır[3]. Bu tip kartlar pasaport ve uluslararası geçişlerde kullanılmak üzere verilen vizelerde kullanılmaktadır.

2.2. ISO 7816 - Temaslı Tümleşik Devre Kartı Standartı

Kimlik kartlarıyla ilgili en önemli ve en geniş bilginin olduğu, akıllı kartların uyduğu temel standart ISO 7816 standartıdır. Bu standartta tanımlanan kartlar akıllı kartlar olarak da bilinmektedir. ISO 7816 standartı farklı ve bağımsız parçalardan oluşmuştur. Her bir parçada kartın fiziksel karakteristiği, düzeni, veri erişim teknikleri, veri saklama teknikleri, sayı sistemleri ve kaydetme prosedürleri gibi konular açıklanmıştır[5]. Tezde gerçekleştirilen uygulamalar da bu standartlardan yararlanılarak gerçekleştirilmiştir.

Bu standart aşağıdaki bölümleri kapsamaktadır.

- Bölüm 1 - Fiziksel karakteristikler
- Bölüm 2 - Çipin boyutu ve yeri
- Bölüm 3 - Elektronik sinyaller ve iletişim protokolleri
- Bölüm 4 - Endüstriyel ortak komutlar
- Bölüm 5 - Uygulama tanımlayıcıları için sayı sistemi ve kaydetme prosedürü
- Bölüm 6 - Değişim yapmak üzere kullanılacak veri elemanları

– Bölüm 7 - Endüstriyel ortak değişim komutları

ISO 7816 standartı farklı bölümlerden oluştuğu için, her bölüm gelişen teknoloji ve piyasa koşullarına göre birbirinden bağımsız olarak değiştirilebilmektedir.

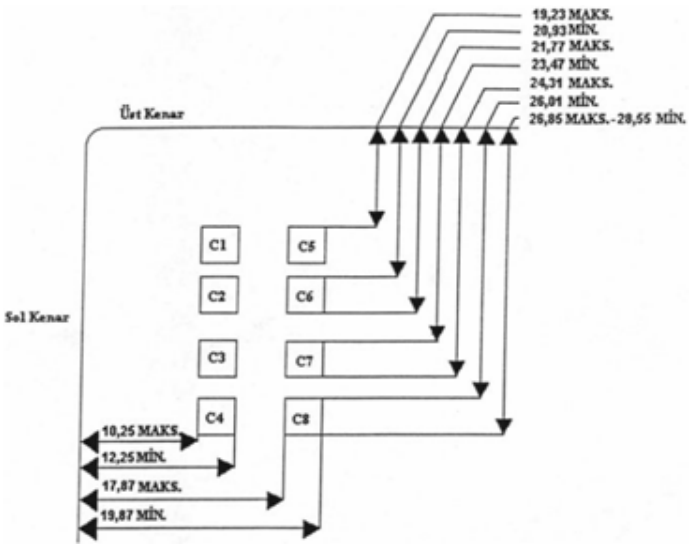
Birinci bölümde; kartın fiziksel özellikleri (imal edileceği malzemenin türü , kalınlığı, boyutları, çalışma sıcaklık aralıkları v.b.) belirtilmiştir. Bunların dışında kartın çalışabileceği ortam koşulları da belirtilmiştir[3].

İkinci bölümde; elektrik elemanlarının boyutları ve kart üzerindeki yerleri belirtilmiştir. Okuyucuların bütün tümleşik devre kartalrını okuyabilmesi için, çipin yerinin ve boyutlarının standart olması şarttır[10].

Tümleşik devre kartı 8 tane elektrik elemanı taşımaktadır.Bunlar C1'den C8'e kadar tanımlanmıştır. Bu 8 elamanın hepsi fiziksel olarak mikroişlemciye bağlı değildir. 2 tanesi ileride kullanılmak üzere saklanmıştır.

1990 yılında temaslı devre kartlarının bağlantılarının Şekil 2.3 'deki gibi olması kararlaştırılmıştır. Burada çip pozisyonu kartın uzun eksenine daha yakındır[4].

Şekil 2.3. Temaslı devre kartının elektrilsel elemanları'nın kart üzerindeki yerleşimini göstermektedir.



Şekil 2.3. Temaslı devre kartının elektrilsel elemanları[4]

Üzerinde durulması gereken bir başka konu da kart bağlantılarının kartın hangi yüzünde bulunması gerektiği konusudur. Aslında kartın her iki yüzünün de kullanılmasına izin verilmiş olmasına rağmen genellikle bağlantılar, kabartma ile birlikte kartların ön yüzünde bulunmaktadır. Şekil 2.4'de manyetik şeritin bulunduğu arka yüz görülmektedir[4].

Şekil 2.4. Kart üzerinde bulunan veri birimleri[4]

Tablo 2.1'de kartın elektriksel elamanların açklamaları görülmektedir.

Tablo 2.1. Akıllı kart elektrik elemanları ve işlevleri

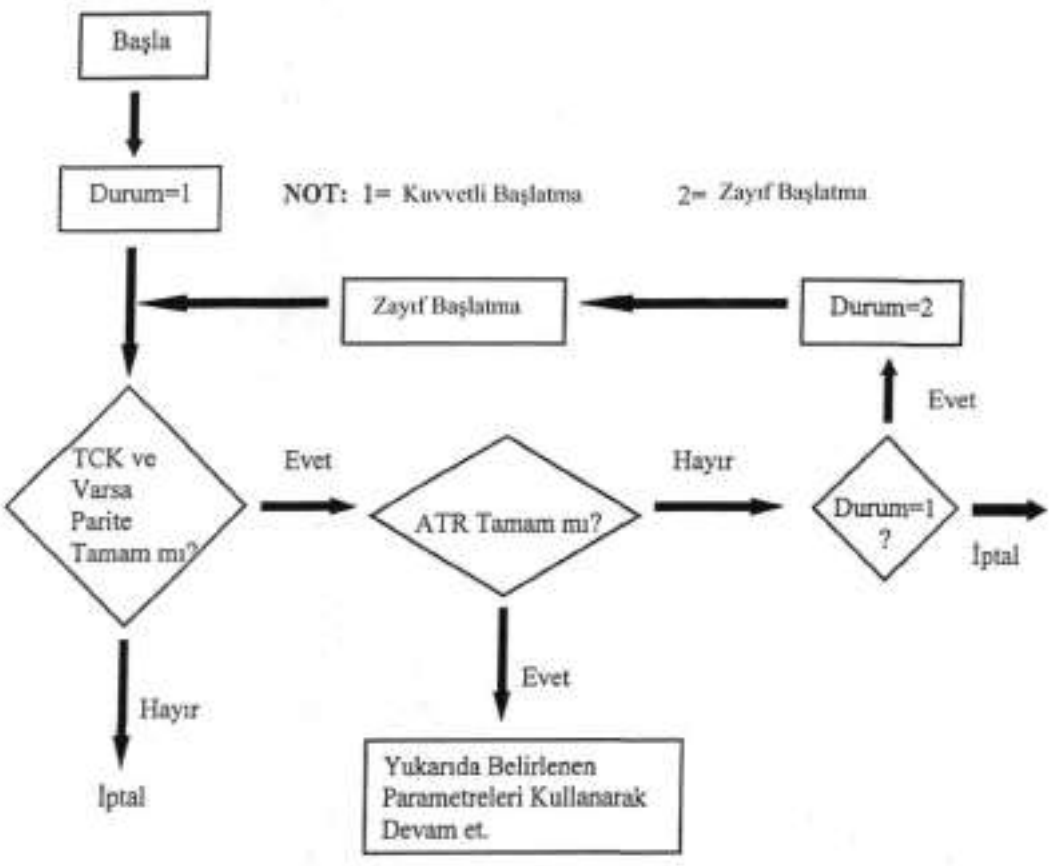
Kontak	Sembol	İşlev
C1	VCC	Besleme gerilimi, (3V-5V)
C2	RST	Mikroişlemciye yeniden başlatma (reset) sinyali göndermede kullanılır.
C3	CLK	Saat sinyali
C4	RFU	Daha sonra kullanılmak üzere aynlmıştır
C5	GND	Toprak 0 V
C6	VPP	EEPROM programlamak için gerekli olan programlama voltaj girişidir.
C7	I/O	Veri hattı iletişiminin nasıl gerçekleştireleceği
C8	RFU.	Daha sonra kullanılmak üzere aynlmıştır

Üçüncü bölümde; elektriksel özellikler ve iletişim kuralları belirtilmiştir. Ayrıca kart ile okuyucu terminal arasındaki iletişim protokolleri açıklanmıştır. Akıllı kart ile terminal arasındaki iletişim komut/cevap mimarisine dayanmaktadır. Karta gönderilen komuta karşılık karttan cevap alınmaktadır. Burada tanımlanan elektriksel

özellikler ve iletişim kuralları kartın diğer cihazlarla karşılıklı çalışabilmesi için gerekli koşulları belirleyen temel konulardır[11].

Üçüncü bölüm, başlatma komutunun sinyallerini ve karşılık olarak terminale vereceği yanıtları belirler. Başlatma komutu, kartı ilk durumuna getirir. Başlatma komutu, akıll kart ile okuyucu terminal arasında el sıkışma işlemi sırasında (iletişim kurulması sırasında) kullanılan ilk komuttur. Bu el sıkışma sırasında, kartın ve okuyucunun teknik kapasitesine göre haberleşme protokolü belirlenir.

Başlatma komutu ile gönderilen baytlarda kartın kapasitesi, çalışma gerilimi (3 volt gibi), veri aktarım hızı, asenkron çalışabilme imkanı, blok iletişim protokolü ile ilgili bilgiler bulunur. Ayrıca başlatma komutunda mikroişlemcinin çalışma hızı da belirtilir.



Şekil 2.5. Başlatma komutu[4]

Bu bölümde tanımlanan elektriksel özellikler Tablo 2.1'de verilmiş olan elektrik elemanlarını kapsamaktadır.

VCC(Power Suply Input - besleme gerilimi), kart için güç besleme gerilimi 4.75 volt ve 5.25 volt arasındadır ve kullamlan maksimum akim 200 mA' dir. Yeni üretilen çiplerde 0.8 um ve hatta 0.5 um teknolojisi kullanılmaktadır. Bu çipler 3 volt ile çalışabilmektedirler ve böylece daha az akım tüketmektedirler[6,11].

RST(Reset Signal - başlatma sinyali), tümleşik devre kartını okuyan ara yüz cihazı tarafından verilir ve kartın hafızasındaki programı başlatmak için kullanılır. ISO standartlarında; dahili başlatma, etkin zayıf başlatma ve senkronize etkin kuvvetli başlatma olmak üzere üç ayrı başlatma modu tanımlanmıştır. Birçok tümleşik devre mikro işlemcisi, başlatma geriliminin yüksek gerilim seviyesine dönmesiyle, tümleşik devre kartlarının kontrolü programın başlangıç adresine gönderdiği, etkin zayıf başlatma modunu kullanır. Telefon kartları gibi bellek tümleşik devre kartları daha çok senkronize modda çalışırlar[11].

Kart okuyucu cihaza takıldığı zaman kart okuyucu ara yüz cihazının etkin hale geliş sıralaması şöyledir :

- RST'yi düşük seviyeye çek,
- VCC gerilimi ver.
- Giriş/Çıkış'ı alıcı moduna getir,
- VPP gerilimini bekleme moduna al,
- Saat sinyali uygula,
- RST'yi yüksek seviyeye çek.

Bu işlem kartla ilgili yapılacak olan işlemlerin karta fiziksel olarak bir zarar vermemesi için yapılması gereken işlemlerdir.

Aynı şekilde kart üzerinde işlemler gerçekleştirildikten sonra kartı okuyucu cihazdan çıkartmadan önce yapılması gereken işlemlerin sıralaması şöyledir:

- RST'yi düşük seviyeye çek,
- Saat sinyalini düşük seviyeye çek,
- VPP gerilimini kes,

- Giriş/Çıkış'ı düşük seviyeye çek,
- VCC gerilimini kes.

CLK(Clocking Signal - saat sinyali), tümleşik devreler çalışabilmek için kendi saat devrelerini içerebilecekleri gibi genellikle birçok tümşeşik devre saat sinyalini diğer cihazdan almaktadır. Giriş/Çıkış portundan yapılan seri haberleşme hızının bu saat frekansı ile belirlenmektedir. ISO standartlarında 3.579545 MHz (T=0) ve 4.9152 MHz (T=1) olmak üzere iki ayrı harici saat frekansı belirlenmiştir. Bunlardan birincisi daha yaygın kullanılmaktadır. Her ikisi de 9600 bps seri iletişim hızı sağlamaktadır[4,11].

Standartlara göre, başlatma işleminden sonra bu frekanslardan sadece bir tanesi kullanılmakla beraber, protokol tipi seçimi ile bunun değiştirilebilmektedir.

VPP(Programmin Voltage Input - Programlama Gerilimi), akıllı kartların ilk çıktığı zamanlarda kalıcı belleğe bilgi yazma ve silme işlemleri için gereken yüksek gerilimi sağlayabilecek şekilde tasarlanmıştır. EPROM tipi belleklerin programlanabilmesi için devre bağlantıları aracılığıyla dışardan alınan yüksek gerilimlere (12.5V veya 21V) ihtiyaç bulunmaktadır. Daha çok T=0 protokolünün haberleşmesinde kullanılmaktadır. Günümüzde kullanılan kartlar 3-5V ile çalıştığı için bu işlemi VCC kullanılarak yapılmaktadır ve VPP kullanılmamaktadır.[4,11].

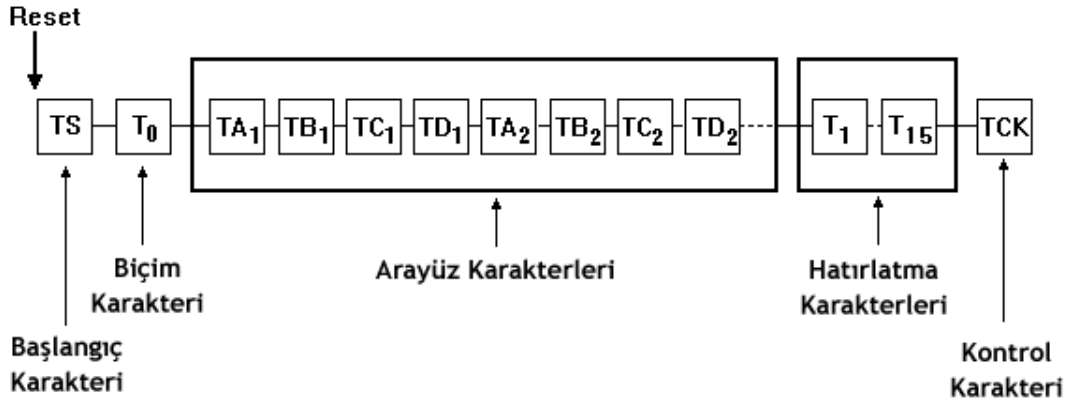
I/O(Input/Output - giriş/çıkış), ISO standartları, tümleşik devre kartı ve okuyucu arayüz cihazı arasındaki veri alış verişi için sadece bir hat tanımlar. Yani bu hat tümleşik devre kartı veri iletirken ve alırken yön değiştiriyor olmalıdır. Günümüzde kullanılan tek yönlü, yarı çift yönlü, tam çift yönlü olmak üzere iki cihazın haberleşmesinde kullanılan iletişim tekniklerinden kartın desteklediği ve kullandığı yarı çift yönlü olandır. Okuyucu tarafından istek yapılır, karttan yapılan bu isteğe göre aynı veri yoluyla cevap gönderilir[4,11].

ATR(Answer To Reset - başlama cevabı) kart okuyucu arayüz cihaz başlatma sinyalini gönderdikten belli bir süre sonra tümleşik devre kartından başlatma cevabı gelir. Etkin zayıf başlatma modunda, tümleşik devre kartı başlatma sinyalinin yükselen kenarından sonra 400 - 40000 saat çevrimi içerisinde cevap vermelidir.

Başlatma cevabı başlangıç karakteri dahil en fazla 33 karakter uzunluğunda ve 5 bölümlüdür:

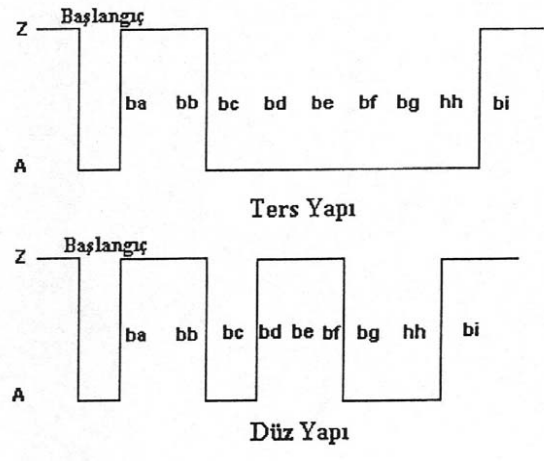
- Başlangıç karakteri (TS)
- Format karakteri (TO)
- Arayüz karakterleri (TA_i, TB_i, TQ_i, TD_i)
- Hatırlama karakterleri (T_1, T_2 ...T_k)
- Kontrol karakteri (TC_k)

Bu bölümler Şekil 2.6'da belirtildiği sırada gönderilir.



Şekil 2.6. Başlatma komutunun cevap yapısı

Bütün bu bölümler Şekil 2.6'daki sırada gönderilirler. Başlangıç karakteri TS, aslında veri iletişim hızını ve mantığını belirleyen bir bit senkronizasyon modelidir. Başlangıç karakterinin formatı Şekil 2.7'de gösterilmiştir. Burada düz ve ters olmak üzere iki ayrı muhtemel yapı gösterilmektedir. Mantıksal 1 seviyesinin düşük seviyeyi gösterdiği ters yapıda en önemli bit önce gönderilir. Mantıksal 1 seviyesinin yüksek seviyeyi gösterdiği, düz yapıda en az önemli bit en önce gönderilir. Bu da uygun yapının seçimine göre, başlangıç karakterinin düz yapıda, onaltılık sistemde, "3B" ve ters yapıda da "3F" ile gösterileceği anlamına gelir[4].



Şekil 2.7. Ts başlangıç karakterinin yapısı[4]

Biçim karakteri, başlatma cevabının diğer karakterleri hakkında bilgi verir. En önemli 4 biti; TA_1, TB_1, TC_1, ve TD_1 karakterlerinin bulunup, bulunmadığını gösterir. Örneğin, en önemli 8. bit 1 durumunda ise başlatma mesajı TD_1 karakterini içermektedir. Aynı şekilde 7. bit 1 durumunda ise TC_1 karakteri bulunmaktadır[4].

Biçim karakterinin en az önemli 4 biti, hatırlama bölümündeki karakter sayısını verir. Böylece, burada 4 bit kullanılmış olması, hatırlama karakterlerinin sayısının en fazla 15 olabileceğini gösterir.

Arayüz karakterlerinin (TA_i, TB_i, TC_i, TD_i) bulunduğu bölüm başlatma cevabının en karmaşık bölümüdür. Bu karakterler, EPROM'un o anki parametreleri, kullanılan programlama gerilimi ve mümkün olan iletişim protokolleri ile ilgili bilgi taşırlar. ISO 7816-3 bölümü, protokol tipini ve parametrelerini daha kolay değiştirebilmek ve karışıklıkları önlemek için yeniden gözden geçirilmektedir. Gerçekte işi karmaşık hale getiren neden, daha önce sadece T=0 protokolünü dikkate alarak yazılmış uygulamaların protokolünü seçimli olduğu ortamda çalışabilir olmasını sağlamak isteğidir. Şu anda uygulamalar T=0 veya T=1 protokolü ile çalışmaktadır.

Hatırlama karakterleri, kartın yaşam süresi hakkında bilgi vermek amacıyla kullanılırlar. Fakat henüz fikir birliğine varılmamış başka kullanımlarıda vardır. Bu da hazırlanan ISO 7816-4'te incelenmektedir[4].

Kontrol karakterleri, başlatma cevabında sadece T=0 protokolü belirtilmiş ise kontrol karakteri gönderilmez. Bütün diğer durumlarda, kontrol karakteri başlatma cevabının

son karakteri olarak gönderilir. Kontrol karakteri, T0'dan TCK' ya kadar bütün baytların XOR'lanmasıyla elde edilir. Bu da sıfıra eşit olmalıdır[7].

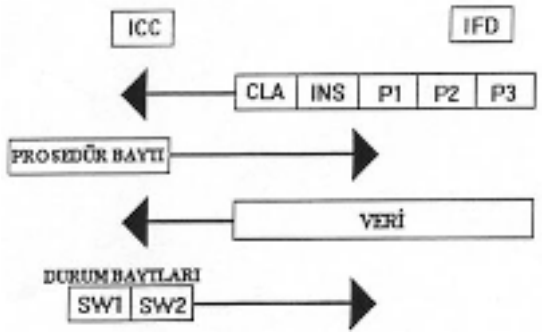
Akıllı kart haberleşme protokolleri diğer haberleşme protokollerinden biraz farklıdır. ISO 7816-3 standartı, kartın çoklu protokol yapısına izin vermesini, gereğinde protokol değiştirebilmesini öngörür. Böylece kartların bütün terminallerde çalışabilmesi sağlanır.

ISO standartlarında, iki protokol tanımı vardır. Bunlar;

T=0 asenkron, yarı çift yönlü karakter aktarımı protokolü, en basit olanıdır ve karta en az iş yükü getirendir. T=1 protokolü çok daha ileri düzeydedir ve hata düzeltme özellikleri vardır. T=1 protokolü, haberleşme açısından çok daha iyidir fakat kartın daha fazla programlama ve RAM belleğine sahip olması gerekir. T=0 protokolü ISO 7816 standartında ilk tanımlanan protokol olması sebebiyle daha çok kullanılmaktadır[7]. Günümüzdeki cep telefonlarında kullanılan akıllı kartları bu iletişim protokolünü kullanarak haberleşme gerçekleştirmektedirler.

Okuyucu ara yüz cihazı daima başlangıç olarak T=0 protokolünü kullanır. Daha sonra cihaz ve tümleşik devre kartı arasında ardışık komut ve cevaplar gerçekleşir. Bu protokolde komut cevap çifti için veri ancak bir yönde gidebilir. Yani, veriler ya tümleşik devre kartına gelen komut mesajı içerisindedir ya da tümleşik devre kartından dönen cevap mesajı içerisindedir. Veri akışının yönü, komut tanımının içerisinde kapalı olarak bulunmaktadır. Bu yüzden de hem cihaz hem de tümleşik devre kartı daha önceden bir ön bilgi sahibi olmalıdır. Özel bir komut için her iki yönde veri akışı gerekirse, cevap verilerini almak için ilk komuttan sonra bit cevap alma komutu gönderilir[7].

T=0 iletişim protokolünün veri akışı Şekil 2.8’de belirtildiği gibi öncelikle kart okuyucu cihaz tarafından karta beş baytlık komut gönderilir, kart tarafından alınan komut prosedür baytı olarak veri işlemeye hazır olduğunu belirtir, buna karşılık olarak başlık bilgisinde P3 olarak gönderilen parametredeki veri karta gönderilir ve alınan veriyle ilgili komut işletimi gerçeklşetirildikten sonra, işlemle ilgili durum baytları kart okuyucuya gönderilir.



Şekil 2.8. T=0 protokolünün mesaj akışı[4]

T=1 asenkron, yarı çift yönlü blok aktarımı protokolü, hata yakalama ve düzeltme mekanizması dışında T=0 protokolündeki gibi çalışır. Aslında bu protokol, karakter bloklarını aşağıdaki işlemlere izin veren bir zarfın içine koyar.

T=1 protokolünün en açık avantajı her iki yönde de veri akışına izin vermesidir. T=0 protokolünde, aynı komut için veri yalnız bir yönde gitmekteydi. Aslında bu limit komutla ilgili veri uzunluğunu tek bir bayt ile tanımlamaktan kaynaklanmaktadır.

T=l protokolü, T=0 protokolündeki arayüz cihazının komutu başlattığı ve tümleşik devre kartının cevapladığı emir-komuta ilişkisini de ortadan kaldırır. Bu, blok protokolünde protokol kısıtlamalarına bağlı kalmak koşulu ile komut hem arayüz cihazı hem de tümleşik devre kartı tarafından başlatılabilir.

T=1 protokolünün başka bir avantajı da, çok uzun bir veri bloğunun, uygun sayıda çerçeve ile zincirlenerek tek bir komutta gönderilmesine izin vermesidir.

Blok protokolünün çok daha gelişmiş bir hata yönetim sistemi vardır. Burada, blok hata yakalama kodu (EDC) kullanır ve hataların oluştuğu bazı bloklar yeniden gönderilir. T=0 protokolünün hata yakalama ve düzeltme mekanizması ise çok daha basittir. Elbette daha yüksek protokol seviyesi kullanmanın bir bedeli vardır. Tümleşik devre kartı ve arayüz cihazı üzerindeki çok daha karmaşık yazılımın dışında, tümleşik devre kartı son giden bloğu, tekrar gönderme durumuna karşı, RAM belleğinde saklayabilmelidir. T=1 protokolü belli bir komutla her iki yöne de veri akışının gerektiği, büyük veri bloklarının kullanıldığı uygulamalarda daha avantajlıdır[4].

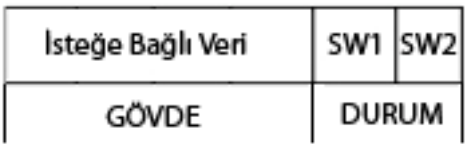
Dördüncü bölümde; kart ile okuyucu arasında bilgi aktarımı sırasında kullanılacak ortak endüstriyel komutlar belirlenir. Aslında bu komutlar üretici için temel komut setini belirler. Dördüncü bölümde belirlenen komutların işletilmesi üçüncü bölümdeki elektriksel iletişimin temellerine dayanmaktadır. Şekil 2.9'da karta gönderilecek olan komutun yapısı görülmektedir.

Şekil 2.9. Komut yapısı

Bu yapıdaki kullanılan sabitlerin açıklamaları şu şekildedir:

- CLA komutun sınıfını belirtmektedir. Gönderilecek olan komutun ISO standartından bir komut mu olacağı ya da iletişimin güvenli bir şekilde sağlanmak istediğinin belirtilmesi üzerine bir bilgidir.
- INS işletilecek olan komutu belirtmektedir.
- P1, P2 komutun içerdiği parametrelerdir.
- Lc isteğe bağlı olarak gönderilecek olan verinin boyutu belirtmektedir.
- Le kart tarafından verilecek olan cevabın uzunluğunu belirtmektedir. Eğer buradaki alan 0 ise karttan gelen tüm veri cevap olarak değerlendirilir.

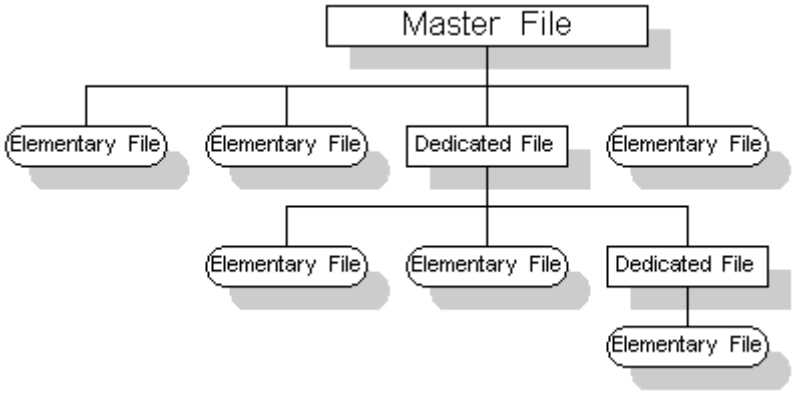
Şekil 2.10'de Karttan gelen cevap yapısı görülmektedir.



Şekil 2.10. Karttan gelen cevap yapısı

SW1, SW2 karta gönderilen komuta göre geri döndürülen mesajlar hakkında bilgi vermketedirler. Eğer komut başarılı bir şekilde işletilmişse 0x9000 cevap olarak dönmektedir.

Dördüncü bölümde kartın içerisinde yer alan veri yapısı Şekil 2.11'de görülmektedir.

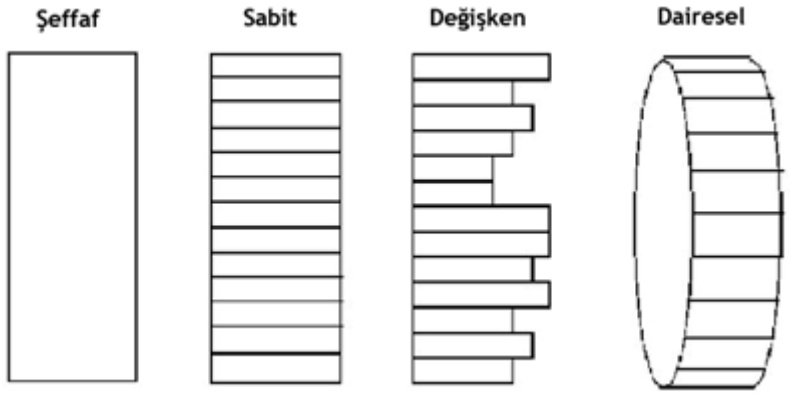


Şekil 2.11. Tümleşik devre kartı dosya yapısı [8]

Kartın içerisindeki dosya sistemi tanımlanırken günümüz işletim sistemlerinde kullanılan dosya yapısı şeklinde tasarlanmıştır. Dedicated File (DF) ve Elementary File (EF) olmak üzere iki tip dosya yapısı içermektedir. Her bir dosya yapısı 2 bayt dosya tanımlayıcısı ya da sembolik isimlerle ifade edilmektedir. EF tipindeki dosyalar sadece veri içerebilirler. Bu dosyalar oluşturulmaları sırasında maksimum dosya boyutu belirtilmelidir. DF tipindeki dosyalar işletim sistemindeki dizinlere karşılık gelmektedir. DF tipindeki dosyalar içerisinde birden fazla DF ya da EF tipinde dosya barındırabilir. Kartın içerisindeki her uygulamanın kendine ait bir DF tipi dosyası bulunmaktadır ve uygulama ile ilgili tüm işlemler bu dosya üzerinde gerçekleştirilir. Bunların dışında MF adıyla tanımlanmış bir dosya sistemin ana dosyasıdır ve belirttiğimiz DF, EF yapısındaki dosyaları içerisinde barındırmaktadır. Her kartta sadece bir tane MF yer almaktadır. Belirtilen ISO standartlarına göre MF dosyalarının tanımlayıcısı 0x3F00'dır[9].

Tanımlanmış olan bu dosyalama sisteminde 4 farklı dosya türü bulunmaktadır.

- Şeffaf
- Sabit Kayıtlı
- Değişken Kayıtlı
- Dairesel Kayıtlı



Şekil 2.12. Dosya türleri

Şekil 2.12'de tanımlanmış olan dosya türleri görülmektedir.

Şeffaf dosyalara erişirken dosya tanımlayıcısı ve dosyanın başlangıç adresi ve okunulacak olan dosyanın uzunluğu belirtilmelidir.

Sabit kayıtlı dosyalar dizilere benzetilebilir üzerinde gerçekleştirilecek olan erişim işlemleri aynı şekilde gerçekleştirilmektedir. Her kaydın kendine ait bir kayıt numarası vardır ve üzerinde işlem yapılmak istenen kayıta bu numara ile erişilir. Sabit kayıtlı dosyalarda her kaydın uzunluğu eşittir[9].

Değişen kayıtlı dosyalar uzunlukları farklı olan veri karta kaydetmek amacıyla kullanılırlar ve sadece kaydedilen verinin uzunluğu kadar yer kapsamaktadır böylece kartta yer açısından kazanç sağlanmış olur. Bu tipte dosyalar oluşturulurken kaydedilecek verinin uzunluğunun tutulması gerekmektedir. Aynı şekilde bu kayıtlara da sabit kayıtlı dosyalarda olduğu gibi kayıt numarası ile erişilir[9].

Dairesel dosyaların uzunlukları sabittir. Veri kaydı yapılacağı sırada mutlaka en son kayıttan bir sonraki alana kayıt yapılır, aynı şekilde okuma işlemi de sadece son yazılmış kaydı okuyabilir. Eğer dosyada tanımlanan sabit alan dışında yer yoksa ilk kayıtın üstüne yazma işlemi gerçekleşir. Bu tipteki dosyalar daha çok kartta gerçekleştirlen işlemlerin kaydını tutmak için kullanılır.

Kartta tanımlanan dosya sistemine erişim dört şekilde olmaktadır, bunlar :

Her zaman açık erişim (ALW) : herhangi bir kısıtlama olmaksızın dosyalara erişilebilir.

PIN1 & PIN 2 (CHV1 & CHV2): Kart sahibi tarafından bu erişim kodları doğru girildiği ya da bu kodlar iptal edildiği zaman dosyalara erişilebilir.

Yönetici (ADM) : Sadece yetkili kartın üretici firması tarafından yapılabilmektedir.

Hiçbir zaman (NEV) : Hiçbir şekilde karttaki dosyalara erişilememektedir.

PIN kodu ile korunan dosya sistemine erişilmek istendiği zaman kart üzerinde PIN doğru girilmediği zaman maksimum deneme sayısını azaltan bir mekanizma bulunmaktadır. Maksimum deneme sayısı aşıldığı zaman; karttaki deneme sayısını sayan sayaç 0'a eşit olduğu zaman PIN kodu bloke olur. Bu blokeyi ortadan kaldırmak için bir PIN koduna ihtiyaç vardır. Bu kod da maksimum deneme sayısınca yanlış girildiği zaman kart bloke olur ve kullanılamaz hale gelir. Bu adımdan sonra kartın içerisindeki verilere hiçbir şekilde erişilememektedir[9].

PIN kodu her doğru girildiğinde ise deneme sayısını tutan sayaç ilk konuma (örnek olarak eğer bu deneme sayısı 3 ise 3'e) getirilir.

PIN kodları kartın içerisinde EF_{CHV1} ve EF_{CHV2} dosyalarında tutulmaktadır.

ISO 7816 standartının dördüncü kısmında tanımlanan komutlar şu şekildedir:

- Select_File
- Read_Binary
- Write Binary
- Update Binary
- Erase_Binary
- Read_Records
- Write Records
- Log Records
- Update Records
- Get_Data
- Put_Data

- Verify
- Internal_Authenticate
- External_Authenticate
- Get_Challenge
- Manage Channel
- Get_Response
- Envelope

Bu komutlar komutlarnın nasıl işletileceğinin gösterildiği Şekil 2.9 ve Şekil 2.10'da yer almaktadır.

Beşinci bölümde; uluslararası uygulama numaralandırma sistemi ve özel uygulamaların kayıt edilme yöntemini de belirleyen kayıt prosedürü belirtilmektedir. Akıllı kartlar üzerinde işletim sistemi çalıştırabilmektedir. Çalışan bu işletim sisteminde kart üzerinde uygulamalar da çalışmaktadır. Çalışan bu uygulamların her birinin tekil uygulama işlem numarası bulunmaktadır. Kullanılan uygulama işlem numaraları bu bölümdeki standartlara göre belirlenmektedir. Tek uygulamalarda, örneğin kredi kartı gibi, uygulama tanımlama numaraları içerir. Bu kredi kartı numarası olabilir ve bunlara uygulanacak işlemlerin kuralları belirlenir[4].

Aslında bu bölüm bugünün tek uygulamalı kartları için pek bir anlam ifade etmez. Fakat ileride üzerinde birden çok uygulama bulunan kartlar kullanılmaya başlandığında, kart okuyucu uygulama tanımlama numarasını kullanarak, hangi uygulamanın çalıştığını anlayabilecektir (Örneğin, sağlık uygulamaları, sağlık tanımlama numarasına ve üzerinde para saklanan kredi kartı gibi finansal uygulamalar da kendi tanımlama numaralarına sahip olacaklardır).

Altıncı bölümde; akıllı kartlar tarafından kullanılabilecek veri elemanları (isim şifre, son kullanma tarihi, adres bilgisi, vb.) belirtilmiştir. Bu veri elemanları, temel komut setinin çeşitli komutlarında önemli rol oynamaktadır. Yani bu bölüm dördüncü bölümde belirlenen komutların çok basit bir veri sözlüğü olarak tanımlanabilir[13].

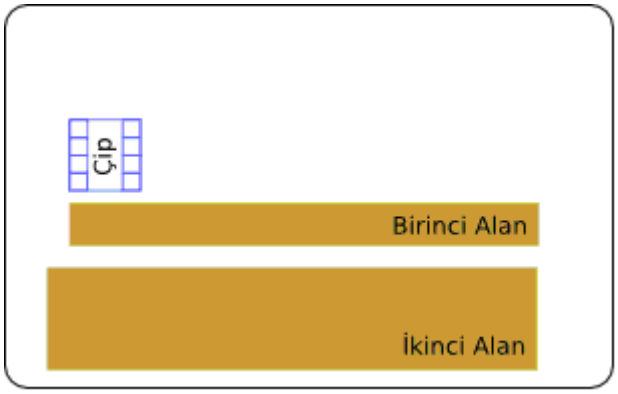
Yedinci bölüm; henüz geliştirilmektedir ve güvenlik mimarisi ile ileri seviyedeki komutları konu almaktadır.

2.3. Kimlik Kartlarının Fiziksel Yapısı

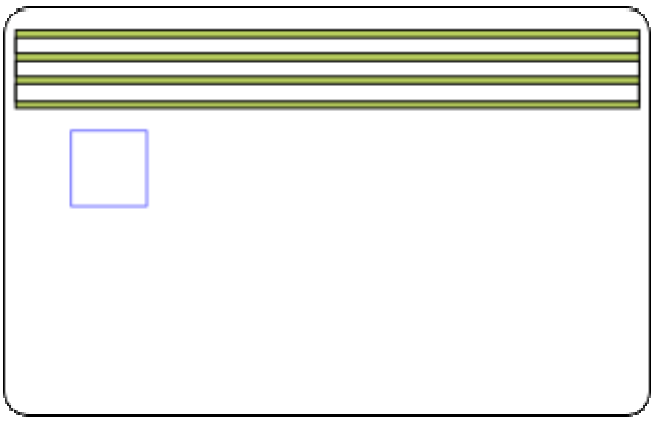
Kimlik kartlarında iki tip boyut kullanılmaktadır. Bunlardan birincisi; tüm bankacılık işlemlerinde, kimlik kartı, telefon kartı yerine de kullanılan ID-1 diğeri ise ID-1'den türeilmiş olan ve cep telefonlarından kullanılan ID-000'dır.

2.3.1. Boyutlar

Temel kart biçimi ve boyutu ISO 7810 standartında tanımlanan ID-1'dir. Bu manyetik ve çipli tüm kredi kartlarının uyduğu ortak boyut olup Şekil 2.13 ön, Şekil 2.14 akıllı kartların arka yüz görünümünü göstermektedir.



Şekil 2.13. Akıllı kart ön yüz görünümü[12]

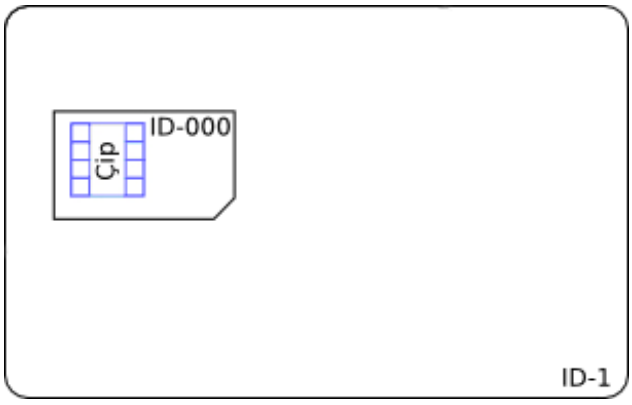


Şekil 2.14. Akıllı kart arka yüz görünümü[12]

Şekil 2.13'te kartın ön yüzünde görülen birinci alan kabartma olarak kart numarası için ayrılmıştır. İkinci alan ise yine kabartma olarak kart sahibine ilişkin isim, adres, son kullanma tarihi bilgileri içindir[14].

Şekil 2.14'de görülen arka yüzdeki manyetik şerit, üç ayrı iz halinde ayrılmıştır. İlk iki iz okunabilir, üçüncü iz ise hem okunabilir hem yazılabilir bilgi taşır. Bu izlere yazılacak olan bilgiler ISO 7813 Finansal İşlem Kartları standartında belirtilmiştir. Manyetik şeritin kapasitesi 1000 bit civarında olmakla birlikte, kabartmalardaki bilgileri taşımak için fazlasıyla yeterlidir.

Bu kart boyutunun cep telefonları için büyük kalması nedeniyle GSM kartları için ID-000 adlı daha ufak bir biçim de standartlaştırılmıştır. ID-1 boyutundaki temaslı çip kartları kesilerek mini boyuttaki kartlar elde edilebilir[4].



Şekil 2.15. Iso 7810 standartında tanımlanan kart tipleri

BÖLÜM 3. AKILLI KARTLAR VE AKILLI KARTLARDA GÜVENLİK

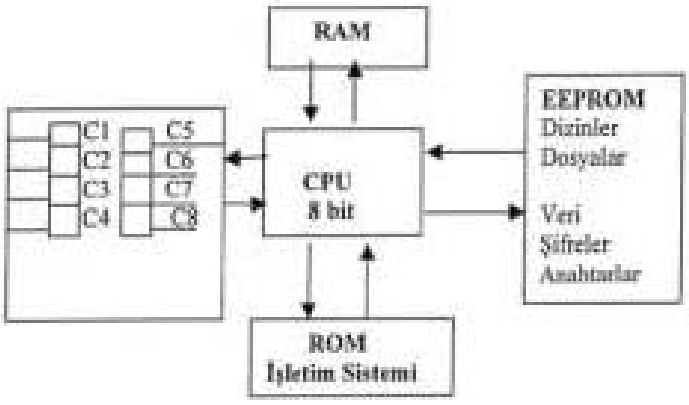
Akıllı kartlar günlük hayatta sıklıkla kullanılan manyetik şeritli kartlara benzemekle birlikte veri depolama, kendine özgü işletim komutlarını işletebilmesi özellikleriyle de manyetik kartlardan farklıdır. Veri depolama ve işletim komutlarını işletebilme özelliklerini içinde barındırdığı CPU, RAM, ROM ve EEPROM'lar aracılığıyla gerçekleştirmektedir. Bu yapısıyla akıllı kartlar küçük bir bilgisayar gibi çalışırlar.

Akıllı kartlar farklı hafıza kapasitesi ve teknik özelliklerine göre çeşitli uygulama alanlarında kullanılmaktadırlar. Manyetik şeritli kartlar ile karşılaştırıldığında, akıllı kartlar yüzlerce defa daha yüksek kapasiteye sahiptir, daha dayanıklıdır ve ileri derecede şifreleme gibi mekanizmalar nedeniyle çok daha güvenlidir. Karta kaydedilen verinin şifrelenerek güvenliği sağlanır. Bu sayede yetkisiz kişilerce kartta bulunan verilerin okunması, silinmesi ve değiştirilmesi engellenmiş olur. Akıllı kartların sağladığı en önemli avantajlar taşınabilirlik ve sağladığı üstün güvenlik özellikleridir. Kişiye ait kimlik işlemlerinde kullandığı gizli bilgiler kartta güvenli bir şekilde depolanabilmektedir. En önemli özelliklerinden birisi de içindeki bilgilerin kopyalanamamasıdır. Kredi kartlarındaki manyetik şerit kopyalanabilir ve bilgiler kullanılabilirken akıllı kart tabanlı kredi kartlarında kopyalama gibi bir işlemin yapılması mümkün değildir[15].

Akıllı kartlar güvenlik seviyerleri ve erişim yetkilerinin tasarlandığı bir sistemde kapıyı açmak için gerekli bilgiyi depolayabilir, bu bilgi ile kullanıcı kendi bilgisayarında oturum açabilir ya da aynı şekilde bu bilgi ile alışveriş yaparken ödeme yapabilir. Aynı şekilde internet bankacılığı sistemlerinde kişi kimliğinin doğrulanması esnasında kişi kartta bulunan kendi özel anahtarını kullanabilir, bu yöntem günümüzde kullanılan şifre ile kimlik doğrulama işlemlerinden daha güvenlidir.

3.1. Akıllı Kart Mimarisi

Akıllı kartlarda bulunan mikrodenetleyici; yapısında mikroişlemci(CPU), yalnızca okunabilir bellek(ROM), elektiriksel olarak silinebilir programlanabilir yalnızca okunabilir bellek(EEPROM) ve rastgele erişimli bellek(RAM)'ten oluşmaktadır. Bu birimler Şekil 3.1'de görülmektedir. Buradaki elemanlardan CPU genellikle 8 bittir, daha yüksek kapasiteli işlemler için 16-32 bitlik CPU'lar da mevcuttur. Bu CPU'nun yanında şifreleme işlemlerinin performansını yükselten kriptografik mikroişlemciler vardır. ROM içerisindeki bilgiler kartın işletim sistemini içermektedir ve bu bilgiler kartın üretimi sırasında karta yazılmaktadır. İşletim sisteminin dışında karta özel uygulamalar da yazılabilmektedir. EEPROM karta tutulması planlanan bilgilerin depolanması içindir. Sabit disk gibi kullanılan bu birim buraya kartın sahibiyle ilgili şifreler, anahtarlar bulunabilir. Aynı zamanda kartın kullanılmak üzere tasarlandığı sistemle ilgili dosyalar, dizinler de burada tutulmaktadır. RAM üzerindeki veriler yalnıza kart okuyucuya takıldığı zaman yazılmaktadır. Buraya yazılan veriler işletim sistemi tarafından organize edilmektedir. Kart okuyucudan çıkarıldığı zaman veriler silinmektedir.



Şekil 3.1. Akıllı kart mimarisi[4]

3.2. Akıllı Kartların Sağladığı Faydalar

Akıllı kartların, veriyi saklama ve işleme özelliklerinin yam sıra güvenlik ve taşınabilmeleri önemli avantajlar sağlamaktadır. Mikroişlemci, bellek ve giriş/çıkış birimleri tek bir entegre devre olarak plastik karta monte edilmiştir. Bu nedenle, dış kaynaklara bağlı zararlara karşı dayanıklıdır.

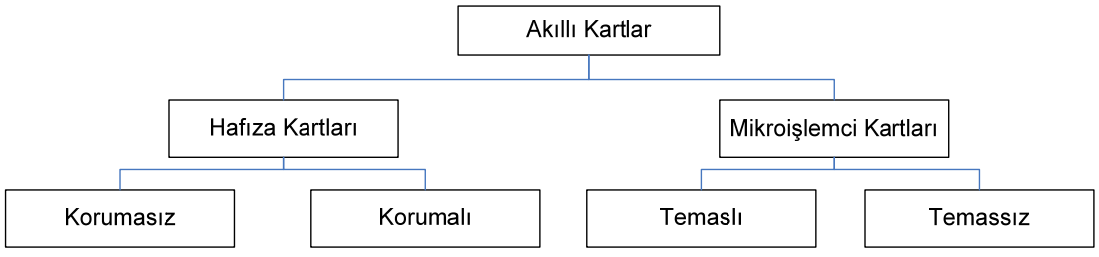
Kart içerisinde saklı olan veriyi okumak için, kart okuyucu cihaza ihtiyaç duyulmaktadır. Akıllı kart yazılım ve donanımı hakkında bilgi sahibi olma şartı da güvenliği arttırmaktadır. Aynca kart üzerindeki veriler şifreli olarak saklanabilir ve kart okuyucu ile kart arasındaki iletişim şifreli gerçekleştirilebilir. Şifreli erişim sayesinde yetkisiz kişilerin karttaki verileri okuması, silmesi ve değiştirmesi engellenmiş olmaktadır.

Akıllı kart kullanıcılarının fiziksel ve elektronik sistemlere erişimini denetler, kişiye ait dijital imza, biyometrik veriler, PIN bilgisini bulundurarak, kart kimliğini doğrulamayı kolaylaştırmaktadır. Kullanıcı, birden fazla şifre hatırlayıp, formlar doldurmak zorunda değildir.

Dijital kimlik sağladığı için kullanıcının birden fazla kart taşıyıp bu kartlara ait kullanıcı bilgisi, şifre bilgisi hatırlanması gerekliliğini ortadan kaldırmaktadır.

3.3. Akıllı Kart Çeşitleri

Akıllı kart çeşitleri hafıza kartları ve mikro işlemcili kartlar olmak üzere ikiye ayrılmaktadır. Bu kartlar da kendi arasında ikiye ayrılırlar[20]. Şekil 3.2'de kartların sınıflandırılması gösterilmektedir.



Şekil 3.2. Akıllı kartların sınıflandırılması

3.3.1. Hafıza kartları

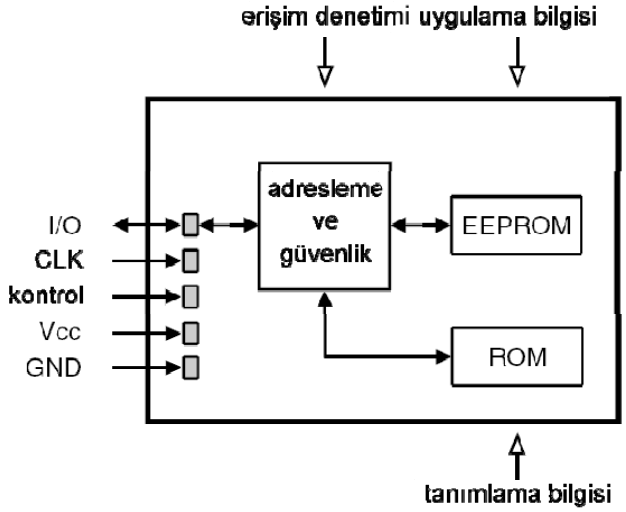
İlk akıllı kartlar telefon kartları olarak kullanılmak üzere tasarlamış hafıza kartlarıdır. Bu kartlar; kart her kullanıldığında telefon makinesi tarafından içerisindeki krediden azaltma yapacak şekilde tasarlanmıştır. Aynı zamanda kullanıcının manyetik şeritli

kartlarda uygulanan kopyalama işlemine bağlı olarak kartın içerisinden kredi bilgisini arttırması işleminden korunması gerekmektedir. Hafıza kartlarında çipin içindeki verinin kopyalanması ve kullanıldıktan sonra tekrar geri yazılması işlemi mümkün değildir. Hafıza kartlarının tek kötü yanı içerisindeki kredi verisi sıfırlanınca tekrar kullanılamamasıdır[20].

Hafıza kartlarının yüksek dosya işleme kapasiteleri yoktur. Bu tip kartlara, sadece veri yazma ve okuma işlemi yapılabilir. Kart üzerinde mikroişlemci ve EEPROM (Electrically Erasable Programmable Read Only Memory-Elektriksel Silinebilir Programlanabilir Sadece Okunur Bellek) bellek bulunur. Kapasiteleri 1 Kb ile 4 Kb arasında değişmektedir. Ucuz maliyetinden dolayı telefon kartı olarak kullanılması dışında basit olarak sadece kimlik doğrulama gereken uygulamalarda da tercih edilmektedirler. Şifre korumalı hafıza kartları içindeki verinin değiştirilmesi ya da dışarıdan yapılacak olan müdahalelerle değiştirilmesini engellemektedir.

Bellek kartları bazen senkron kartlar olarak da anılırlar. Çünkü bu kartlarla terminaller arasındaki iletişim sırasında bütün kontrol terminaldedir. Mikroişlemcili kartlar ise asenkron kartlardır ve bu kartlar bir dizi işlemi yapıp bitirdiklerinde sonuçları terminale gönderirler.

Şekil 3.3'te kartın veri iletişim bilgisi ve elektriksel elemanları görülmektedir.



Şekil 3.3. Hafıza kartının yapısı ve veri iletişim bilgisi[18]

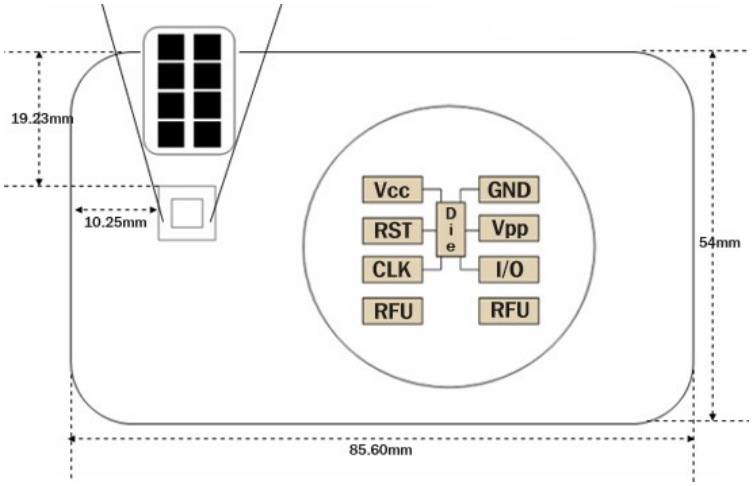
Hafıza kartlarındaki uygulamalarda kullanılacak olan veriler EEPROM'a yazılmaktadır. Verinin değiştirilmesi ya da silinmesine karşı erişim güvenlik sistemi

tarafından belirli adreslere yazdığı erişim denetimleri aracılığıyla korunmaktadır. Bu basit sistemden farklı olarak bazı hafıza kartları verinin şifrelenmesini gerçekleştirebilen daha karmaşık güvenlik sistemleri içermektedirler. Şekilden de görüldüğü gibi hafıza kartları mikroişlemcili akıllı kartlardan farklı olarak işlemciye sahip değillerdir ve işlem yapabilme kapasiteleri sınırlıdır. ROM sadece karta yüklenmiş olan bir uygulamayı çalıştırır ve EEPROM'daki uygulama ile ilgili bilgilere erişir[18].

3.3.2. Mikroişlemcili kartlar

Üzerinde işletim sistemi bulunan mikroişlemciye sahip kartlardır. Bu tip kartlar, belleklerinde bulunan veri üzerinde işlem yapabilirler. SIM kartları ve kredi kartları mikroişlemcili kartlara örnek gösterilebilir.

Temel olarak mikroişlemcili bir akıllı kart; CPU (Central Processing Unit-Merkezi İşlem Birimi), ROM (Read Only Memory-Sadece Okunabilir Bellek), RAM (Random Access Memory-Rastgele Erişilebilir Bellek) ve EEPROM(Electrically Erasable Programmable Read-Only Memory-Elektriksel Silinebilir Programlanabilir Sadece Okunabilir Bellek) bileşenlerinden oluşmaktadır[16]. Kartlar 8, 16 veya 32 bitlik mikroişlemci içerirler, genellikle maliyet açısından 8 biltlik mikroişlemciler tercih edilmektedir. ROM bellek içerisinde, kart işletim sistemi, kalıcı uygulamalar ile kartın tekil bilgileri bulunur. Bu belleğe bilgiler üretici firma tarafından üretim işlemleri sırasında yazılır. Daha sonra bellek içerisinde bulunan bilgiler değiştirilemez. Kart işletim sistemi ve karta sonradan yüklenen uygulamalar ise RAM bellek üzerinde çalışır. Geçici çalışma alanıdır. Bu bellekte bulunan bilgiler kartın enerjisi kesildiğinde kaybolur. EEPROM bellek ise kartta saklanacak veriler için kullanılır. EEPROM üzerinde veri yazma, değiştirme ve okuma işlemleri yapılabilir. Kartın enerjisi kesildiğinde EEPROM içindeki veriler kaybolmaz[5].



Şekil 3.4. Mikroişlemcili akıllı kart[21]

Temassız Akıllı kartlar, kart okuyucu ile iletişim için fiziksel temasa ihtiyaç duymazlar. Kart okuyucu belli bir mesafe yaklaştırıldığında, çalışması için gerekli olan enerji ve veri aktarımı kablosuz olarak radyo frekanslarıyla gerçekleşmektedir. Kart okuyucu ve akıllı kart birer antene sahiptirler. Kartta bulunan anten sayesinde kartın her iki tarafı da kullanılabilir. Bu kartların 10 cm altında çalışan ve 1 metreye kadar uzak mesafeden çalışan tipleri mevcuttur.

Şekil 3.5. Temassız akıllı kart yapısı[16]

Temassız akıllı kart, plastik bir kart içerisine yerleştirilmiş tümleşik devre ve tel antenden oluşmaktadır. Çalışmaya başlanması için temassız akıllı kartın, okuyucu etkili manyetik alanına girmesi gerekmektedir. Kart okuyucu ile bağlantı kurulduğunda gerekli olan güç ve haberleşmeyi radyo frekans arayüzü sağlar, temassız akıllı kartların RFID kartlar bu özellikleri sebebiyle adlandırılmaktadırlar[16].

ISO/IEC 14443 ve ISO/IEC 15693 standartlan ile temassız akıllı kartlarda uygulanacak olan standartlar belirlenmiştir. Bu standartlar kartın fiziksel özellikleri, RF arayüzü, iletişim protokolleri gibi özellikleri içermektedir.

Ulaşım, personel giriş-çıkış kontrolü ve güvenlik sistemlerinde yaygın olarak kullanılmaktadırlar.

Temassız akıllı kartların temaslı akıllı kartlara gore avantajlan şunlardır:

- Uzun kullanım süresi
- Kolay kullanım
- Daha az yıpranma ve aşınma.

Bu avantajlarının yanısıra dezavantajları ise şöyle sıralanabilir:

- Uzun işlem süresi
- İletişim problemleri
- Taklit edilebilme problemleri

3.4. Akıllı Kartların Uygulama Alanları

Akıllı kartlar günümüzde birçok alanda uygulama ve kullanım alanı bulmaktadırlar. Akıllı kartların en çok kullanıldıklan alanlar şunlardır:

Finans: Akıllı kartlar, bankacılık sistemlerinde yaygın olarak kullanılmaktadır. Finans sektörü, ilk uygulama ve kullanım alanlanndandır. Bankacılık sistemlerinde kullanılan kredi kartları, e-cüzdan uygulamalan ile farklı sektörlerde para dolaşımı işlemlerinde kullanılmaktadır[16].

Telekomünükasyon: Akıllı kartların en fazla kullanıldığı sektördür. Akıllı kartların yaygınlaşmasında, telekomünikasyon sektöründe kullanılmasının büyük önemi vardır. Cep telefonlannda kullanılan SIM kartlar birer akıllı karttır. SIM kartları, abonenin, kablosuz şebekeye girişinde tanınmasını sağlayan kişisel bilgiler içerir. GSM operatörü, bu şekilde abonelerini takip ederek daha iyi hizmet verebilir[16].

Sağlık: Birçok ülkede sağlık sistemlerinde akıllı kartlar kullanılmaktadır. Kişilere verilen akıllı kartlar sayesinde, sağlık bilgilerine sağlık personeli tarafından anında ulaşılmaktadır. Sağlık akıllı kartları içinde kişilerin özlük bilgileri, geçirdiği hastalıklar, gördüğü tedaviler, kullandığı ilaçlar ve alerjik tepkileri gibi bilgiler bulunmaktadır. Tüm bu veriler değerlendirilerek hastanın daha etkili ve kısa sürede iyileşmesine yönelik tedavi yöntemlerinin geliştirilebilmektedir[16].

Ulaşım: Toplu taşıma sistemlerinde en önemli problem, taşıma hizmeti için alınacak ücretin alınma şekli ve toplu taşıma araçlarının kontrolüdür. Günümüze kadar taşıma sistemlerinin ücretlendirilmesinde bilet, jeton, paso ve abonman kartları kullanılmıştır. Toplu taşıma sistemlerinde akıllı kartların kullanılması ile birlikte, yukanda belirtilen problemler çözüme kavuşmuştur. Araçlara konulan kart okuyucu cihazlar, kartın uzaktan gösterilmesi ile kartla iletişim kurduklanndan, yolcuların ödeme yapma işlemleri hızlanmıştır. Aynca kişiler, her defasında bilet almak zorunluluğundan kurtulmuşlardır. Kişiler kartlarını istedikleri bir ortamdan doldurabilmektedirler. Bu uygulamanın dışında karayollarında kullanılmakta olan OGS(Otomatik Geçis Sistemi) ve KGS(Kartlı Geçis Sistemi) bu uygulamalara örnek olarak gösterilebilir. Kişi otoyoldan aldığı hizmetin karşılığını anında hesabından düşmektedir.

Kimlik: Nüfus, okul, müşteri, spor kulübü gibi alanlarda kullanılan kimlikler yerine akıllı kartlar kullanımı hızla yaygınlaşmaktadır. Nüfus kartları, ehliyetler, sağlık kartları, ruhsatlar ve pasaportlar dünyanın birçok ülkesinde eski formalarından akıllı kartlara geçişe başlamış durumdadır. Akıllı kartların kullanımı sayesinde, bilgilere hızlı, güvenli ve kolay erişim sağlandığı gibi formaliteleri, hatalı ve usulsüz işlemleri en aza indirmek mümkün olmaktadır[16].

Trafik: Kişiye verilen akıllı kartlı sürücü belgesi sayesinde, sürücünün bilgilerine anında ulaşılmaktadır. Kişinin daha önce işlemiş olduğu trafik suçlarına erişilebilmektedir. Ruhsatın yerine akıllı kart kullanılarak, araç ile ilgili bilgilere ulaşma ve işlem yapma daha hızlı ve güvenli hale gelir. Aracın çalıntı olup olmadığı, muayene süresinin dolup dolmadığı, üzerinde tahdit bulunup bulunmadığı gibi bilgilerin kontrolü de kolaylaşmaktadır[16].

3.5. Akıllı Kartlarda Güvenlik

Yerel bir bilgisayardaki kullanıcının, karşılıklı olarak yapılan bir görüşmede karşı taraftaki kişinin ya da mesajın gerçekten gönderen kişinin kimliğinin doğrulanması bilgisayar dünyasında süregelen sorunların başında gelmektedir. Akıllı kartlar içerdikleri kriptografik işlem yetenekleri sayesinde bu sorununun çözümünde çok önemli bir paya sahiptirler.

Akıllı kart, kaynaklara erişim izni vermeden önce kiminle iletişim kurduğunu anlamak zorundadır. Benzer şekilde, diğer elemanlar tarafından kabul edilmeden önce de kendisinin kim olduğunu ispatlaması gerekir. Bu sebepledir ki akıllı kartın aktif hale getirildikten sonra öncelikli olarak gerçekleştireceği görevlerden biri diğer sistem elemanlarına kendini doğrulamasıdır. Bunlar öncelikli olarak kartı terminale yerleştiren insanla terminal arasındaki doğrulama, daha sonra ise Kartın diğer tüm varlıklarla arasındaki tanımlama ve doğrulama işlemleridir.

Kimlik denetimi, kimi zaman önceden belirlenmiş bir 4 haneli PIN gösterimi olabileceği gibi karşı taraftan gelen şifrelenmiş bir mesajı, belli bir anahtar, algoritma ya da önceden tanımlanmış işlem protokolü kullanıp anlayabileceği hale getirme gibi karmaşık bir işlem de olabilir. Bu kimlik denetimi sırasında herhangi bir noktada, bir varlık olması gerekenden farklı davranışlar sergilerse, o varlıkla o aşamadan sonra yapılacak olan tüm iletişimler engellenir. Bu başarısız girişimleri her biri, belli bir sayıya ulaştığında kaynaklara erişimin kısıtlanması ya da sonraki tüm işlemlerin engellenmesi amacıyla akıllı kartta depolanabilir.

Akıllı kartlara önerilebilecek alternatif kimlik doğrulama ve güvenli iletişim için çözüm yöntemleri şifrelere ya da şifreler yerine kullanılabilecek birden çok kelimelere dayanmaktadır. Şifrelere internet bankacılığında kullanılan parolalar, şifre kelimelerine de parolanın yanında önceden müşterinin tanımlamış olduğu bilgileri girmesi istenmektedir. Bu şifreler yetkisiz kişiler tarafından ele geçirilebilir ya da güvensiz bir şekilde yazı ile başka bir kişiye iletilebilir. Bu sebeplerden dolayı akıllı kartlar kimlik doğrulama ve güvenli iletişim için doğru tercihtirler.

Akıllı kartlardaki güvenli iletişimin sağlanması kriptografinin getirdiği şifreleme algoritmalarına dayalıdır.

Kriptografi mesajların güvenliğini sağlayan bilim dalıdır. Kısaca mesajların güvenliğini sağlamak için içeriklerinin alıcı haricindekilerin anlamayacağı şekilde sistematik olarak bozulması yani şifrelenmesi ve yine aynı şekilde şifre çözme işlemiyle yeniden elde edilmesini amaçlamaktır[28].

Kriptografi sadece mesajların şifrelenmesi ve şifre çözümünden ibaret değildir. Aynı zamanda bilgi güvenliğine ihtiyaç duyulan gerçek dünya problemlerinin çözümüyle de uğraşmaktadır. Kriptografinin 4 ana nesnesi vardır[6]

3.5.1. Veri bütünlüğü

Veri bütünlüğü, bilginin bir hile ve bozulma olmaksızın iletimini sağlamaktadır. Alıcı, vericinin gönderdiği mesajı değişmeden alındığından emin olmalıdır. Veri doğrulama işlemi bilginin bir özet fonksiyon kullanılarak metni tanımlayan imzasının çıkarılması işlemidir. Bir anlam bütünlüğü içermeyen ve rasgele seçilmiş sayılar görüntüsü yaratan bu çıktı bilgiye özeldir. Gönderen tarafaından mesajın imzası çıkarılır ve mesaja eklenir. Alıcı gönderenin hangi fonksiyonu kullanarak bu işlemi gerçekleştirdiğini bilir ve aynı işlemi o da uygular eğer çıkan sonuç alıcıdan gelen imza ile aynı ise veri bütünlüğü doğrulanmış olur aksi takdirde bilginin değiştiği varsayılır ve mesaj kabul edilmez[22].

MD5, SHA-1 gibi tek yönlü çalışan verilen metnin imzasını çıkaran çeşitli veri bütünlüğünü doğrulayan algoritmalar olmasına rağmen genellikle akıllı kartlarda elektronik olarak verideki kontrol bitlerinin kontrol edilmesiyle veya MAC(Message Authentication Code-Mesaj Doğrulama Kodu) algoritması kullanılarak veri bütünlüğü sağlanmaktadır[9].

3.5.1.1. Onaylama

Bazı uygulamalarda alıcı sadece belirli bir vericiden mesaj aldığından emin olmak ister. Bu işlem fiziksel olarak bir dökümanı imzalamaya benzemektedir. İmza tektir. Sayısal imza taranmış bir kelime olup herhangi bir dokümana yerleştirilebilir. Bu işlem iki anahtar gerçekleştirilerek gerçekleştirilir. Kişideki herkese açık anahtar ile mesaj imzalanır ve alıcı mesajı açık anahtarı kullanarak kullnıcının kimliğini

doğrular. Akıllı kartlarda onaylama işlemi için kullanılan yöntem MAC algoritmasıdır. Bu algoritma aynı zamanda veriyi şifrelemede de kullanılmaktadır[9].

3.5.1.2. Red Edilmeme

Kullanıcı gönderilen verinin kendisi tarafından gönderilmediğini iddia edemez. Akıllı kartlara kullanıcının kimlik bilgileri kullanılarak elektronik imzası yazılmaktadır. Bir kez kişi kartını kullanarak imzalama işlemi gerçekleştirmişse kesinlikle imzanın red edilmesi gibi bir durum söz konusu olmamaktadır. Çünkü bu imza yetkili kuruluşlar tarafından sorgulanarak kişinin kimliği tescil edilmektedir ve imzanın geçerliliği doğrulanmaktadır[22].

3.5.1.3. Gizlilik

Gizlilik, kriptografik teknikler kullanılarak onay verilmemiş girişimlere karşı bilginin korunmasıdır. Dışarıdan birisi alıcı ve verici arasındaki haberleşmeyi dinlememelidir. Dinlediği takdirde eline geçireceği veriler şifrelendiği için bu verileri kullanması mümkün olmamalıdır. Bu işlem için şifreleme yöntemleri kullanılmaktadır.

3.5.2. Akıllı kartlarda kullanılan şifreleme algoritmaları

Şifreleme yöntemleri simetrik ve asimetrik olmak üzere ikiye ayrılmaktadır[23]. Simetrik algoritmalarda şifreleme ve şifre çözme işlemi için aynı anahtar kullanılırken; asimetrik algoritmalarda şifreleme için farklı bir anahtar çözme işlemi için ise farklı bir anahtar kullanılmaktadır[23]. Şifreleme işlemlerinde kullanılan anahtarlar karttaki dosyalarda saklanmakta, algoritma ve protokoller ise kartta bulunan yazılımlara entegre edilmiştir.

Şifreleme akıllı karttan dışarıya ya da dışarıdan karta doğru yapılacak olan tüm mesaj trafiğine uygulanabileceği gibi sadece belli mesajlara da uygulanabilir. Eğer akıllı kart aynı anda iki uygulamayla iletişim içerisindeyse, bu uygulamaların her ikisi için ayrı şifreleme anahtarları kullanabilir.

Akıllı kart uygulama geliştiricileri yeni kimlik denetim ya da şifreleme algoritmaları tasarlamak zorunda değillerdir. Bunun yerine, akıllı kartın üzerinde hali hazırda bulunan fonksiyonları kullanabilirler. Bunlar, önceden denetlenmiş ve belli bir doğruluk seviyesinde çalıştığı ispatlanmış olanlardır. Yeni algoritmaların tasarlanması kolay olmadığı gibi, doğruluklarının ispatı da uygulama geliştiricileri tarafından tercih edilmemektedir.

3.5.2.1. DES veri şifreleme standartı (data encryption standard)

1974'de IBM'in NSA ile birlikte işbirliği ile geliştirilen Veri Şifreleme Standartı DES dünyada yaygın olarak kullanılan bir şifreleme standartı olmuştur. Şifreleme piyasasındaki yaygınlığından dolayı DES farklı şifreleme cihazları arasındaki mükemmel bir standarttır[23].

DES karıştırma ve yayılma şifreleme tekniğine dayanır. Karıştırma yer değiştirme ile başarılır. Özellikle verinin seçilen bölgeleri orjinal veriden takip eden bölgeler ile yer değiştirilir. Yer değiştirilen verinin seçimi anahtara ve orjinal sade metne bağlıdır. Yayılma permütasyon ile başarılır. Farklı kısımların sırası yeniden düzenlenerek veri değiş tokuş edilir. Bu permutasyonlar, yerdeğiştirmeye benzer şekilde, anahtar ve orjinal yalın metne bağlıdır. Yerdeğiştirmeler ve permütasyonlar DES algoritması tarafından belirlenir[23].

DES, 16 döngüye sahip 56-bit anahtar (K), kullanarak 64-bit bloklar üzerinde şifreleme yapan bir şifreleme algoritmasıdır. 16 döngülük şifreleme işlemi yapmadan önce açık metne $IP(x) = L^0R^0$ (x açık metin) olacak şekilde başlangıç permütasyonu IP (initial permutation) uygulanır. 16 döngü şifreleme işleminden sonra ters permütasyon IP^{-1} $y = IP^{-1}(R^{16}L^{16})$ olacak (y şifreli metin) şekilde uygulanır[23].

Döngü fonksiyonu *g* aşağıdaki yapıya sahiptir:

$$g(L^{i-1}, R^{i-1}, K^i) = (L^i, R^i)$$
$$L^i = R^{i-1}$$
$$R^i = L^{i-1} \oplus f(R^{i-1}, K^i)$$

Her L^i ve R^i 32 bit uzunluğundadır ve fonksiyon f tanımlamasında gösterildiği gibi 32-bit uzunluğunda o anki durumun sağ yarısını ve döngü anahtarını giriş olarak alır ve 32-bit değer üretir[23].

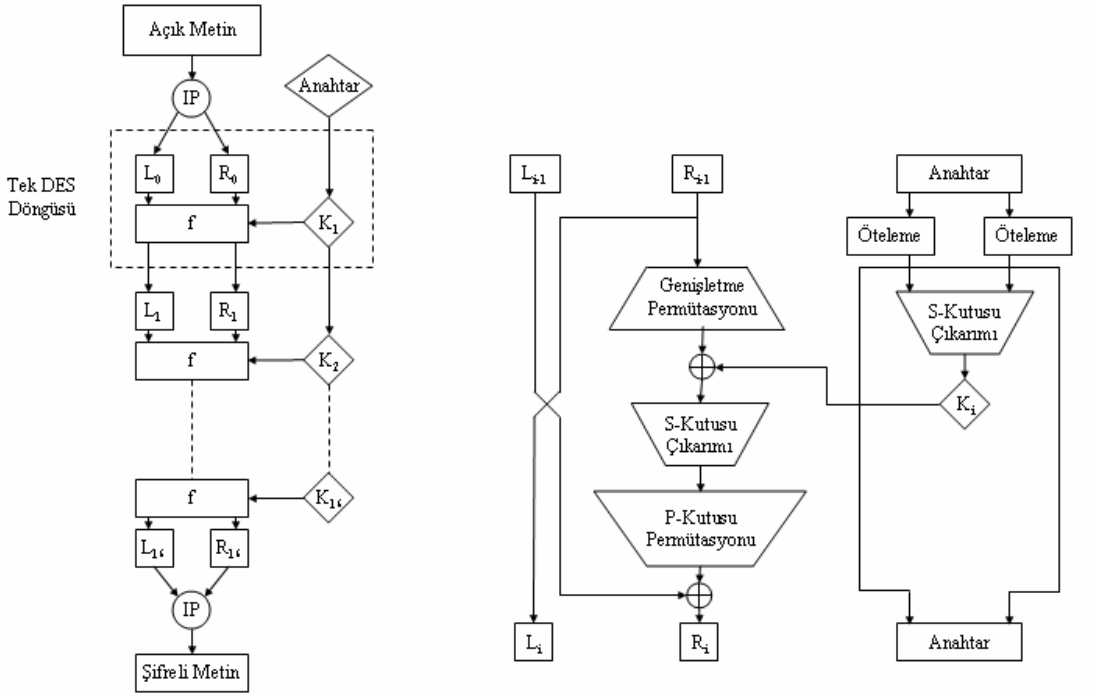
$$f : \{0,1\}^{32} x \{0,1\}^{48} \rightarrow \{0,1\}^{32}$$

Anahtar planlama, $(K^1, K^2, ..., K^{16})$, 56-bit ana anahtardan elde edilen 48-bit döngü anahtarları içerir. DES fonksiyonu f 'in çalışması da aşağıdaki gibi özetlenebilir:

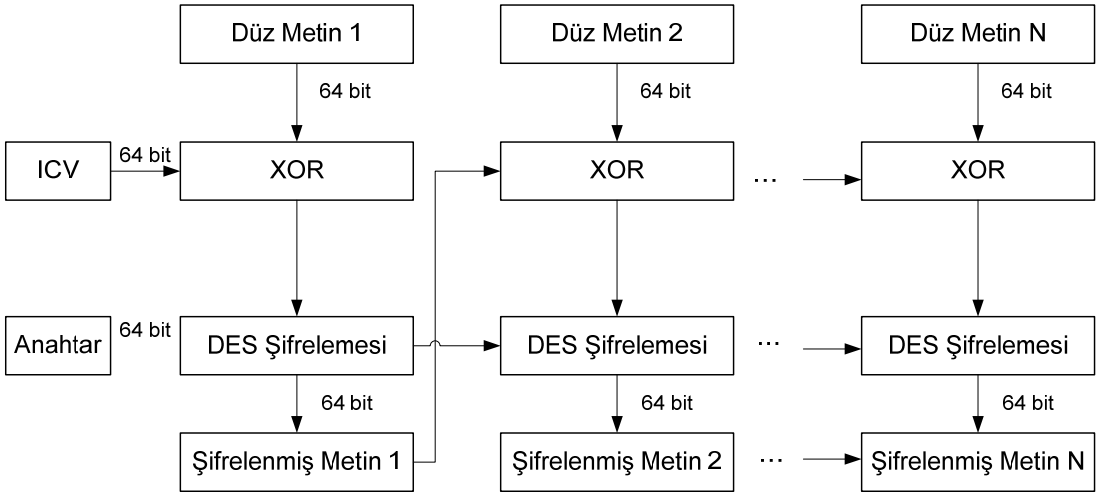
- 32-bit gelen veri 48-bit olacak şekilde genişletme permütasyonuna sokulur.
- Üretilen 48-bit değer ile anahtar planlamadan gelen o döngü için elde edilen 48-bit anahtar ile XOR'lanır.
- Diğer adımda $S_i : \{0,1\}^6 \rightarrow \{0,1\}^4$ şeklinde tanımlanan 8 kutusuna bu elde edilen 48- bit değer giriş olarak kullanılır.
- Elde edilen 32-bit değer 32-bit'lik bir P permütasyonuna sokularak 32-bit uzunluğunda yeni bir bit dizisi elde edilir.

Şekil 3.6 DES algoritmasını ve tek döngülük şifreleme işlemini göstermektedir. DES algoritmasının çalışması aşağıdaki gibi özetlenebilir:

- 56-bit anahtardan 48-bitlik $(K^1, K^2, ..., K^{16})$ olmak üzere 16 adet anahtar üret.
- 64-bit açık metni (x) başlangıç permütasyonuna sok. ($IP(x) = L^0R^0$), L^0R^0'ı elde et.
- Elde edilen 64-bit diziyi sırasıyla L^i ve R^i olarak isimlendirilen sol ve sağ parçaya ayır.
- Sağ parçayı sol parçaya ata.($L^i = R^{i-1}$)
- Yeni sağ parçayı elde et. ($R^i = L^{i-1} \oplus f(R^{i-1}, K^i)$)
- Diğer döngünün başlangıcına 64-bit değer olarak elde edilen bu diziyi yerleştir.
- Yukarıdaki maddeyi 16 döngü boyunca uygula.
- y şifreli metin olmak üzere şifreli metni $y = IP^{-1}(R^{16}L^{16})$ şeklinde elde et.



Şekil 3.6. DES algoritması ve genişletilmiş tek adım[23]



Şekil 3.7. DES algotirmasının 64 bitlik bloklar halinde uygulanması[9]

Her aşamada 64 bitlk bloklar halinde oluşturulan metinler birsonraki blokla bit toplama işlemi olan xor ile işleme sokulur ve DES aşamaları uygulanır. Şekil 3.7'de bu işlem gösterilmektedir. ICV olarak verilen anahtar ilk işlem için tüm bitler 0 alınır[23].

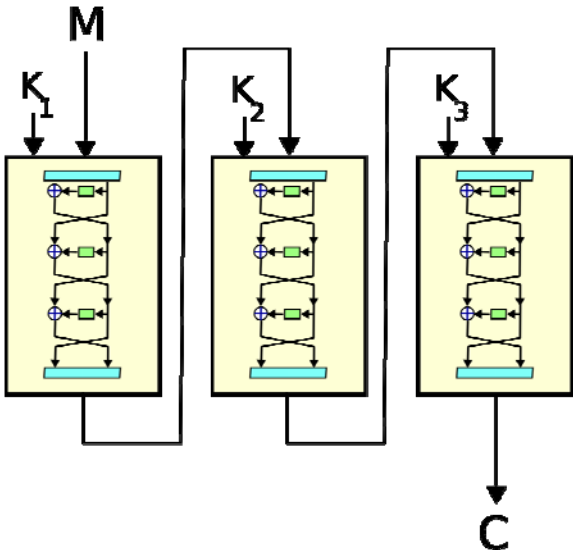
DES'in en büyük zaafı onun 56 bit anahtarıdır. Geliştirildiği zamanlarda çok iyi bir şifreleme algoritması olmasına rağmen modern bilgisayarlar tarafından yapılan

anahtar saldırılarına karşı yetersiz kalmaya başlamıştır. Daha büyük şifreleme ihtiyacının bir sonucu olarak DES, Triple-DES şeklinde geliştirilmiştir. Triple-Des, 3 adet 56 bitlik anahtarı kullanarak şifreleme yapmaktadır. Bu 168 bitlik anahtar gücüne eşit bir güç demektir. Bu uygulama bununla beraber şifreleme ve deşifreleme için 3 kat fazla çevrim gerektirir[23].

Triple DES algoritmasının uygulanması

Şekil 3.8'de gösterilmektedir. Birinci aşamada metin alınarak bilinen DES şifreleme algoritması uygulanır, ikinci aşamada ikinci anahtar ile şifre çözme işlemi gerçekleştirilir, arından son aşamada ise üçüncü anahtar kullanılanarak ikinci aşamada elde edilen metin şifrelenerek asıl şifrelenmiş metin elde edilmektedir[23].

DES algoritmasının kırmak için kullanılan tüm olası anahtarları tahmin etme yöntemi bu algoritma için geçersiz kalmaktadır. Çünkü 3 anahtarın hesaplanması; 56 bitlik anahtarın hesaplanmasından 2^{56} x 2^{56} x 2^{56} kez daha fazla zaman alacaktır.



Şekil 3.8. Triple DES algoritmasının uygulanışı[24]

3.5.2.2. RSA açık anahtar tekniği (public key technique)

Asimetrik kriptografi algoritmalarında simetrik kriptografi algoritmalarına göre farklı bir yöntem izlenir. Metni şifrelemek için kullnılan gizli anahtar elemanı sadece gönderen tarafta, buna karşın açık anahtar hem gönderen hem de alıcı taraf tarafından bilinmektedir. Başka bir deyişle şifreleme anahtarı açıktır herkes tarafından bilinir.

Ancak alıcı taraftaki gizli anahtar olmaksızın şifre çözme işleminin yapılması hemen hemen imkansızdır[26].

Açık anahtarlı kriptografik sistemlerin en önemli noktaları matematiksel işlevler üzerine temellenmiş olmalarıdır, aslında açık anahtarlı kriptografi için matematiğin çözüm getiremediği bir takım durumları (örneğin çok büyük bir sayının iki asal çarpanının bulunmasının matematikte herhangi bir doğrudan çözümü olmaması gibi) kullanarak güvenlik sağlamaktadır. Daha da önemlisi, açık anahtarlı kriptografi, tek anahtar kullanan simetrik geleneksel şifreleme algoritmalarının tersine, iki ayrı anahtarın asimetrik kullanımını öngörmektedir. Açık anahtarlı kriptografi teknikleri bir önceki bölümde değinilen veri bütünlüğü, onaylama, red edilememe, gizlilik, kimlik denetimi gerektiren durumlarda etkili sonuçlar ortaya koymaktadır[25,26].

Şifreleme işlemi için kullanılan anahtar ile çözme işlemi için kullanılancak olan anahtar arasında matematiksel bir bağıntı vardır lakin bu anahtarlar bir birinden türetilemezler ve birbirinden farklı olmak zorundadırlar. Şifreleme işlemi herhangi bir anahtar ile yapılabilmektedir. Diğer anahtar ile de çözme işlemi gerçekleştirilebilmektedir[26].

Veri güvenliği için gizlilik yöntemi şu şekilde sağlanmaktadır:

- Şifreleme ve şifre çözme için kullanılacak anahtarlar önceden oluşturulur.
- Şifreleme anahtarı(açık anahtar-public key) herkesçe erişilebilecek bir şekilde paylaşılır. Özel anahtar saklı tutulur.
- A kişisi tarafından, bir B kişisine, B kişisinin bu mesajı kendisinden başka kimsenin görüntüleyemediğine emin olabileceği bir mesaj yollamak isterse, mesajı B kişisinin açık anahtarını kullanarak şifreler.
- B kişisi, mesajı aldığında, bu mesajı kendi özel anahtarını kullanarak şifresini çözer. Bu mesajı elde eden diğer hiçbir alıcı mesajı çözemez, çünkü mesajı çözecek olan özel anahtarı sadece B kişisi tarafından bilinmektedir.

Bu yukardaki senaryo ile, B kişisi sadece kendisinin okuduğundan ve başka herhangi bir kimsenin görüntüleyemediğinden emin olduğu bir mesaj alır. Fakat bunun kimden geldiğinden emin olamaz. Gizlilik sağlanmış olur[25].

Yukardaki son iki adımın şu şekilde gerçekleşmiş olduğu bir senaryo ile kimlik denetimi de gerçekleştirilmektedir:

- Herhangi bir A kişisi, herhangi bir B kişisine B kişisinin A kişisinden geldiğine emin olarak okuyabileceği bir mesaj yollamak isterse, mesajı kendisinin gizli anahtarını kullanarak şifreler.
- B kişisi, mesajı aldığında, bu mesajı A kişisin açık anahtarı ile çözer. Bu iki kişi dışındaki alıcıların her biri de bunu yapablilir, çünkü A kişisinin açık anahtarı herkesce bilinmektedir. Bu durumda B kişisi, bu mesajın A kişisinden geldiğinden, ve kendisine ulaşana kadar yolda herhangi bir yerinin değiştirilmediğinden emin olur. Çünkü A kişisinin açık anahtarı ile çözdüğü mesajın sadece A kişisinin bilebileceği özel anahtar ile şifrelenmiş olduğunu bilir.

Bu senaryo ile de gizlilik yerine kimlik denetimi sağlanmış olur. Hem gizliliğin hem de kimlik denetiminin sağlanabileceği bir senaryo da şu şekilde gerçekleştirilmektedir:

- A kişisi, herhangi bir B kişisine, B kişisinin A kişisinden geldiğine ve yolda kendisinden başka kimsenin içeriğini görüntüleyemediğine emin olarak okuyabileceği bir mesaj yollamak isterse, mesajı kendisinin gizli anahtarını kullanarak şifreler, daha sonra ortaya çıkan mesajı da B kişisinin açık anahtarını kullanarak şifreler.

Bu sayede de hem gizlilik hem de iki taraflı kimlik denetimi sağlanmış olur[25,26].

Bu kripto sistemin en çok kullanılanı RSA (Rivest Shamir Adleman) algotirmasıdır. RSA'da düz metin, bloklar içinde şifrelenir, her blok bir *n* sayısından daha az bir ikili değere sahiptir. Bloğun büyüklüğü $\log_2(n)$ değerine eşit ya da daha az olmalıdır; pratik olarak blok büyüklüğü 2^k bittir, bu durumda *n* için sağlanması gereken durum da $2^k < n \le 2^{k+1}$ eşitsizliğidir. Şifreleme ve çözme bir düz metin bloğu M ve şifreli metin bloğu C için şu şekildedir:

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Hem gönderici, hem de alıcı *n* değerini bilmelidir. Gönderen, *e* değerini bilir ve sadece alıcı *d* değerini bilir. Bu tanımlanan koşullara göre *KU*=[*e, n*] bir genel anahtar ve *KR*=[*d , n*] de bir özel anahtar olmaktadır[26].

- $M<n$ olduğu koşulda, $M^{ed}=M \bmod n$ iken; *e, d, n* değerlerini bulmak mümkün olmalıdır.
- $M<n$ olduğu koşul sağlayan tüm *M* değerleri için M^e ve C^d değerlerinin hesaplanması kolay olmalıdır.
- Yalnız *e* ve *n* verildiğinde, *d* değerinin hesaplanması imkansız olmalıdır.

$1-M^{ed} = \bmod n$
$2-m^{k\lambda(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$
$3-\lambda(pq)= (p-1)(q-1)$
$4-ed = k\lambda(n)+1$
$5-ed \equiv \bmod \lambda(n)$
$6-d \equiv e^{-1} \bmod \lambda(n)$

2 numaralı eşitlikteki $\lambda(n)$ fonksiyonunun döndürdüğü değer, *n* değerinden küçük olan ve *n* ile aralarında asal olan tam sayıların sayısıdır. *p* ve *q* asal sayılar olduğu durumda 3 numaralı eşitlik sağlanmış olmaktadır. Bu eşitliklerden 4, 5, 6 numaralı eşitlik sağlanmaktadır. Buradaki işlemlerden görüleceği gibi *e* ve *d* $\bmod \lambda(n)$ fonksiyonunun çarpmaya göre tersidir. Bu denkliklerin doğru olabilmesi için *d*, *e*, $\lambda(n)$ nin aralarında asal olması gerekmektedir[26].

Bu bilgilerden elde edilen bilgileri şunlar elde edilmektedir:

- *p*, *q*: iki asal sayı (gizli, seçilmiş)
- *n*=*pq*: *n* değeri (açık, hesaplanmış)
- *e*: *e* değeri (açık, $\gcd(\lambda(n), d) = 1$ ve $1 < e < \lambda(n)$ olacak şekilde seçilmiş)
- $d \equiv e^{-1} \bmod \lambda(n)$: *d* değeri (gizli, hesaplanmış)

Bu seçim ve hesaplamalar doğrultusunda [*d,n*] çifti gizli anahtarı, [*e,n*] çifti de açık anahtarı oluşturmaktadır. A kullanıcısı, B kullanıcısına, B kullanıcısının açık

anahtarını kullanarak M mesajını göndermek istiyor. Bu durumda A kullanıcısı, $M^{ed}=M^{e} \bmod n$ ile ürettiği C şifreli mesajını elde edecek ve bunu B kullanıcısına gönderecektir, B kullanıcısı da bu mesajı aldığında $M=C^{d} \pmod n$ formülü ile elindeki mesajı çözmeyi başaracaktır[26].

Eğer sayısal olarak örneklendirecek olursak:

- İki adet asal sayı seçelim, $p=7$ ve $q=17$ olsun.
- n değerini hesaplayalım, $n=pq=7x17=119$
- $\lambda(n)$ değerini hesaplayalım, $\lambda(n)=(p-1)(q-1)=96$

Şimdi de $\lambda(n)$ değerinden küçük olacak ve $\lambda(n)$ ile aralarında asal olack şekilde bir tane e tamsayısı seçelim, burada $e=5$ olsun (bu değer bizim açık anahtarımız olacak). Son olarak öyle bir d sayısı seçmemiz gerekiyor ki, daha önce bahsettiğimiz şekilde $de=1 \pmod{96}$ eşitliğini ve $d<96$ eşitsizliğini sağlasın. Bu durumda $d=77$ olacaktır.

{5,119} açık anahtarımız, {77,119} da gizli anahtarımız oldu.

19 sayısını şifrelersek:

$$C = M^{e} \bmod n$$
$$C = 19^{5} \bmod 119$$
$$C = 2476099/119$$
$$C = 66$$

Elde ettiğimiz bu şifrelenmiş veriyi çözersek eğer:

$$M = C^{d} \bmod n$$
$$M = 66^{77} \bmod 119$$
$$M = 1.06x10^{138} \bmod 119$$
$$M = 19$$

Şeklinde tekrar şifrelenmeden önceki salt veri elde edilir[25].

Modüler aritmetik, çarpımın her sonucunda modül işleminin uygulanabilmesine izin verdiği için basit bir uygulama ile sonuca ulaşılabilmektedir. Açık anahtarlı kriptografide güvenliği sağlayan temel matematiksel problem, verilmiş bir sayının

asal çarpanlarını bulmadaki zorluktur, bu sayede iki asal çarpandan oluşan yeterli büyüklükteki bir n verildiğinde p ve q değerlerine ulaşmak hesapsal olarak imkansız olarak kabul edilebilir. Modüler aritmetik işlemlerini kullanması nedeniyle bu algoritma donanımsal olarak da gerçekleştirilebilmektedir.

BÖLÜM 4. TEK KART AKILLI KİMLİK KARTI UYGULAMASI

Son yirmi yılda, bilgi ve iletişim teknolojileri alanındaki gelişmeler ve bu gelişmelerin toplumsal yaşama yansımaları; eğitim, sağlık, tarım ve sanayi başta olmak üzere bütün toplumsal alanları, örgütlenme ve yaşam tarzını önemli ölçüde değiştirmiştir. 2000'li yıllarda, başta Avrupa Birliği (AB) gibi bölgesel oluşumlar olmak üzere birçok ülke, sanayi toplumundan bilgi toplumuna geçişi, bir amaç olarak belirlemiş ve bu amacı gerçekleştirmek için eylem planları hazırlamıştır. Bu gelişmeler, kamu yönetimi anlayışını da değiştirmiş; bilgi ve iletişim teknolojilerinin sunduğu olanaklar, kamu kurumlarının hizmet sunumunda da kullanılmaya başlanmıştır.

Bu süreçte birçok kurum birbirinden bağımsız, merkezi bir koordinasyondan uzak bir şekilde, hizmet sunmak amacıyla kurumun ihtiyaçlarını karşılayacak yazılımları geliştirmiş, kurumun sunduğu hizmetlere yönelik veritabanları oluşturmuştur. Bu durum, kurumların sunduğu aynı nitelikteki hizmetler için, her bir kurumun ayrı ayrı faaliyette bulunmasına yol açmıştır. Bu süreç; eşgüdüm içerisinde olmayan, birbirinden bağımsız hareket eden ve ortak bir politikası olmayan bir yapı ortaya çıkarmıştır.

Bu yapı; verinin gereksiz tekrarı, bu verilerin kaydedilmesi esnasında yapılabilecek olan insan kaynaklı olası hatalar, kayıt süresine bağlı olarak işlem süresinin uzaması ve getirdiği zaman kayıpları, vatandaşa ait kurumla ilgili, işlem yapılmasını sağlayacak olan aynı nitelikte kullanılan farklı farklı ama aynı bilgileri barındıran kimlik kartları ve bu kartlarla ilgili maliyetler, gerçekleştirilecek olan işlemlerle ilgil kırtasiye masrafları, evrak takibinin zorluğu gibi getirdiği olumsuzluklar hem vatandaş hem de devlet açısından sorun teşkil etmektedir.

Klasik bürokratik devlet anlayışında işleyen sistemin getirdiği bu kayıplar zamanla nüfusun artmasıyla birlikte ve de ülkenin gösterdiği büyümeye bağlı olarak istendiği anda istenilen bilgiye ulaşılamaması, bir evrak rakibiyle ilgili anlık elde edilebilecek

olan bir belgenin, ya da işlem sonucunun insan gücüne bağlı olarak günler hatta haftalarca uzaması gibi sorunları da beraberinde getirmektedir. Bilgi toplumu olma yolunda hazırlanan eylem planlarının içeriğinde bu gibi bürokratik devlet anlayışından şeffaf, hızlı ve etkin çözümler sunan, işlerin sonuçlandırılmasıyla ilgil sürelerin en aza indirildiği, vatandaşla ilgili kayıtları tek bir merkezde toplanan ve tüm kamu ve kuruluşlarla eş zamanlı olarak çalışan sistemlerin geliştirilmesi kaçınılmaz bir hal almaktadır. Bu yolda ilerlerken vatandaşla ilgili şu anki sistemde gerçekleştirilen işlemlerle ilgili olarak tüm kamu kurum ve kuruluşlarının ortak bir noktadan işlem yapabileceği koordine sistemler ve bu sistemlerle ilgili vatandaşın kişi yönünden önem arz eden verilerinin bir merkezde toplanması hedeflenmektedir. Bu merkezi idare birimine bağlı olarak vatandaşın günlük hayatta kullandığı tüm işlemler için merkezdeki bilgilerine erişilerek işlemlerini kısa sürelerde gerçekleştirebilecektir.

Tüm bu işlemler vatandaşın kimlik bilgisinin doğrulanması ve işlemi gerçekleştiren kişinin gerçekten kimlik sahibi kişinin olduğundan emin olunması gerekmektedir. Günümüzde bu işlem için nufüs cüzdanı kullanılmaktadır. Fakat bu kullanım sahtecilik, başkasının yerine işlem yapma, ya da dış koşullara bağlı olarak kimlik üzerinde bilgilerin silinmesi gibi sorunlar oluşmaktadır. Merkezi oluşum için kullanılacak olan veri vatandaşlık numarasıdır. Vatandaşlık numarası, günümüzde kullanılan kimliklerde yer almaktadır. Ve şu anda gerçekleştirilen kamu uygulamalarının dönüşümü sürecinde işlemler vatandaşlık numarası üzerinden yapılmaktadır. Fakat daha önce de bahsettiğimiz gibi vatandaş ile ilgili özlük bilgileri kurumların kendi veritabanlarında merkezi bir sistemden uzak, kurumun ihtiyaçlarını karşılayacak bir şekilde kaydedilmektedir. Bu da kaydetme esnasındaki bilgi girişinin kontrolünü ve olası yapılabilecek olan yanlışların önlenmesini sağlayamamaktadır.

Akıllı kartlar, tüm kamu ve kurumlarda kullanılmak üzere işlemin gerçekleşmesi için gerekli olan bilgiyi içererek işlemin hızlı, güvenilir, hatasız ve kolay bir şekilde tamamlanmasını sağlamaktadır.

Bu sorunların önüne geçilmesi aşamasında kamu kurum ve kuruluşlarının vatandaşa yönelik sunduğu hizmetler için gereken veriler merkezi bir yerde kayıt altına alınmalı

ve gerekli veriler bu merkezlerden sağlanmalıdır. Ancak bu şekilde gereksiz veri tekrarı, hatalı veri girişi, veri girişinden kaynaklı zaman kayıpları azaltılarak daha hizmetlerin sunulması hızlanacak, veriye ulaşmak daha kolay ve verimli bir şekilde sağlanmış olacaktır. Aynı zamanda kurumlar arasındaki bilgi alışverişi de daha etkin ve koordineli bir şekilde sağlanmış olacaktır.

Bu tez çalışmasında tasarlanan sistem merkezi veritabanının simülasyonu niteliğindedir ve içermekte olduğu veriler örnek teşkil etmektedir.

4.1. Sistemin Amacı

Günümüzde kullanılmakta olan sağlık karnesi, trafik işlemlerinde kullanılmakta olan ehliyet, alışveriş işlemlerinde ödeme amaçlı kullandığımız bankamatik, kredi kartları ve bunların dışında kimlik doğrulama ile ilgili gereken tüm kartların iptal edilip tek kart üzerinden tüm işlemlerin gerçekleştirilebilmesini sağlayacak bir sistem alt yapısı tasarlamak amacıyla oluşturulmuştur.

Bahsi geçen kullanılan kartların maliyeti tüm ülke geneline baz alındığı zaman ekonomik yönden ciddi tasarruflar sağlanmaktadır[17]. Getirdiği kolaylıklar, güvenlik, iş süreçlerinin azalması, hız ve maliyet; gerek ekonomik yönden gerekse işlemlerin elektronik ortamda yapılmasını öngören AB uyum sürecinde DPT'taradından planlanan eylem planlarının uygulanmasına da katkıda bulunulmaktadır[17].

Bu kart sayesinde kişinin yaptığı tüm işlemler vatandaşlık numarasıyla sistemde yer alan kayıt veritabanında tutulacağı için zamanla verilerin artmasıyla birlikte yapılacak olan istatistiki çalışmalara ışık tutacaktır. Bu istatistiki bilgilerin ışığında ekonomik yönden çok önemli yere sahip yatırımlar planlanabilecek ve bunlar gerektiğinde vatandaşın kullanımına sunulabilecektir.

4.2. Sistemin Yapısı

Tasarlanan sistem MBS(Merkezi Bilgi Sistemi), NAS(Nakit Akış Sistemi), ETKS(Emniyet Trafik Kontrol Sistemi), SBS(Sağlık Bilgi Sistemi), İKS(İşlem Kayıt

Sistemi) olmak üzere beş uygulamadan oluşmaktadır. Bunlardan MBS olarak nitelendirilen uygulamada vatandaşa ait özlük bilgileri, kimlik kartının; ne zaman verildiği, son kimliğin geçerlilik tarihi gibi bilgiler yer almaktadır. Geliştirilen tüm uygulamlar bu ortak noktadan öncelikle vatandaşla ilgili veri alıp bu veriler doğrultusunda işlem gerçekleştirmektedir.

NAS uygulamasında vatandaşın nakit işlemleriyle ilgili veriler ve müşterisi olduğu banka hesapları bilgileri saklanmaktadır. Ödeme işlemlerinde vatandaşın bilgilerine bu uygulamadan erişilerek; istediği hesabı kullanarak ödeme işlemlerini gerçekleştirmektedir.

ETKS uygulamasında vatandaşın ehliyet, ruhsat, araç muayenesi, egzos pulu, motorlu taşıtlar vergisi verileri ile ilgili denetim işlemleri yer almaktadır. Bu vergilerin ödenip ödenmediği bilgisine bağlı olarak araçla ilgili ceza işlemi yapılmaktadır.

SBS uygulamasında kullanıcının reçete bilgileri, hangi hastanede ne şekilde hangi doktor tarafından tedavi edildiği, kullandığı ilaçlar; bunların kullanım zamanları ve tekrar ne zaman alabileceği bilgisi. Hastayla ilgili olarak alerjisi olduğu ilaçların ilaç yazma işleminde hesaba katılması, önceden kullandığı ilaçlara bağlı olarak ilaç yazma işlemleri gibi işlemler yapılmaktadır. Bu uygulamanın son aşaması ilaç teminidir ve herhangi bir eczaneden vatandaşlık kartını kullanarak ilaçlar temin edilmektedir.

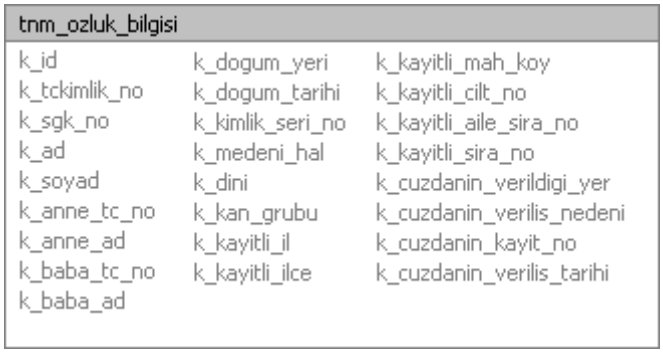
İKS uygulaması tüm bahsedilen uygulamalarda gerçekleştirilen işlemleri kayıt altına almaktadır. Kayıt altına alınan verilerin sayısının artmasıyla bu veriler analiz edilerek gerek kişi gerek ülkedeki genel eğilimlerle ilgili istatistiki bilgilere ulaşılabilecektir.

4.2.1. Merkezi bilgi sistemi

Vatandaşın kendisiyle ilgili tüm kimlik ve özlük bilgilerinin tutulacağı bu veritabanı uygulaması sistemimizin temelini oluşturmaktadır. Geliştirilmesi planlanan tüm uygulamalarda; vatandaşla ilgili kimlik doğrulama işlemleri bu sistem üzerinden gerçekleşmektedir.

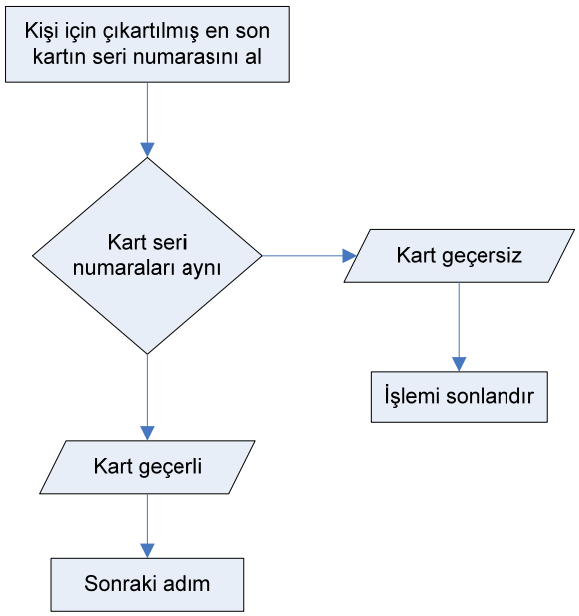
Tüm işlemlerin merkezden ve tek numara üzerinden yapılmasına bağlı olarak isim benzerliğinden kaynaklanan hataların giderilmesi, kurum ve kuruluşlarda veri girişi sırasında insan kaynaklı olarak yapılan hataların önüne geçilmesi, kurumlar arası bilgi alışverişinin kolaylaştırılması, kimlik tespitinin hızlı ve kolay bir şekilde yapılması, kurum ve kuruluşların vatandaştan ayrı bir belge istemesine son verilmesinin yanı sıra kırtasiye masraflarının da önlenmesi hedeflenmektedir.

Şekil 4.1'de kişilerin merkezi veritabanında tutulan veriler görülmektedir.



Şekil 4.1. Kişilerin özlük bilgileri

Oluşturulan sistemde kişinin kimlik kartını herhangi bir işlemde kullandığı sırada MBS veritabanından öncelikle kullanılan kartın geçerli olup olmadığı bilgisine ulaşılmaktadır. Bu işlem kimlik kartının seri numarasının sistemde kayıtlı olan kartların seri numaralarının kontrol edilmesiyle yapılmaktadır. Bu sorgulama esnasında vatandaşa ait en son çıkartılmış olan kimlik kartı bilgisi ile kullanılan mevcut kartın seri numarası Şekil 4.2'de gösterildiği üzre eşleştirilmektedir. Eğer gelen veri ile kartın seri numarası aynı değilse, kart geçersiz sayılıp işlem yapılmamaktadır. Eğer kart seri numaraları eşleşiyorsa bir sonraki adıma geçilmektedir.

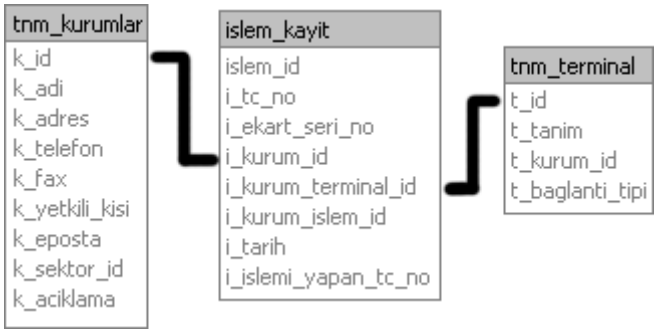


Şekil 4.2. Kimlik geçerliliğinin akış şeması

Kontrol amaçlı olarak kimlik kartının geçersiz sayıldığı durumlarda; işlem kayıt sisteminden mevcut kartın seri numarası ile sorgulama yapılarak en son işlem tarihi bilgisi karşılaştırılarak elde edilen bilginin doğruluğu sağlanmış olmaktadır.

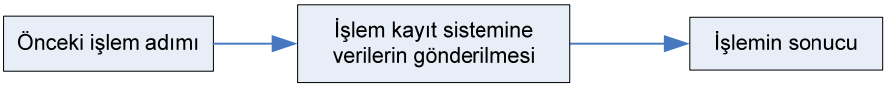
4.2.2. İşlem kayıt sistemi

İşlem kayıt sistemi vatandaşın günlük gerçekleştirdiği işlemlerin kaydını tutmaktadır. Bu kayıtlar esnasında işlemin numarası, işlemi gerçekleştiren terminal numarası, hangi kurum ya da kuruluş tarafından, ne zaman, kim tarafından, hangi kimlik numarasıyla yapıldığı gibi bilgileri tutmaktadır. Bu sistem sadece kayıt etmekte kullanılmakta olsa da ileride veriler üzerinden anlamlı istatistiki bilgiler elde edilebilecektir. Bu istatistik verilerine bağlı olarak vatandaşlara yönelik hizmetler geliştirilebilecektir. Bunların yanında olası bir hata durumuna karşı yapılan işlemlerin kayıt altına alınması hatanın neden kaynaklandığına dair bilgi toplanması sürecinde önem arz etmektedir. Bu nedenle gerçekleştirilen her işlemin kaydının alınması ihtiyacı doğmaktadır. Bu sistem de merkezi sistem gibi tüm diğer sistemlerle birlikte çalışacaktır.



Şekil 4.3. İşlem kayıt sisteminin veritabanı yapısı

Şekil 4.3'te gösterilen veritabanı yapısındaki islem_kayit tablosu işlemlerin kaydedildiği tablo olup; islem_id alanı işlemin kaydedilme sırasını belirtmektedir. Vatandaş tarafından terminal cihazları üzerinden ya da masa üstü bilgisayar yazılımları kullanan kamu kurum ve kuruluşlarında gerçekleştirilen her işlem bir kart okuyucu cihaz tarafından gerçekleştirilmektedir. Cihazdan verilen çıktılardan bir tanesi vatandaşa bir tanesi de kurumda kalmak üzere iki çıktı verilmektedir. Kurumda kalacak olan çıktıda bu tabloda yer alan islem_id, kuruma sağlanan terminalin numarası i_kurum_terminal_id, i_tarih alanı işlemin gerçekleştirildiği zamanı, i_islemi_yapan_tc_no alanı da işlemi gerçekleştiren kişinin vatadaşlık numarasını içermektedir. Buradaki yapıdan yola çıkılarak vatandaşın nerede, ne zaman kartı kullandığı bilgisine erişilebilmektedir. Aynı zamanda i_kurum_islem_id kurumun kendi veritabanına kaydettiği işlem numarasını belirtmektedir, gerektiği takdirde bu numara kullanılarak kurumdan yapılan işlemle ilgili detaylı bilgi alınabilmektedir. Diğer tnm_kurumlar tablosu ise işlemin gerçekleştirildiği terminalin kurumu hakkında iletişim, kurumun hangi sektörde yer aldığı gibi bilgiler bulunmaktadır. Tnm_terminal tablosunda ise kuruma verilen terminalin tanım özellikleri ve de merkeze hangi tip bağlantı ile bağlanacağı bilgisi yer almaktadır. İşlem kayıt sisteminin işleyiş yapısı Şekil 4.4'de görüldüğü gibi öncelikle yapılmak istenen işlem yapılmakta ve ardından son adım olarak gerçekleştirilen işlemle ilgili kayıtlar tutulmaktadır. Bu bilgiler kaydedilirken terminal cihazların kendine özgü işlem değişkenleri kullanılmaktadır.



Şekil 4.4. İşlem kayıt sisteminin işleyişi

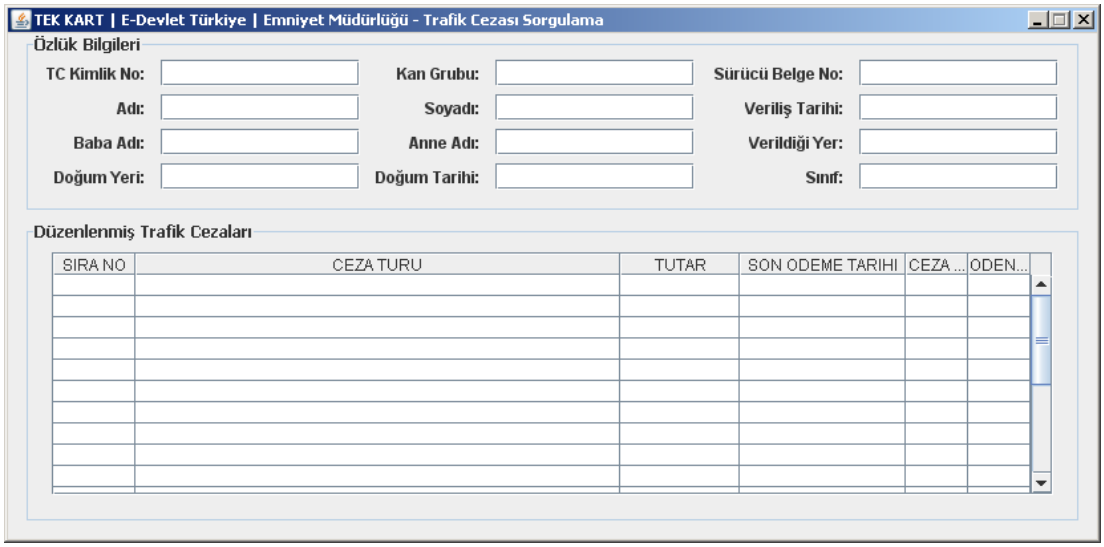
Tabloda yer alan t_id değişkeni her terminal için tektir. Aynı şekilde terminale uygulamanın yüklenmesi sırasında ilgili kurumun kodu da yazılmaktadır.

4.2.3. Emniyet trafik kontrol sistemi

Mevcut trafik denetim sisteminde; kişinin araçla ilgili ruhsat, egzos muayenesi pulu, araç muayene belgesi, trafik sigortasının yaptırıldığını gösterir belge gibi tüm evrakları araçta bulundurması gerekmektedir. Tüm bu evrakların hepsinin bulundurulması zaman zaman sorun olmaktadır. Ruhsat unutulmakta ya da kaybolmakta, yıllık yaptırılan sigorta belgeleri de kaybolabilmektedir. Aynı zamanda sürücü belgesi de belirli bir zaman sonra yıpranmakta ve değiştirilmesi gerekmektedir, bu işlem kişinin günlük işlerini bir aksatmasına sebep olarak gerekli belgeleri çıkartmak için birkaç yere giderek ödeme yapması, bu belgelerle ilgili evrakları doldurması gerekmektedir. Bu durum ciddi zaman kayıplarını beraberinde getirmektedir. Gerek bu işleri yerine getiren kurum, gerekse vatandaş açısından büyük zaman kayıpları meydana gelmektedir. Zaman kayıplarının yanında tüm bu belgelerin basılması, üretilmesi, dağıtılması işlemi maliyeti hesaplandığı zaman ortaya ciddi rakamlar çıkmaktadır.

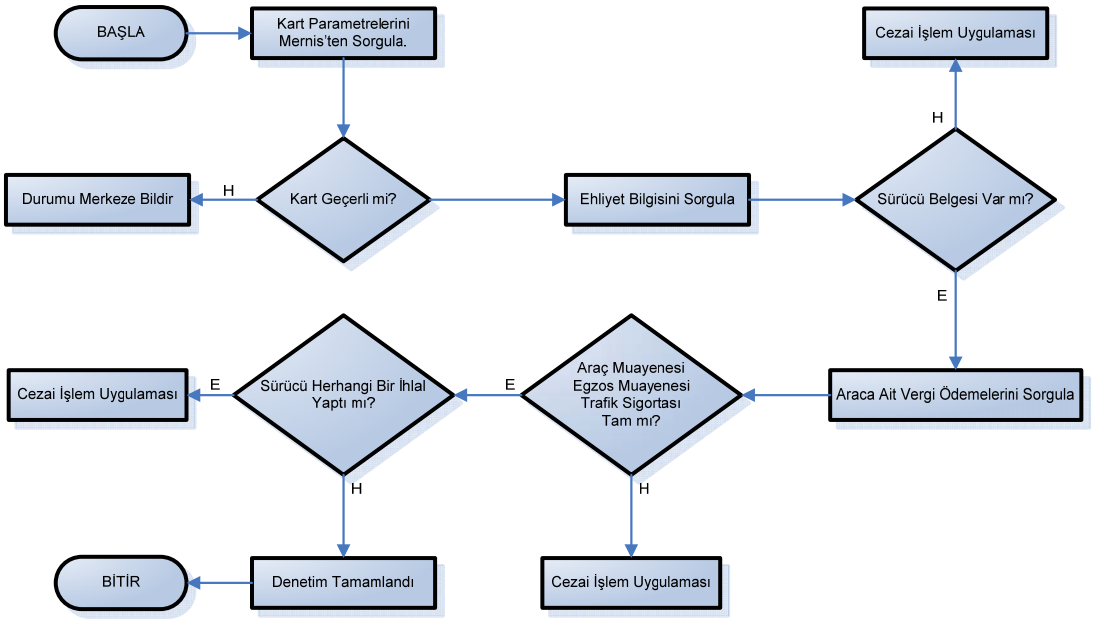
Tasarlanan sistemde trafik denetim işlemlerinin elektronik ortamda gerçekleştirilebilmesi için gereken veritabanı alt yapısı oluşturularak söz edilen ödemelerin yapılıp yapılmadığı bilgisi veri tabanından çevrim içi olarak sorgulanabilmektedir. Aynı zamanda bu vergilerle ilgili ödeme işlemleri herhangi bir bankadan ya da internet bankacılığı kullanılarak yapılabilmektedir. Kişi bu ödeme işlemlerini vatandaşlık kartını kullanarak gerçekleştireceği için ilgili veritabanına ödendi bilgisi işlenmektedir, olası bir denetim durumunda vatandaşlık kartını kullanarak sürücü belgesinin olup olmadığı, ne zaman aldığı gibi günümüzde kullanılan sürücü belgesinin üzerindeki tüm bilgilere ve bu bilgilerin yanında bahsi geçen vergi ödeme işlemlerinin gerçekleştirilp gerçekleştirilmediği bilgisine de

ulaşılmaktadır. Eğer yıl içinde yapılması zorunlu herhangi bir vergi ödeme işlemi yapılmamışsa sistem otomatik olarak cezai işlemleri gerçekleştirmektedir. Bu yöntemle görevli trafik memurunun iş yükü azalmakta ve gerekli evrakların kontrolü daha kısa zamanda gerçekleştirilmektedir. Aynı zamanda ceza işlemleri otomatik olarak sistem tarafından gerçekleştirildiği için rüşvet ya da suça göz yumma gibi bir durumunda önüne geçilmiş olmaktadır. İnsan gücüne dayalı herhangi bir yaptırımın bulunmadığı durumlarda kurallar daha kesin ve net uygulanacağı için sürücüler üzerinde de etkisini göstererek trafik suçlarının azalacağı düşünülmektedir.



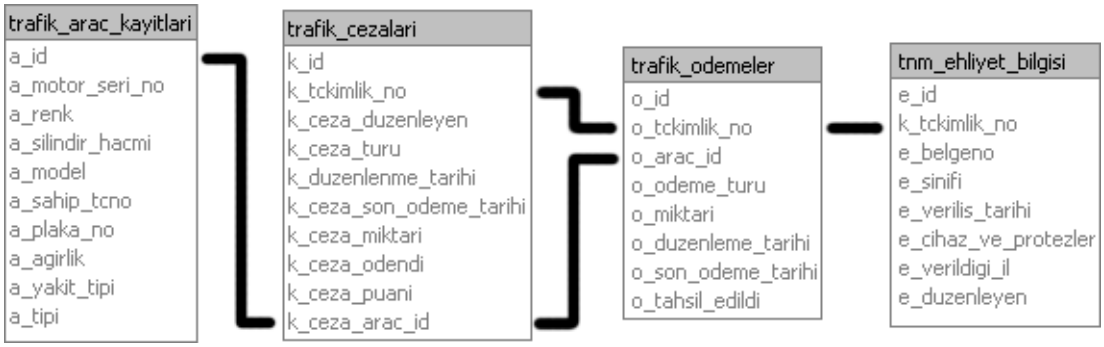
Şekil 4.5. Trafik denetim sistemi görsel ekranı

Şekil 4.5'te trafik denetim sisteminin arayüzü görülmektedir. Bu uygulamada Şekil 4.6'daki akış şeması incelenecek olursa öncelike merkezi sistemden vatandaşın kimlik bilgisinin geçerliliği kontrol edilmektedir. Eğer kimlik geçerli değilse durum Emniyet Müdürlüğü'ne bildirilerek gereken işlem yapılmaktadır. Kimlik geçerli ise Emniyet Müdürlüğü'nün sisteminden kişinin sürücü belgesinin olup olmadığı bilgisi gelmektedir. Gelen bu bilgiye göre eğer kişinin ehliyeti yoksa otomatik olarak denetimi gerçekleştiren memurdan bağımsız olmak üzere kişi için cezai işlem uygulanmaktadır. Eğer sürücü belgesi varsa kullanılan araca ait vergi ödemeleri kontrol edilmektedir, aynı yöntemle eğer ödemlerde eksiklik varsa otomatik olarak cezai işlem uygulanmaktadır. Vergi ödemeleri de tamsa bir sonraki adımda eğer bir trafik suçu işlenmişse gereken suç ile ilgili yaptırım işlemi denetimi gerçekleştiren memur tarafından uygulanarak merkeze iletilmektedir.



Şekil 4.6. Trafik denetim sisteminin iş akış şeması

Sistemde kullanılan veritabanı yapısı Şekil 4.7'de gösterilmketedir. Kullanılan tnm_ehliyet_bilgisi tablosu tüm ehliyet sahibi olan vatandaşların verilerini içermektedir. Aynı şekilde trafikte bulunan tüm araçların kayıtları da trafik_arac_kayitlari tablosunda bulunmaktadır. Sürücülerle ilgili kesilen tüm cezalar trafik_cezalari tablosunda yer almaktadır. Araçlara ait yıllık egzos muayenesi, motorlu taşıtlar vergisi, trafik sigortası, araç muayenesi gibi bilgiler de trafik_odemeler tablosunda yer almaktadır. Tabloların birbirlerine ilişkilerle bağlı oldukları için sistemde veri akışı hızlı ve etkin bir şekilde sağlanmaktadır. Kişinin bilgilerinin farklı farklı tablolarda tutulması hem gereksiz bilgi tekrarını hem de kullanılan bilgilerde bir değişiklik olduğu zaman kaydedilmiş bilgilerin geçerliliğini yitirmesi gibi bir durum söz konusu olmaktadır. Bu sorunun önüne geçilmesi için tüm uygulama ve işlem adımlarında kişinin vatandaşın kimlik numarası kullanılmıştır.



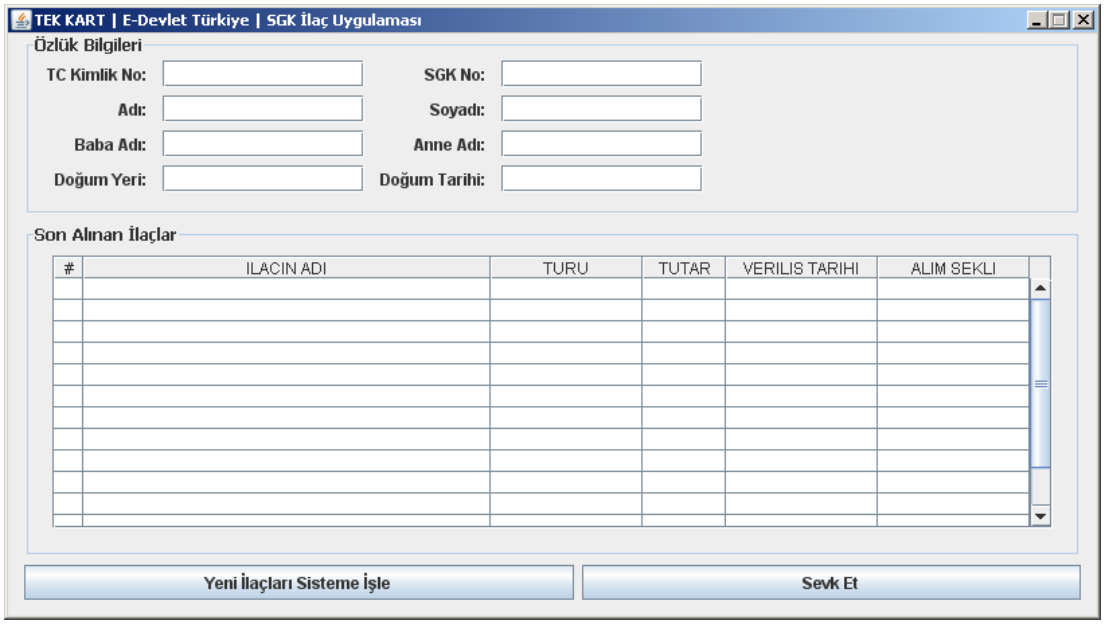
Şekil 4.7. Trafik denetim sistemi veritabanı yapısı

4.2.4. Sağlık sistemi

Mevcut sağlık sisteminde, sağlık güvencesi olan her bireyin sağlık karnesi bulunmaktadır. Bu karneler aracılığıyla muayene olduktan sonra doktor tarafından karneye ilaçlar eczanelerden temin edilmektedir. İlaçların temin edilmesi sırasında reçeteye yazılanların okunamaması, kullanım süresi bitmemiş bir ilacın yazılması, ilacın sağlık güvencesini sağlayan kurum tarafından karşılanmaması, gibi sorunlarla karşılaşılmaktadır. Sağlık karnelerinin basımı, dağıtımı ve diğer kırtasiye masrafları hesaplandığında ortaya maliyet açısından büyük meblağlar çıkmaktadır.

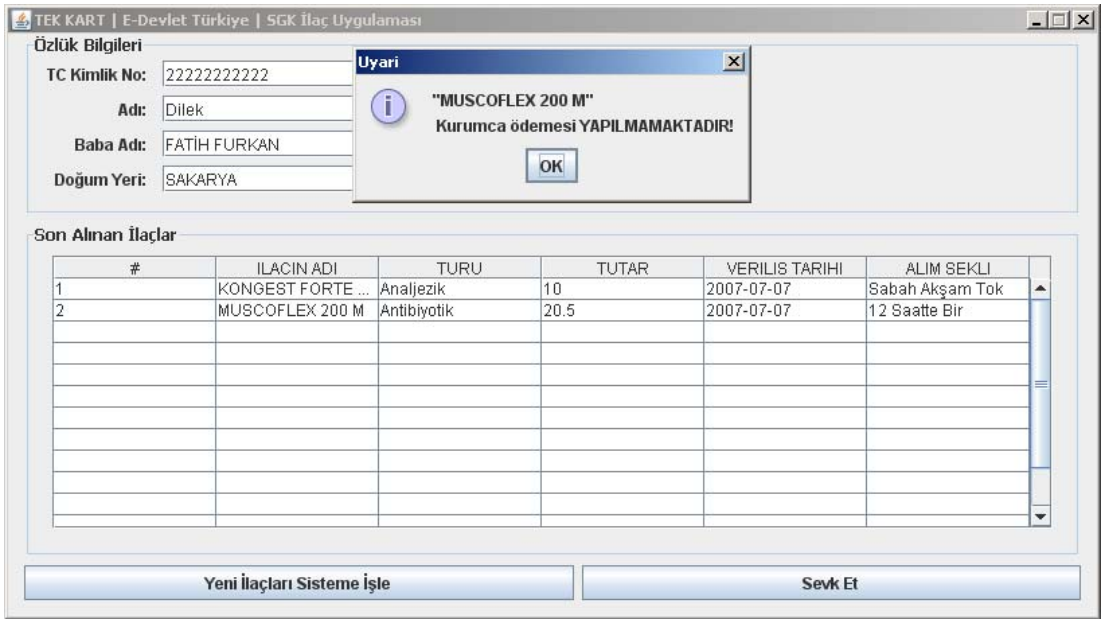
Geliştirilen bu sistemde; hastaneye gidildiği zaman kimlik doğrulama işlemlerinden sonra hastanın geçmiş dönemlerde, hangi hastanede muayene olduğu, kullandığı ilaç bilgisi bu ilacın kimin tarafından yazıldığı, geçirmiş olduğu hastalıklar gibi bilgilere ulaşılabilecektir.

İlaç yazımı sırasında eğer hastanın yazılan ilaca karşı bir alerjisi varsa bu doktor tarafından görülebilmekte ve buna göre ilaç değiştirilmektedir. Yazılan ilaçlar tamamen elektronik ortamda tutulduğu ve de reçete ortadan kaldırıldığı için; reçeteye sonradan ilaç eklenmesi gibi işlemlerin de önüne geçilmektedir. Yazılan ilaçların temini için hasta herhangi bir eczaneye gittiği zaman bu otomasyona dahil olan eczane tarafından yapılması gereken işlem kimlik kartının okuyucu cihaza yerleştirilip hastanın alaması gereken ilaçların temin edilerek ilaçların alındığına dair onayın sisteme kaydedilmesidir. İlaçlar alındıktan sonra ödeme işlemi için de aynı kimlik kartı kullanılmaktadır.



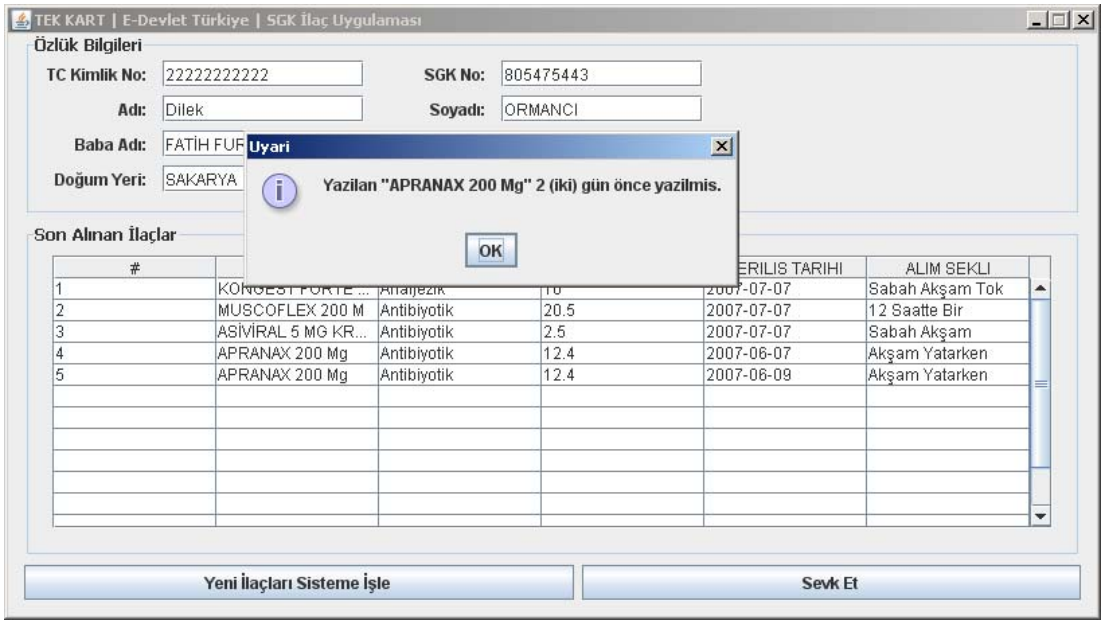
Şekil 4.8. Sağlık sistemi hastane arayüzü

Sistemin arayüzü Şekil 4.8'de görülmektedir. Buradaki bilgiler merkezi sağlık veritabanından hastanın vatandaşlık numarası kullanılarak sorugulanmaktadır. Yazılan ilaçlar hastanın sosyal güvenlik kurumu tarafından karşılanmıyorsa ilgili ilacın karşılanmadığına dair uyarı görüntülenmektedir.



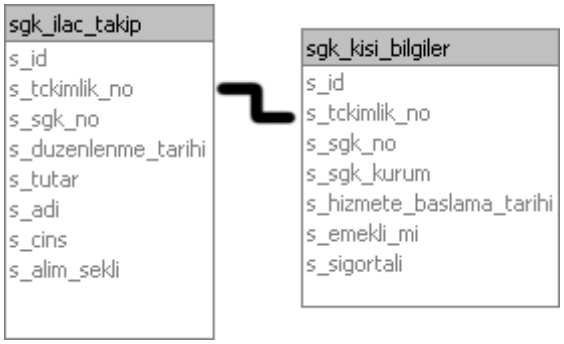
Şekil 4.9. Kurumca ödenmeyen ilaç yazımında uyarı ekranı

Yeni ilaç yazımında yazılan ilacın ödeme bilgisinin yanında eğer halen kullanılmaktaysa ilgili uyarı ekranda görüntülenmektedir



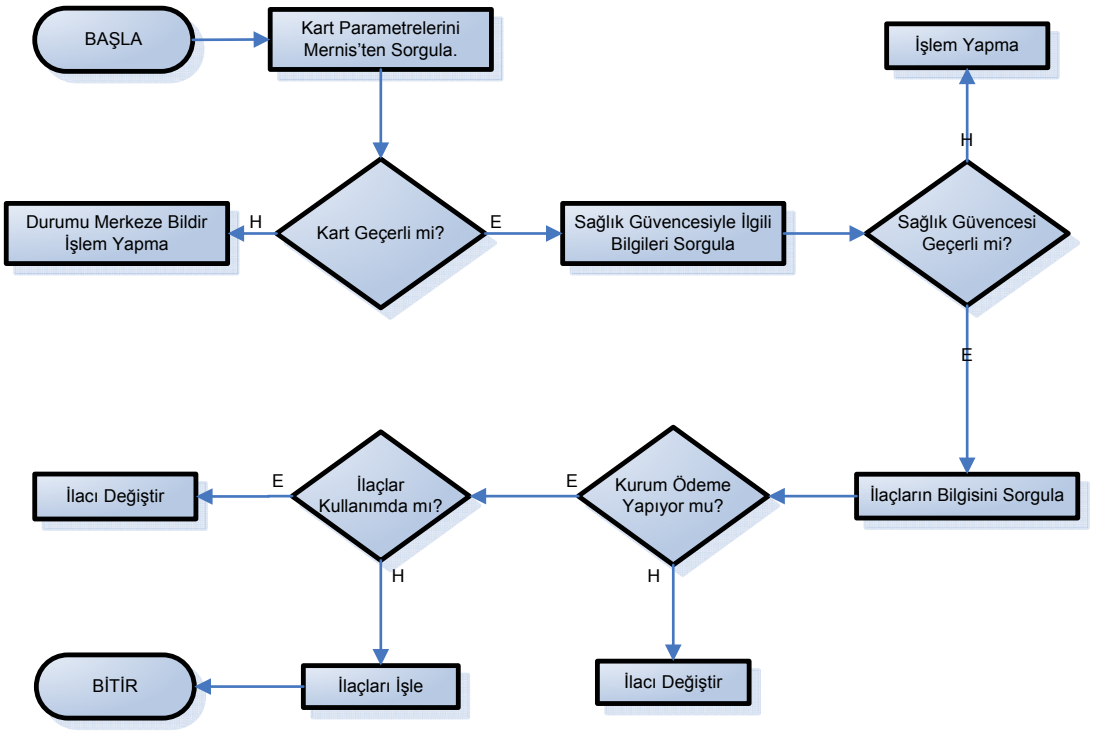
Şekil 4.10. İlaç kullanım süresi bitmeden yazılan ilaç için uyarı ekranı

Sistemin akış şeması Şekil 4.12'da görülmektedir. İlk olarak bireyin kimliğinin geçerliliği kontrol edilmektedir, ikinci adım olarak bireyin sağlık güvencesinin geçerliliği konrtol edilmektedir, üçüncü adımda daha önceden yazılmış olan ilaçların listesi merkezden alınmaktadır. Yeni ilaç yazımı aynı ekrandan yapılmaktadır.



Şekil 4.11. Sağlık sistemi veritabanı yapısı

Şekil 4.11'de sağlık sistemiyle ilgili kayıtların tutulacağı veritabanı yapısı yer almaktadır.



Şekil 4.12. Sağlık sisteminin akış şeması

Bu sağlık sistemiyle birlikte tüm hastaların yazılan ilaçları merkezi veritabanında kayıt altında tutulmaktadır. Bunun yanında hastayla ilgili bulgular, konulan teşhis de veritabanına kaydedilmektedir. Zamanla kayıtların artmasıyla birlikte bu kayıtlar değerlendirilerek sıklıkla karşılaşılan hastalıklar, en çok yazılan ilaçlar gibi istatistiki bilgiler ışığında sağlık sektöründe gerek ilaç alımları gerekse sık görülen hastalıkların önlenmesiyle ilgili tedbirler alınabilecektir.

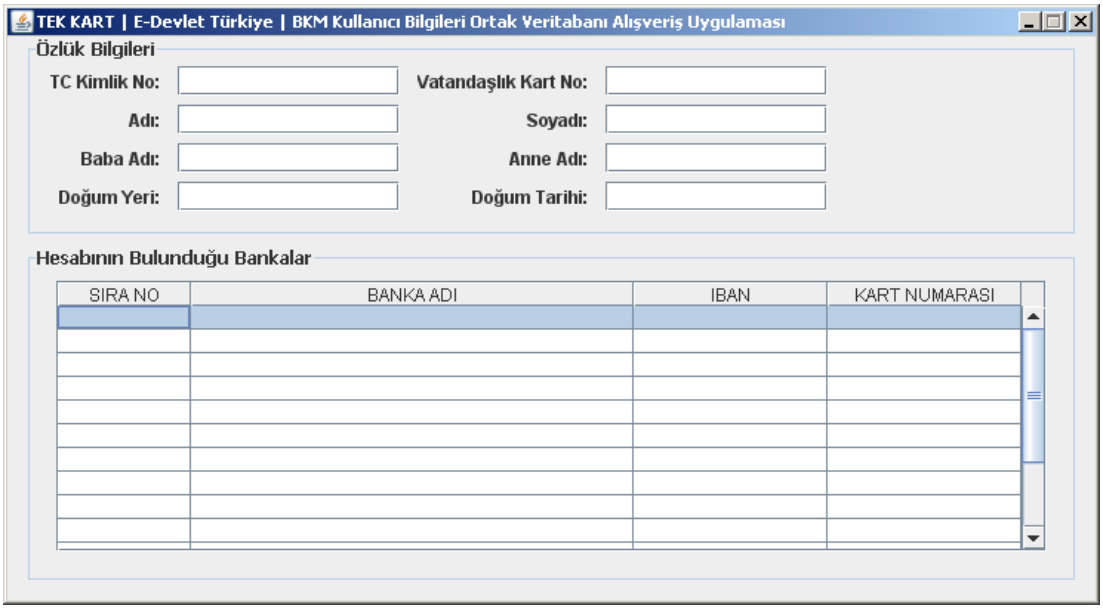
4.2.5. Nakit ödeme sistemi

Günümüzde nakit ödeme işlemleri için bankalarca bireylere verilen bankamatik ya da kredi kartları ile gerçekleştirilmektedir. Bu sistemde ödeme işlemi için POS(Point Of Sale) cihazları kullanılarak yapılmaktadır. Kartlar kişinin kimliği yerine geçmekte olup merkezdeki veritabanından kartın bağlı olduğu hesaptan ödeme miktarını ödeme yapılan kurumun hesabına aktaracak şekilde para transferi gerçekleşmektedir. Kullanılan manyetik şeritli kartların kopyalanabilir olması, zayıf güvenlik denetimeleri yüzünden kartlarda sahtecilik, başkasının kartını kullanma gibi sorunlar çıkmaktadır. Tasarlanan sistemde tüm banka tarafından bireye tahsis edilen kartların

yerine; bireylerin banka hesaplarının tutulduğu bir veritabanı havuzu oluşrutulup kişilerin hesaplarına ait kayıtlar burada tutulmaktadır. Şekil 4.13'de görüldüğü bigi bir veritabanı yapısı oluşturulmuştur. bu yapıda kişinin vatandaşlık numrası ile tüm banka hesapları ilişkilendirilmiştir.

Şekil 4.13. Nakit ödeme sistemi için veritabanı yapısı

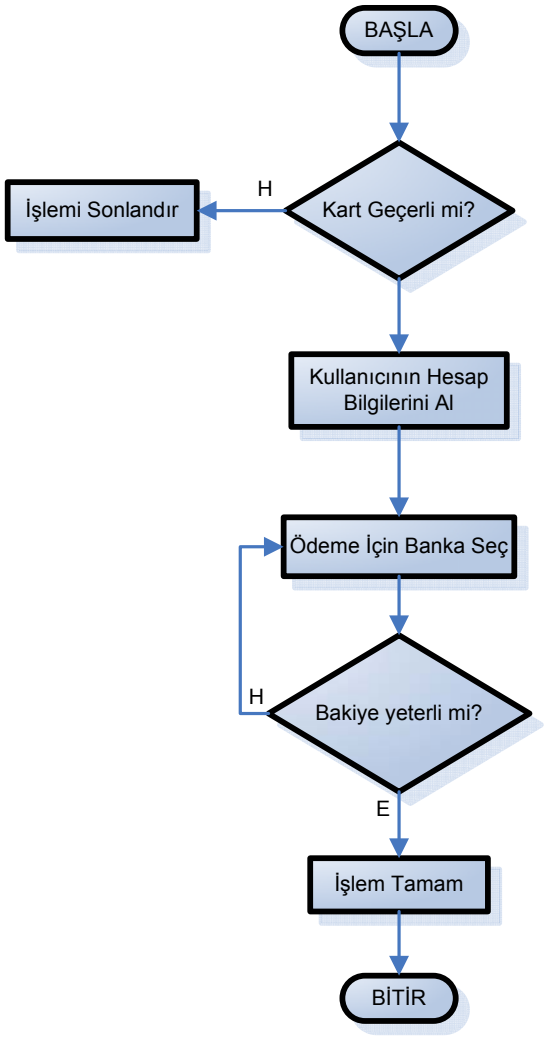
Bu ilişkilendirme sonucunda kişi herhangi bir yerde alışveriş yaptığı zaman kendisine ait tüm hesaplara pos cihazının ekranından ulaşılabilmektedir. Kişi dilediği hesabını seçip ödeme işlemini gerçekleştirmektedir.



Şekil 4.14. Nakit ödeme sistemi arayüzü

Kart kullanılırken ilk olarak kartın geçerliliği kontrol edilmektedir. İkinci adımda kişinin hesabının bulunduğu, ödeme işlemini gerçekleştirebileceği bankaların listesi gelmektedir. Üçüncü adımda ise kişinin isteğine bağlı olarak bir banka seçilip nakit ödeme miktarı karşılanmak üzere işlem yapılmaktadır. Eğer bakiye yeterliyse işlemin

onayı alınmakta ve işlem sonlanmaktadır. İşlem adımları Şekil 4.15'deki akış şemasında görülmektedir.

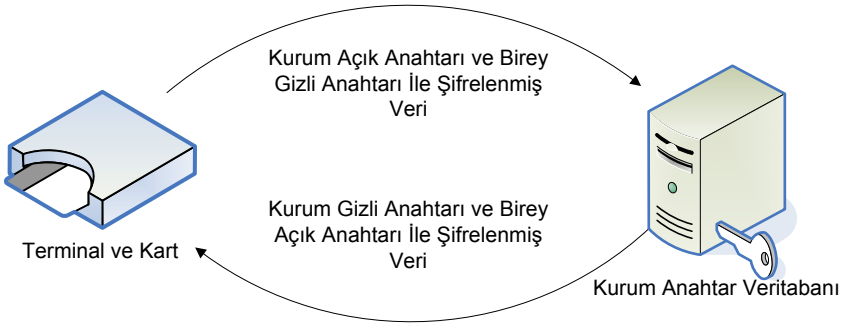


Şekil 4.15. Nakit ödeme işlemleri için akış şeması

4.3. Sistemin Güvenliği

Tasarlanan sistemin güvenliği için; açık anahtarlı şifreleme yöntemleri kullanılmaktadır. Tüm bireylerin açık anahtarları sadece gerekli izinleri tanılanmış kurum ve kuruluşlarca erişilebilecek şekilde merkezi bir veritabanında tutulmaktadır. Veri iletişimi esnasında karta yazılan bireyin gizli anahtarı ve kurum tarafından terminal cihaza yüklenmiş olan kurumun açık anahtarı ile veri şifrelenmektedir. Kuruma ulaşan bu şifreli veri kurumun gizli, bireyin de açık anahtarı kullanılarak

açılmaktadır. Bu şekilde açılan veriye göre kurum tarafından gerekli işlem gerçekleştrilmektedir.



Şekil 4.16. Veri iletimi esnasında şifreleme işlemi

Şekil 4.16'da bu iletişimin gerçekleşmesi işlemi gösterilmektedir. Bu şekilde veri iletimi esnasında istenmeyen kişiler tarafından verilin ele geçirilmesi, değiştirilmesi gibi güvenlik sorunlarının önüne geçilmiştir. Aynı zamanda veri bütünlüğü, kimlik denetimi, gizlilik gibi güvenliğin sağlanmasında önemli faktörler de sağlanmış olmaktadır. Kurumların kendilerine özgü açık anahtarları kart okuyucu terminale önceden yüklenmektedir.

BÖLÜM 5. SONUÇ VE ÖNERİLER

Gerçekleştirilen bu çalışmada günümüzde kimlik doğrulama amacıyla sağlık, trafik, alışveriş sistemlerinde kullanılan tüm belgelerin yerine tek bir kart kullanımı için gereken sistem altyapısı tasarlanmış; uygulamalar geliştirilmiştir. Geliştirilen bu sistemin günümüz mevcut sistemlerine kıyasla getireceği yenilikler ve kolaylıklar ortaya konmuştur.

Mevcut sistemde kişiye ait özlük bilgilerinin farklı farklı yerlerde tutulması verilerin tutarsızlığını meydana getirmektedir; bu sorun kişiye ait bilgilerin merkezi bir yerde tutularak önlenmesi hedeflenmiştir. Yapılan işlemlerin kağıt üzerinde gerçekleştirilmesi iş süreçlerinin uzunluğunu, bu uygulamaların birbirinden bağımsız çalışması ve gerektiğinde veriye erişilmesini zorlaştırmaktadır; kağıt üzerinde gerçekleştirilen işlemlerin yerini çevrim içi erişilebilen veritabanları alarak istenilen bilgiye daha kısa ve etkin sürelerde, her yerden ulaşılması amaçlanmıştır. Aynı zamanda günümüzde farklı kişinin kimliğini kullanarak işlem yapma gibi sorun teşkil eden evrak sahteciliği işlerinin de önüne geçilmesi amaçlanmıştır. Geliştirlen sistem, kişilerin günlük işlerini daha süratli ve etkin bir şekilde yapabileceklerdir.

Bu tek kartın kullanımına ilişkin sistem tasarımının ele alındığı bu tez çalışmasında ileriye yönelik olarak; karta kişinin biyometrik verileri de yüklenerek kimlik doğrulama işlemleri daha yüksek oranda güvenlik ve doğruluk sağlayacak şekilde geliştirilebilir. Aynı zamanda kısıtlı uygulama alanlarını örnek olarak ele aldığımız bu çalışma farklı farklı (eğitim, adalet, tapu gibi) uygulama alanlarına da uygulanabilir.

Tüm işlemlerin elektronik ortama taşınmasıyla birlikte ileriye yönelik olarak elde edilen verilerden çıkarılacak olan analizlerle ülkenin ekonomisine katkı sağlayacak pazarlama ve pazar oluşturma stratejileri geliştirilebilir, ülkenin geleceğe yönelik tasarruflarının belirlenmesine yön verilebilir.

KAYNAKLAR

[1] BARAKLI, B., Yarıiletken elemanların model parametrelerinin çıkarımına yönelik yeni bir yaklaşım, Sakarya Üniversitesi, Sakarya, 2007

[2] DI MAIO, A., Smart id cards in europe, Gartner Research, Şubat 2002

[3] ISO/IEC 7816-1 Identification cards, integrated circuits cards with contacts- part 1: physical characteristics.

[4] ÇOKSAK, F., Akıllı kartlar ile kütüphane otomasyonu, Süleyman Demirel Üniversitesi, Isparta, 2004

[5] FURCHE, A., Computer Money, Dpunkt, Germay, 1996

[6] ISO/EC 7816-3 Identification Cards, Integrated Circuits Cards with Contacts- Part 3: Electronics Signals and Transmission Protocols.

[7] TÜRKOĞLU, T., Akıllı Olan Kartlar, Para ve Banka TeknolojileriDergisi, Sayı:2 Mayıs-Haziran 1999

[8] http://people.cs.uchicago.edu/~dinoj/smartcard/security.html

[9] HANSMANN, U., Smart card application development using Java 2nd Edition, Germany, 2002

[10] ISO/EC 7816-2 Identification Cards, Integrated Circuits Cards with Contacts- Part 2: Dimensions and Location of the Contacts.

[11] ISO/EC 7816-3 Identification Cards, Integrated Circuits Cards with Contacts- Part 3: Electronics Signals and Transmission Protocols.

[12] http://cekirdek.pardus.org.tr/~gurer/kart/

[13] ISO/EC 7816-6 Identification Cards, Integrated Circuits Cards with Contacts- Part 6:Inter-Industry Data Elements.

[14] ISO/EC 7816-4 Identification Cards, Integrated Circuits Cards With Contacts- Part 4: Inter-Industry Commands For Interchange.

[15] NICKLOUS, M., SCHAECK, T., Smart Card Application Development Using Java, Germany, 1999

[16] KOÇAK, A., Akıllı Kartlar Kullanarak Sayısal Araç Ruhsatı İçin Web Tabanlı Bir Prototip Geliştirilmesi, Gazi Üniversitesi, 2006

[17] DPT, Bilgi Toplumu Stratejisi (2006 – 2010), Ankara, 2006

[18] RANKL, W., EFFING, W., Smart Card Handbook, Germany, 2002

[19] ŞAHİN, M., Smart Kart Özellikleri Ve Smart Kart Kullanılarak Kapı Kontrolünün Tasarımı, Sakarya Üniversitesi, 2004

[20] TRASK, N. And MEYERSTEIN, M., "Smart Cards in Electronic Commerce", BT Technol J., 1999.

[21] http://www.scantec.de/modules.php?name=News&file=article&sid=229

[22] BİNİCİ, A., Bilgi sistemlerinde açık anahtar altyapısı kullanımı, Sakarya Üniversitesi, 2005

[23] SAKALLI, M., Modern şifreleme yöntemlerinin gücünün incelenmesi, Trakya Üniversitesi, 2006

[24] http://en.wikipedia.org/wiki/Triple_DES

[25] YERLİKAYA, T., Yeni şifreleme algoritmalarının analizi, Trakya Üniversitesi, 2006

[26] EREN, A., Açık anahtarlı kriptografi, Penguence Sayı:2, 2005

[27] GUTHERY, S., JURGENSEN, T., Smart Card Developer's Kit, 1999

[28] ALBAYRAK, S., PIC mikrodenetleyicisi ile akıllı kartlarda dinamik güvenlik algoritmasının oluşturulması, Sakarya Üniversitesi, 2004

ÖZGEÇMİŞ

Ahmet ŞANSLI 1983 yılında Kırcali'de doğdu. İlk ve orta öğrenimini İstanbul'da gördükten sonra 2001 yılında kazandığı Sakarya Üniversitesi Bilgisayar Mühendisliği bölümünü 2005 yılında bitirerek, Sakarya Üniversitesi Bilgisayar ve Bilişim Mühendisliği EABD'da yüksel lisans eğitimi yapmaya başladı aynı zamanda, Bilgi İşlem Dairesi Başkanlığı'nda yazılım uzmanı olarak çalışmaya başladı.