Ödeme Kaydedici Cihaz Ortamlarında Yeni TCKK ve EKDS Ortamlarının Adaptasyonu/Entegrasyonu

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Ramazan Yoldaş
tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

İstanbul Şehir Üniversitesi

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Prof. Dr. Ensar Gül ....
(Tez Danışmanı)

Dr. Oktay Adalıer
(Tez Eş-danışmanı)

Prof.Dr Nizamettin Aydın ....

Yrd. Doç. Dr Onur Güzey ....

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 24.01.2017

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Ramazan Yoldaş, başlığı, 'Ödeme Kaydedici Cihaz Ortamlarında Yeni TCKK ve EKDS Ortamlarının Adaptasyonu/Entegrasyonu' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza:

Tarih: 24.01.2017

"Şans, yalnızca hazır olan zihinlere güler."

L.Pasteur

Ödeme Kaydedici Cihaz Ortamlarında Yeni TCKK ve EKDS Ortamlarının Adaptasyonu/Entegrasyonu

Ramazan Yoldaş

Öz

Günümüzde bilişim teknolojilerindeki gelişmeler, birçok alanda olduğu gibi kamu uygulamalarında da yeni bir anlayışı ortaya çıkarmıştır. Elektronik devlet (e-devlet) diye adlandırılan bu oluşum kapsamında, kamunun elindeki bilgiler elektronik ortamda, çevrimiçi olarak vatandaşlara ve kurumlarla paylaşılmaktadır. Bu yaklaşım, bir taraftan kurumların hizmet sunumunda ihtiyaç duyduğu bilgileri diğer kurumlardan anında alabilmesini, diğer yandan da vatandaşın kamu kurumlarındaki işlerini elektronik ortamda yapabilmesini sağlamaktadır. Ayrıca vatandaşı hizmetin odağına koyarak, vatandaş ağırlıklı bir sistemin giriş kapısı olmaktadır. Yakın zamanda kullanıma sunulan Türkiye Cumhuriyeti Elektronik Kimlik Kartı bu oluşumda önemli bir rol oynamaktadır. Elektronik Kimlik Kartları üzerinde sunulacak olan Chip&PIN doğrulama yöntemi bugün itibariyle tüm banka kartları için kullanılan EMV standardı olan Chip&PIN doğrulama yöntemleri ile güvenlik açısından aynı seviyede bir güvenlik sunmaktadır. Bu çalışma kapsamında; geçmişten günümüze kadar kullanılan nüfus kâğıtlarının yerini alacak olan Elektronik Kimlik Kartları ile Gelir İdaresi, TÜBİTAK ve yazarkasa firmaları tarafından ortak yürütülen ve kullanıma sunulan IP Tabanlı Yeni Nesil Ödeme Kaydedici Cihazlarının entegrasyonu, bu entegrasyonun gerekliliği, sağladığı faydaları, getireceği yenilikleri ve entegrasyon çözümü ele alınmaktadır.

Anahtar Sözcükler: Yeni nesil ödeme kaydedici cihaz, yazar kasa, elektronik kimlik kartı, akıllı kart

Saygıdeğer aileme ve sevgili nişanlıma . . .

Teşekkür

Bu çalışmam süresince her türlü yardım ve desteği sağlayan; bilgi, tecrübe ve teşvikleri ile çalışmama ışık tutan danışmanım Sayın Dr. Oktay Adalıer' e teşekkür ederim.

Tezimin hazırlanması sırasında destek sağlayan değerleri arkadaşlarıma, manevi desteklerini esirgemeyen aileme ve nişanlıma teşekkürü bir borç bilirim.

İçindekiler

Şekil Listesi

Kısaltmalar

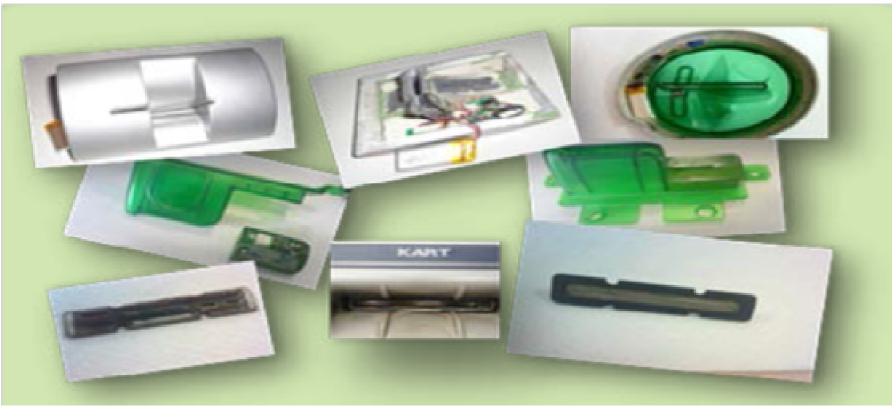
ABD	**A**merika **B**irleşik **D**evletleri
AES	**A**dvanced **E**ncryption **S**tandard
API	**A**pplication **P**rograming **I**nterfaces
EFT	**E**lektronik **F**on **T**ransfer
EFT POS	**E**electronic **F**unds **T**ransfer at **P**oint **Of S**ale
EKDS	**E**lektronik **K**imlik **D**oğrulama **S**istemi
ERP	**E**nterprise **R**esource **P**lanning
ESHS	**E**elektronik **S**ertifika **H**izmet **S**ağlayıcı
GİB	**G**elir **I**daresi **B**aşkanlığı
GMP	**G**elir **İ**daresi **B**aşkanlığı
HSM	**H**ardware **S**ecurity **M**odule
IP	**I**nternet **P**rotocol
ISO	**I**nternational **O**rganization for **S**tandardization
İETT	**İ**stanbul **E**elektrik **T**ramvay ve **T**ünel **İ**şletmeleri
KDBO	**K**imlik **D**oğrulama**B**aşarım **O**nayı
KDP	**K**imlik **D**oğrulama **P**rotokolü
KDPS	**K**imlik **D**oğrulama **P**olitika ve **S**unucusu
KDS	**K**imlik **D**oğrulama **S**unucusu
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol
OKTEM	**O**rtak **K**riterler **T**est ve **D**eğerlendirme **M**erkezi
PCI-PTS	**P**ayment **C**ard **I**ndustry **PIN T**ransaction **S**ecurity
PIN	**P**ersonal **I**dentification **N**umber
POS	**P**oint **Of S**ale
RSA	**R**ivest **S**hamir **A**dleman
SAM	**S**ecure **A**ccess **M**odule

SİL	**S**ertifika **İ**ptal **L**istesi
SM	**S**ertifika **M**akamı
SMS	**S**hort **M**essage **S**ervice
SSL	**S**ecure **S**ocket **L**ayer
TCKK	**T**ürkiye **C**umhuriyeti **K**imlik **K**artı
TCKN	**T**ürkiye **C**umhuriyeti **K**imlik ve **N**umarası
TSM	**T**rusted **S**ervice **M**anager
TÜBİTAK	**TÜ**rkiye **Bİ**limsel **T**eknolojik **A**raştırma **K**urumu
UEKAE	**U**lusal **E**elektronik ve **K**riptoloji ve **A**raştırma **E**nstitüsü
VPN	**V**irtual **P**rivate **N**etwork
YNÖKC	**Y**eni **N**esil **O**deme **K**aydedici **C**ihaz

Bölüm 1

Giriş

Banka kartlarının üçüncü kişilerce haksız kullanımı neticesinde birçok kart kullanıcısı mağdur olmaktadır. Bu duruma banka kartı sahibinin hatası sebep olabildiği gibi online alışveriş yapılan sistem ya da POS cihazı kullandıran işyerlerinin ihmali de neden olabilmektedir. Bu istenmeyen durumun en büyük sebebi banka kartının teknik altyapısının kolay bir şekilde kopyalanmaya izin vermesinden kaynaklanmaktadır. Kopyalama işlemi Şekil 1.1' de görülen Skimmer(kopyalama) cihazlarının, Şekil 1.3' de gösterildiği gibi ATM'lere takılması ile kartın arka yüzünde yer alan manyetik şerit üzerindeki bilgiler kopyalanmakta, ATM klavyesi üzerine yerleştirilen sahte bir klavye veya Şekil 1.2' de görülen mini bir kablosuz kamera ile de şifre elde edilme işlemi gerçekleşmektedir. Böylelikle kart kullanıcısı farkına varmadan kart hesabı hızlı bir şekilde boşaltılmaktadır [2].



Şekil 1.1: Kopyalama İşleminde Kullanılan (Skimmer) Kopyalama Cihazı Örnekleri

ATM tavanına yapıştırılan plastik düzeneğin içine gizlenen cep telefonunun kamerası kullanılarak kullanıcının klavye hareketleri gözlemlenmektedir.

Şekil 1.2: Kopyalama İşleminde ATM' ye Takılan Kamera Düzeneği

Her yıl ortalama 10 binden fazla kart kopyalama olayı ve ortalama 500 milyon euro' luk bir kayıp söz konusu olmaktadır[3]

Şekil 1.3: Kart Kopyalama Düzeneğinin ATM' ye Yerleşimi

Banka kartlarının haksız kullanımı ile ilgili sorumlu olan tarafı her ne kadar kanunlar belirlemiş olsa da kanunla ilgili maddelerin eksiklerinden ve bankaların sorumluluktan kaçmasından kaynaklanan mağduriyetlerin önüne geçilememektedir. Yakın dönemde kullanıma sunulan Elektronik Kimlik Kartları' nın sahip olduğu altyapı bize bu kartların banka kartı olarak da kullanılabileceğini göstermektedir. Kart içerisinde yer alan elektronik veriler, kriptografik anahtarlar ile korumalı olarak saklanabilmektedir. Bunun yanı sıra içinde tuttuğu özel kriptografik anahtarları ve bu anahtarlarla ilişkili olan sayısal sertifikaları sayesinde ataklara karşı dirençli bir belleği de içermektedir [27]

Akıllı kart işletim sisteminin milli olması hem maddi açıdan hem de güvenlik açısından birçok fayda sağlamaktadır. Güvenlik açısından değerlendirildiğinde, işletim sistemi yalnız ülkemize özgü olduğu için üçüncü şahıslar tarafından içeriğinin bilinememesi ile beraber içeriğinde güvenlik açığı yaratabilecek kodların bulunmadığından emin olunmaktadır. İşletim sistemi Common Criteria EAL4+ seviyesinde güvenlik sağlamaktadır.

Kimlik kartının temaslı arayüzü için tasarlanan yonga tamamen özgün, ulusal kaynaklı ve uluslararası standartları destekleyecek özellikler taşımaktadır. Sahip olduğu Common Criteria EAL 5 + güvenlik seviyesi ve tümdevre yüzeyinin saldırılara karşı etkin kalkan ile korunması, lazer ve hata saldırılarını algılama ve yan kanal analizlerine karşı önlemleri ile güvenlik, işlevsellik, performans, fiyat açılarından rekabet gücü oluşturarak elektronik devlet, bankacılık gibi güvenlik uygulamaları için güvenilir bir seçenek oluşturmaktadır. Kartın sahip olduğu temaslı yonga sayesinde yeni nesil ödeme kaydedici cihazlarla belirli güvenlik protokolleri ile haberleşebilmektedir. Yeni Nesil Ödeme Kaydedici Cihazlar içerdikleri Secure IC' den dolayı TCKK ile yaptığı bütün işlemleri güvenilir bir şekilde gerçekleştirebilmektedir. Secure IC, TCKK ile haberleşmesi sırasında kriptografik anahtarların ve parametrelerin saklandığı yer için uygundur.

Kimlik kartları, vatandaşların sahip oldukları ve yalnızca kendilerinin bileceği PIN kodları sayesinde kamu ve özel sektör uygulamalarında Chip&PIN doğrulaması yapılmasına imkân verebilmekte; ayrıca bünyesinde barındırdığı biyometrik özellikleri ile (parmak izi, damar izi, avuç içi izi) gerekli görüldüğü durumlarda vatandaşların biyometrik doğrulamalarının da yapılmasını sağlayabilmektedir. Mevcut durumda 11 farklı doğrulama yöntemi ile doğrulanabilecek Eleketronik Kimlik Kartları' nın doğrulama yöntemleri incelendiğinde; "Chip&PIN" doğrulama yönteminin gerek ihtiyaç duyulan asgari güvenlik şartlarını sağlaması gerekse geniş sektörel kullanım yaygınlığına ulaşabilmesi açısından en ideal olan yöntem olduğu görülmektedir. Chip uygulaması kartın kopyalanmasının önüne geçmekte, PIN işlemi ise çalınmış kartların üçüncü kişi tarafından kullanımını engellemektedir[26]. Chip&PIN doğrulama yönteminin üzerine ek bir güvenlik seviyesine ihtiyaç duyulan özel uygulamalarda ise biyometrik doğrulama yönteminin kullanımı sektörel oyuncuların kendi tercihlerine bırakılmaktadır. Chip&PIN doğrulama yöntemi, bugün itibariyle tüm banka ve kredi kartları için kullanılan EMV standardı olan Chip&PIN doğrulama yöntemleri ile güvenlik açısından aynı seviyede bir güvenlik sunduğu görülmektedir[4].

Bu değerlendirmeler çerçevesinde, e-kimliklerin Chip&PIN doğrulaması ile kullanılabilmesi sayesinde gerek yüz yüze bankacılık kanallarında(şube) gerekse mesafeli bankacılık kanallarında(Internet Bankacılığı, Mobil Bankacılık, ATM, vb.) finansal tüketicilerin kolaylıkla ve güvenli bir şekilde doğrulanabilmeleri mümkün olmaktadır. Bu vesile ile gerek sürekli iş ilişkilerinin ilk tesisi süreçlerinde, gerekse de mevcut müşterilerin şube ve mesafeli bankacılık ara yüzlerine erişiminde e-kimlik kullanılabilir hale gelmektedir[4].

Bu çalışma kapsamında; Elektronik Kimlik Kartları ile IP Tabanlı Yeni Nesil Ödeme Kaydedici Cihazlarının entegrasyonu, bu entegrasyonun faydaları, entegrasyon çözümü ve gerekli olan idari ve mevzuatsal süreçler ele alınmaktadır. Bu entegrasyon ile TCKK' nın taklit ve tahrif edilememesi özelliği ile banka kartlarının kopyalanmasından dolayı oluşan mağduriyetlerin önüne geçilmesi sağlanmakta, hizmet veren kurum hizmeti alan vatandaştan emin olmakta, gereksiz yere banka kartı taşımanın önüne geçilmektedir. Banka aidat ücretleri gibi vatandaşların üzerine oluşan külfet kalkmakta ve bankalara olan bağımlılık azalmaktadır. Bu entegrasyonun başlıca hedefleri:

- TCKK' nın taklit ve tahrif edilememesi özelliği ile banka kartlarının kopyalanması ile oluşan mağduriyetlerin önüne geçilmekte, hizmet veren kurum hizmeti alan vatandaştan emin olmakta ayrıca, gereksiz yere banka kartı taşımanın önüne geçilmekte, banka aidat ücretleri gibi vatandaşların üzerine oluşan külfet kalkmakta ve bankalara olan bağımlılık azalmaktadır

- TCKK, vatandaşa ait nüfus, fotoğraf ve parmak izi bilgilerini temaslı yonga üzerinde güvenli bir şekilde sakladığı için ödeme işlemlerinde kimlik doğrulama biyometrik veriler ile de gerçekleştirilebilmektedir. ÖKC' ler mevcut durumda biyometrik veri alma ve o veri ile doğrulama yapmak için gerekli donanımsal ve yazılımsal altyapıyı sunmaktadır

- Kimlik kartının temaslı ara yüzü için tasarlanan yonga, tamamen özgün, ulusal kaynaklı ve uluslararası standartları destekleyecek özellikler taşımaktadır. Sahip olduğu Ortak Kriter EAL 5 + güvenlik seviyesi ve işlevsellik, performans, fiyat açılarından rekabet gücüyle,e-devlet, bankacılık gibi uygulamalar için güvenilir bir seçenek oluşturmaktadır. E-Kimlik Projesi kapsamında kazanılan akıllı kart çip tasarımı ve üretimi konusundaki bilgi birikimi ciddi bir yurtdışı bağımlılığını ortadan kaldırmaktadır.

- Kimlik kartındaki temaslı yonga, kart sahibine ait nitelikli elektronik sertifikanın (NES) yüklenebilmesine olanak sağlamaktadır. Kart sahibi, kimlik kartının elektronik imza (NES) fonksiyonunu kullanmak istediğinde, Bilgi Teknolojileri ve İletişim Kurumu tarafından yetkilendirilmiş ve elektronik imza konusunda faaliyet gösteren herhangi bir özel Elektronik Sertifika Hizmet Sağlayıcı' dan (ESHS) kimlik kartına elektronik imza sertifikası yükletebilmektedir. Kişi, sahip olduğu kart üzerindeki elektronik imza fonksiyonu sayesinde elektronik ortamda gerçekleştirilen işlemlerde ıslak imzası gibi birebir olarak hukuksal bağlayıcılığı olan elektronik imzasını da atabilmektedir. Vatandaşların, başka bir akıllı kart olmaksızın, elektronik ortamlarda ıslak imza ile eşdeğer olan nitelikli elektronik imzanın atılmasını sağladığı için büyük miktarda ödeme işlemlerinde ve para transferlerinde başka herhangi bir onay koduna gerek kalmadan işlemi gerçekleştirerek hizmeti veren kuruma ve hizmeti alan vatandaşa kolaylık sağlayabilmektedir. Ayrıca, Yeni Nesil Ödeme Kaydedici Cihaz' larda mevcut olan sanal pos işlemleri ile online olarak para transferi ve alışveriş de yapılabilmektedir.

- ÖKC ve TCCKK' nın entegre çalışması ile kimlik doğrulama ile ödeme gerektiren (sağlık, finans, e-devlet, e-ticaret, sigorta vb.) gibi yerlerde vatandaşa kolaylık sağlanmakta, bürokrasi azaltılmakta aynı zamanda kağıt israfı da önlenmektedir.

- Kimlik kartı şifresi girilerek veya biyometrik veri (parmak, parmak damar izi veya el aya izi) okutularak hesaba erişilebildiği için PIN kodu hatırlanmadığı durumlarda kullanım kolaylığı sağlamaktadır.

- Elektronik kimlik kartları çoklu kimlik doğrulama faktörlerini desteklediği için ödeme işlemlerindeki güvenlik seviyesi kullanıcı tarafından belirlenebilmektedir.

- Bu entegrasyon sayesinde kurumların sunduğu online ödeme işlemlerinin nitelikleri ve sayıları artmaktadır.

- Kurumlar tarafından sunulan farklı hizmetlerde, hizmetin niteliğine göre kimlik doğrulama faktörleri seçilebilmektedir.

- Çoklu kimlik doğrulamayı desteklediği için ödeme tutarı bazında kimlik doğrulama yöntemi belirlenebilmektedir.

- Bankalar, vatandaşa yönelik hizmetlerde elektronik iş süreçlerini destekleyen elektronik kimlik kartları ile entegre çalışarak bürokrasi azaltılmakta ve uzaktan ödeme ile (kurumun uç noktasına gitmeden ve başka bir ödeme sistemi veya uygulaması kullanmadan) aynı kart ile hem ödeme hem de kimlik doğrulama işini elektronik ortam da daha hızlı çözebilmektedir.

- Vatandaş üzerinde hem kimlik doğrulama hem de ödeme işlemini yapan kartları taşımak yerine bu işlemlerin her ikisini de içeren akıllı kimlik kartı taşımaktadır. Bulunmasını istediği banka hesaplarını birleştirerek tek kart, tek şifre ile işlem yapma kolaylığı sağlamaktadır.

- Ödeme gerektiren elektronik hizmetlerde internetin bulunduğu her yerden (ev, işyeri vb.) işgücü harcamadan 7/24 erişilebilmektedir.

- Banka hizmetlerinden yararlanan kişilerin hak sahipliği denetimi kolay ve güvenli bir şekilde yapılabilmektedir.

2.bölümde, birçok ülkenin kimlik kartları incelenmiş, kimlik kartlarının hangi uygulamaları desteklediği açıklanmıştır. 3.bölümde, konunun daha iyi anlaşılması için entegrasyon kapsamında bahsi geçen Yeni Nesil Ödeme Kaydedici Cihaz'lar, Türkiye Cumhuriyeti Kimlik Kartları, Elektronik Kimlik Doğrulama Sistemi hakkında bilgiler verilmiş, TCKK' nın ÖKC ortamlarında kullanılma ihtiyacından ve TCKK ÖKC entegrasyonun başlıca hedeflerinden bahsedilmiştir. 4.bölümde, Ticarette ÖKC kullanımından, ÖKC projesinde yer alan Gelir İdaresi Başkanlığından, Güvenli Servis Sağlayıcı' lardan (TSM), ÖKC' nin teknik özellikleri ve haberleşme topolojisinden bahsedilmiştir. 5.bölümde, TCKK ve EKDS hakkında daha fazla detaya girilmiş, kimliğin tarihçesi, TCKK içindeki bilgiler, TCKK' nın özellikleri, TCKK açık anahtar altyapısı, EKDS' nin içeriği, amaç ve hedeflerinden detaylı olarak bahsedilmiştir. 6.bölümde, TCKK' nın ticarette kullanım analizinden bahsedilip 7.bölümde bu entegrasyon için örnek bir senaryo verilmiş ve bu senaryo kapsamında yazılmış olan test uygulamasından detaylı olarak bahsedilmiştir. 8.bölümde TCKK' nın ÖKC ile kullanımında tamamlanması gereken idari ve mevzuatsal süreçler üzerinde durulmuş ve 9.bölümde çözümün endüstride uygulanma fizibilitesi anlatılmıştır. Son bölümde olan 10.bölümde ise çalışmanın kattığı yeniliklerden bahsedilmiş, hedefleri değerlendirilmiş, sonuçlar yorumlanmış ve gelecekte yapılabilecek çalışmalara yönelik önerilerde bulunulmuştur.

Bölüm 2

İlgili Çalışmalar

Akıllı kartların kimlik kartı olarak kullanılmasına ilk olarak Malezya tarafından 2001 yılında başlanmıştır. Daha sonra Malezya'yı 2002 yılında Estonya takip etmiştir. Estonya' da kullanıma geçen kimlik kartı fiziksel kimlik ve elektronik kimlik olarak işlev görecek şekilde oluşturulmuştur. Gömülü bir PKI uygulaması içeren bu kart, elektronik sertifikalarla çevrimiçi kimlik doğrulama ve dijital imza sağlamaktadır [5].

Hükümet, özel sektörde e-kimlik kullanımında herhangi bir kısıtlama koymamıştır.Kimlik doğrulama mekanizması, herhangi bir dış geliştirici tarafından kullanılabilmekte, tanımlama ve kimlik doğrulama için e-kimliği kullanan bir uygulama geliştirebilmektedir. Kimlik kartları, çevrimiçi banka işlemlerine yetki vermek, sözleşmeleri ve vergi beyannamelerini imzalamak, kablosuz ağlara kimlik doğrulaması yapmak, devlet veritabanlarına erişmek, sağlık hizmetlerine erişmek, sürücü veritabanı ile entegre olarak ehliyet olarak kullanılmaktadır. Estonya ayrıca, mobil telefonlar için elektronik kimliği Mobil ID' yi de başlatmıştır. Elektronik kimlik kartında olduğu gibi, Mobil-ID de bireylerin kendilerini tanıtmalarını ve belgeleri dijital olarak imzalamalarını sağlayan sertifikalar içermekte ve bu sertifikaları cep telefonlarında kullanılan SIM kartında saklamaktadır. Birçok dijital hizmet, kişilerin kimlik kartı yerine Mobil ID' yi kullanmasına izin vermektedir. Sonuç olarak Estonya' da e-kimlik' e herhangi bir sınır getirilmemiş tüm uygulamalarda kullanılması hedeflenmiştir. Ayrıca yabancılar için de bu hizmet sunulmaktadır [5]. Kimlik kartının banka işlemleri için kullanılmasını, geniş kullanım alanı ve daha fazla güvenlik sağladığı için büyük bankalar tarafından teşvik edilmektedir. Estonya da Tüm bankacılık işlemlerinin %98 internet üzerinden yürütülmektedir. Ülkede elektronik imza kullanımı, Estonya GSYİH' sinin % 2'si kadar yani Estonya savunma bütçesi büyüklüğü kadar tasarruf etmesine yardımcı olmaktadır [6].

Portekiz Kimlik kartları 2007 yılından itibaren yaygınlaştırılmaya başlanmıştır. Kimlik kartlarının elektronik ortamda kimlik doğrulama, tanıma ve imza atma fonksiyonlarına sahip olması hedeflenmiştir. Birçok banka ve kamu uygulamalarında kullanılmaktadır. Ayrıca kart Avrupa Birliği ülkelerinde seyahat belgesi niteliği de taşımaktadır [1].

İsveç' de devlet tarafından düzenlenen tek bir e-kimlik kartı oluşturmak yerine, özel sektörle ortak bir şekilde bir e-kimlik sistemi oluşturulmuştur. Biri kimlik doğrulamak, biri de imzalama olmak üzere 2 sertifika içermektedir. İsveç'te e-kimlik belgelerinin kullanımı kamu ve özel sektör arasında oldukça eşit olarak bölünmüştür. Çeşitli devlet hizmetleri, kişilere vergilerin gönderilmesi, İsveç Sosyal Sigorta Kurumu'ndan hizmetler alınması, ehliyet başvurusu yapılması ve yenilenmesi ve araçların kaydedilmesi gibi işlemler de elektronik kimlik kartının kullanılmasına izin verilmektedir [5].

Almanya'da 2010 yılında biyometrik veriyi destekleyen kimlik kartı dağıtımına başlanması planlanmasına rağmen henüz başlatılmamıştır. Çevrimiçi e kimlik ve biyometrik veri kullanımı vatandaşın isteğine bırakılmıştır. Kimlik kartının; elektronik ortamda kimlik doğrulama, elektronik imza atma, seyahatlerde kimlik doğrulama amaçlı olmak üzere 3 temel fonksiyona sahip olması hedeflenmiştir [7].

Avusturya kimlik kartı, vatandaşların elektronik olarak kamu makamlarına kendilerini tanıtmalarına ve sözleşmeler veya hükümet formları gibi belgeleri imzalamalarına izin vererek e-devlet uygulamalarına olanak tanımaktadır. Tek bir elektronik kimlik türünün aksine, Avusturya Vatandaşlık Kartı birçok biçim alabilmektedir [5]. Avusturya hükümeti, vatandaşların devlet kimlik kartları, banka kartları, sağlık sigortası kartları ve cep telefonları da dâhil olmak üzere hem kamu hem de özel sektörden çeşitli fiziksel belirteçlerde e-kimlik özelliğini etkinleştirmesine olanak tanımaktadır. Örneğin, Mart 2005'ten bu yana, Avusturya bankaları tarafından yayınlanan tüm banka (ATM) kartlarının, Avusturya yasalarına göre bir elektronik imza oluşturabilecekleri resmi, güvenli imza oluşturma araçları olması gerekmektedir [8]. Bütün vatandaşlık kartları, kişinin adı ve doğum tarihi de dâhil olmak üzere temel kişisel bilgileri saklamaktadır. Buna ek olarak, her kişiye sourcePIN olarak bilinen benzersiz bir tanımlayıcı atanır. SourcePIN, merkez kayıtlarındaki verilerden türetilir ve vatandaşlık kartı üzerinde saklanır. Numaranın amacı, yalnızca isim ve doğum tarihi gibi verilere dayandığında ortaya çıkabilecek bir kişinin kimliğiyle ilgili belirsizliklerin ortadan kaldırılmasına yardımcı olmaktır. Vatandaşlık kartları (Citizen kartları), bireylerin belirli bir e-posta adresine bağlanmayı seçebilecekleri dijital imza için dijital bir sertifika da içermektedir. Vatandaşlık kartı, kart sahibini başka bir kişi veya tüzel kişilik adına hareket etmesi için yetkilendiren bir elektronik görev süresi de içerebilmektedir. Genel olarak, kişiyi tanımlamak için gereken minimum bilgi miktarı her kartta saklanmaktadır [9]. Avusturya e-kimlik sistemi Avusturya'ya özgü bir özellik olan yabancı e-kimliklerle birlikte çalışabilmektedir. Bugüne kadar, Avusturya e-kimlik sisteminde Belçika, Estonya ve İtalyan e-kimlik belgelerinin kullanılmasına izin verilmeye çalışılmıştır. Merkezi Kayıt Kuruluşu ile listelenmeyen, Avusturyalı olmayanlar ek kayıt defterine eklenmekte ve kendi kimlik numaralarına (örneğin, İtalyan kimlik kartlarıyla kullanılan vergi numarası gibi) ait benzersiz tanımlayıcı temelli bir kaynakPIN atanmaktadır. Sistem yabancı e-kimliklerini kabul etmek için uygunken, uygulamalar henüz bu işlevselliğe göre tasarlanmamıştır, bu nedenle yabancıların kullanımı sınırlı olmaktadır [10]

2004 yılında başlatılan Belçika'daki kişisel kimlik kartı, dokuz milyondan fazla e-kimliği dolaşımda bulunmasıyla Avrupa'daki en büyük ulusal e-kimlik sistemidir [11]. Belçika vatandaşları için zorunlu tutulan kimlik kartı, yabancıları da kapsamaktadır. Yabancılar için sunulan hizmet AB'deki yabancı uyruklu kişiler ve AB dışından yabancı uyruklu kişiler olmak üzere 2 çeşittir. Tüm kartların varsayılan olarak etkinleştirilmiş kimlik doğrulama ve imza özellikleri vardır; Ancak kullanıcılar bu özelliklerin kapsamı dışında kalmayı seçebilirler. Kartta saklanan dijital sertifika e-devlet uygulamalarında vatandaşın kimliğini doğrulamak için kullanılmaktadır. Vatandaşlar kimlik kartını, elektronik vergi bildirimlerini dijital olarak imzalama gibi çeşitli uygulamalar için kullanabilmektedir [5].

Yaklaşık 174 milyon nüfusu ile Afrika'nın devi olarak bilinen Nijerya, 2014 yılında elektronik kimlik kartı programı ile Afrika Kıtası' nın en büyük finansal projesini başlatmıştır. Ödeme teknolojisinin ve uygulamaların güvenliği, MasterCard' ın sunduğu güvenlik ile sağlanmıştır. Bu program, kapsayıcı vatandaşlığı, daha etkili yönetimi ve nakitsiz bir ekonomiyi yaratmayı amaçlamaktadır; bunların hepsi de Bu proje nin ekonomik büyümeyi, yatırımı ve ticareti teşvik edeceği düşünülmektedir. Bu projenin Master Card ile ortak yürütülmesinde;

- MasterCard' ın tecrübe ve bilgi birikimini Nijerya Hükümeti ile paylaşma isteği,

- MasterCard' ın esnekliği, aktif oluşu ile hükümetin sorularına ve ihtiyaçlarına hızlı cevaplar vermesi. (MasterCard ekibi, ilişkileri boyunca hükümetten ipuçları almış ve gerektiğinde rehberlik ve destek sağlamıştır),
- Hükümetin, programın mülkiyetine, kontrolüne ve vatandaşlarının veritabanını korumak amacına yönelik isteğine MasterCard' ın saygı göstermesi,

etkili olmuştur. Şekil 2.1'de MasterCard logolu Nijerya kimlik kartının ön ve arka yüzü görünmektedir [12].

Şekil 2.1: Nijerya Kimlik Kartı

Nijerya Elektronik Kimlik Kartı ilk aşamada, ICAO standartlarına dayalı ulusal kimlik ve seyahat belgesi olarak kullanılmaktadır, ikinci aşamada ise, e-voting, e-sağlık, e-hizmet, ehliyet gibi işlemlerde de kullanılması planlanmaktadır. Nijerya'nın yeni ulusal kimlik kartı, çeşitli elektronik hizmetler ve uygulamalar için anahtarlar, sertifikalar ve kişisel ve biyometrik verilerin (parmak izi) saklanması için bir mikroişlemci ile donatılmıştır [12].

Bölüm 3

İlgili Temel Bilgiler

Bu bölümde, gerçekleştirilen entegrasyon kapsamında kullanılacak kavramlar ayrıntılı olarak açıklanmıştır.

3.1 Ödeme Kaydedici Cihaz ve Kullanım Ortamı

Yeni nesil ödeme kaydedici cihazlar, klasik yazarkasalar ile kredi kartları için kullanılan POS cihazlarının özelliklerini bir arada bulunduran, IP tabanlı iletişim yapılı, anlık olarak Gelir İdaresi Başkanlığı ve bankalar ile veri alışverişi yapma yeteneğine sahip, çoklu ortak pos kombinasyonu ile entegre edilmiş cihazlardır. Başlıca kullanım alanları;

- Fatura Tahsilât Merkezleri
- Havalimanları, Eczacılık Sektör Çözümleri
- Mobil Ödeme Noktaları
- Otopark Sektörü
- Restoran Sektörü (Adisyon Sistemi, Yemek Çeki ve Seyyar Ödeme)
- Su, Tüpçü v.b. Seyyar Hizmetlere Yönelik Çözümler
- Muhasebe Programlarına Entegrasyon
- Eğlence Sektörü Biletleme Sistemi

- Toplu Taşıma Biletleme Sistemi
- Zincir Mağaza ve Marketler

Kayıt dışı ekonomi ile mücadele eylem stratejisi doğrultusunda IP Tabanlı akıllı yazar kasa pos sistemi vergi kayıplarının önlenmesi, vergi kaçaklarının minimize edilmesi; adil olarak düzenli kayıtlar tutulması ve daha az maliyet ile sürekli olarak mali kontrolün sağlanması için en uygun çözüm olarak görülmektedir.

Daha önceki sistemde kural koyucular bankalardı ve mükellefe banka seçme şansı bırakmıyordu bu sistemde ise, mükellefin isterleri belirleyici olmaktadır ve hangi banka ile isterse onunla çalışma imkânı bulmaktadır. Tüketici ise kredi kartı ile ödeme yapmada herhangi bir sorun yaşamamaktadır. Yazar kasa ve POS cihazının ortak bir yapıda buluşması ile iki farklı cihazda gerçekleşen işlem tek bir cihazda gerçekleşmektedir. Böylelikle kredi kartı ile yapılan her ödeme işleminde alışverişin fişi istisnasız olarak kesilmektedir. Bu sistemle Türkiye genelinde 5 ila 10 milyar lira arası vergi kaybı önlenmiş olmaktadır. Diğer yandan tüm bankaların pos yapısını bir araya toplayarak iş yerlerinde pos cihazı bulunduran tüm işletmelere daha fazla satış alternatifi sağlamakta ve bir yazarkasa yanında 3-5 pos ile çalışma zahmetinden kurtarmaktadır. Ayrıca işyeri tarafından herhangi bir mal veya hizmet sunulmadan, kredi kartından çekim yapılması karşılığında nakit para alınması ve kredi kartlarının borçlarının ödenmesi gibi POS' un amaç dışı kullanılarak haksız kazanç elde edilmesi olarak tanımlanan pos tefeciliğinin de önüne geçilmektedir.

3.2 TCKK (Türkiye Cumhuriyeti Kimlik Kartı)

Ülkemizde her vatandaşa tekil T.C. Kimlik Numarası verilmiştir. Bu uygulama, kamu/özel sektörde yapılan işlemlerde kolaylığın yanında bir takım güvenlik zafiyetlerini de beraberinde getirmektedir. Örneğin vatandaşın T.C. Kimlik Numarası'na ulaşan biri, onun birçok mahrem bilgisine hakkı olmadığı halde elektronik ortamda erişebilmektedir. Birçok yere vermiş olduğumuz nüfus cüzdanları fotokopilerinin yanlış kişilerin eline geçmesi sonucu; başkası üzerine kredi kartı açma, şirket kurma, GSM hattı açma ile oluşan mağduriyetlerin önü alınamamaktadır. Tüm hususular değerlendirildiğinde hızla gelişen teknoloji günümüzde kimlik kartının nüfus cüzdanından farklı, diğer bir deyişle "akıllı" olmasını zorunlu hale getirmiştir.

Bilgi ve iletişim teknolojilerindeki yenilikler, gerek kamu gereke özel sektör uygulamalarında yeni bir anlayışı ortaya çıkarmıştır. Bu anlayış, kamu ve özel sektör tarafından sunulan hizmetlerin elektronik ortama alınması şeklindedir. Elektronik ortama aktarılan hizmetler sayesinde vatandaş; hizmet noktasına gitmeden, gereksiz zaman ve işgücü harcamadan kamu ve özel sektör hizmetlerinden yararlanabilmektedir. Gerek kamu gerekse özel sektör tarafından elektronik ortamda sunulan hizmetlerin aksamadan kaliteli bir şekilde yürütülebilmesi ancak doğru kişinin hizmet alması ile mümkündür. Kamu ve özel sektör tarafından vatandaşa elektronik ortamda sunulan hizmetlerde, vatandaşın kimliğinin elektronik ortamda güvenli bir şekilde doğrulanabilmesi gerekliliğini ortaya çıkarmaktadır. Kimlik kartı da bu temel ihtiyacı karşılayabilecek yegâne alternatif olarak görülmektedir.[13]

T.C. Kimlik Kartı, vatandaşa ait nüfus bilgilerinin kartın üzerindeki yonga üzerine güvenli bir şekilde kaydedilmesi ve bu işlemden sonra yetkisiz kimseler tarafından yeniden üretilmesini ya da bilgilerinin değiştirilmesini olanaksız hale getirecek şekilde tasarlanması esasına dayanan, görsel ve teknik güvenlik unsurlarına sahip olan bir akıllı karttır [13].

TCKK, vatandaşa ait nüfus, fotoğraf ve parmak izi bilgilerini temaslı yonga üzerinde güvenli bir şekilde saklamaktadır. Kart içerisinde yer alan elektronik veriler, kriptografik anahtarlar ile korumalı olarak saklanabilmektedir. Kullanılan yongalarda, uluslararası ISO/IEC 14443 (Temassız) ve ISO/IEC 7816 (Temaslı) standartları desteklenmektedir. TCKK Üzerindeki Bilgiler (Çip İçindeki Kart Bilgileri: Kişisel Mesaj, Rüşt Mesajı, Biyometrik Hata Sayacı, CVC Sertifikası, Kimlik Doğrulama Sertifikası, Kart Yayıncı Sertifikası, Elektronik İmza Sertifikası (isteğe bağlı) mevcuttur. Kartta saklanacak bilgiler sayesinde bazı hizmetlerin alımı/sunumu kolaylaşmaktadır [13].

3.3 EKDS (Elektronik Kimlik Doğrulama Sistemi)

Kimlik kartı, kullanılması ile birlikte kamu/özel sektör tarafından verilen hizmetlerin alımı ve sunumu kolaylaşacağı için e-hizmetlerin de vazgeçilmez bir bileşeni olacaktır. Bu durum "kimlik kartını elektronik olarak doğrulayabilecek güvenli bir sistemi" zorunlu hale getirmektedir. Bu kapsamda milli, kolay taşınabilir, taklit edilemeyen, tüm kimlik doğrulama fonksiyonlarına sahip, standartlara uygun kimlik kartı ve bu kimlik kartını elektronik ortamda doğrulayabilecek Elektronik Kimlik Doğrulama Sistemi geliştirilmiştir. Elektronik Kimlik Doğrulama sisteminin en önemli özelliği her kurumun kendi ihtiyaçlarına göre uyarlanabilecek kadar esnek bir yapıya sahip olmasıdır. İster kişi bazında isterse uygulama bazında kimlik doğrulama yöntemi seçilebilmektedir [1].

3.4 TCCK' nın ÖKC Ortamında Kullanılma İhtiyacı

Banka kartlarının üçüncü kişilerce haksız kullanımı neticesinde birçok kart kullanıcısı mağdur olmaktadır. Bu duruma banka kartı sahibinin hatası sebep olabildiği gibi online alışveriş yapılan sistem ya da POS cihazı kullandıran işyerlerinin ihmali de sebep olabilmektedir. Bu istenmeyen durumun en büyük sebebi banka kartının teknik altyapısının kolay bir şekilde kopyalanmaya izin vermesinden kaynaklanmaktadır. Kopyalama işlemi, genel olarak ATM'lere bir aparat takılmak suretiyle kartın arka yüzünde yer alan manyetik şerit üzerindeki bilgiler kopyalanması ve ATM klavyesi üzerine yerleştirilen sahte bir klavye veya mini bir kablosuz kamera ile de şifre elde edilmesi ile olmaktadır. Böylelikle kart kullanıcısının farkına varmadan kart hesabı hızlı bir şekilde boşaltılmaktadır [2]. Bu olumsuz durumundan kaynaklanan maddi zararı 5464 sayılı kanunun 8/3 hükmünde "Kart çıkaran kuruluşlar, kartların düzenli ve güvenli kullanımı ile bildirim, talep, şikâyet ve itirazlara ilişkin gerekli tedbirleri almaya yönelik sistemi kurmak ve kesintisiz olarak açık tutmakla yükümlüdür " [14]. belirtildiği üzere bankaları güvenli kullanımı sağlayamadığı için sorumlu kılmaktadır. Her ne kadar 5464 sayılı yasanın 16'ıncı maddesinde banka kartı sahibinin şüpheli durumlarda bildirim zorunluluğu yüklemesine rağmen genelde müşterilerin bunu fark etmeleri mümkün olmamaktadır. Bankalar ise Kart ve PIN birlikte kullanıldığı için sorumluluğu müşteriye atmaktadırlar.

Banka kartlarında yaşanan mağduriyetlerin bir diğeri de online alışverişlerde yaşanmaktadır. Bu alışverişlerde yaşanan mağduriyetlere kimi zaman kart sahibinin ihmali sebep olabilmekte kimi zaman da sistemin güvenlik zafiyetinden kaynaklanmaktaıdr. 5464 sayılı kanunun 15/3 hükmünde "Harcama belgesi düzenlenmeksizin çeşitli iletişim araçları yoluyla veya sipariş formu vasıtasıyla yapılan mal ve hizmet alımlarındaki hukuka aykırı kullanımlardan kaynaklanan zararlardan kart hamili sorumlu tutulamaz" [8] ifadesi yer almaktadır. Yine bu düzenleme ile paralel olarak aynı kanunun 18/2 hükmü "Harcama belgesi düzenlenmeksizin çeşitli iletişim araçları yoluyla veya sipariş formu vasıtasıyla işlem yapılmasına olanak sağlamak üzere kuracakları sistemlerin güvenli bir şekilde çalışmasını temin etmekle yükümlüdür" [14] İfadesi yer almaktadır. Bu iki hükmü birlikte değerlendirdiğimizde sistemlerdeki güvenlik zafiyetinden kaynaklı zararlarda üye işyerleri sorumlu olmaktadır. Yine bankaların müşteri hizmetleri ve diğer uzaktan erişim sistemlerinin hatalarından kaynaklı olarak da zararlar meydana gelebilmektedir. Bu durumda da bankanın sorumluluğu söz konusu olacaktır. Müşterilerin zararın oluşmasında şifre ve korunması gereken bilgileri özenle korumaması durumu mevcut ise bu durumda da birlikte işlenmiş kusurdan söz edilebilmekte ve müşteri de zarardan sorumlu tutulabilmektedir.

Kredi kartlarının kaybedilmesi ve kaybolması da sıklıkla rastlanan problemlerden biridir. Öncelikli olarak 5464 sayılı yasanın 16 maddesi "Kart hamili, kendisine tevdi edilen kartı ve kartın kullanılması bir kod numarası, şifre veya kimliği belirleyici başka bir yöntemin kullanılmasını gerektiriyorsa bu bilgileri güvenli bir şekilde korumak ve başkaları tarafından kullanılmasına engel olacak önlemleri almak, kartın kaybolması, çalınması veya iradesi dışında gerçekleşmiş herhangi bir işlemi öğrenmesi halinde kart çıkaran kuruluşu derhal haberdar etmek zorundadır" [14]. hükmü ile yükümlülükler getirmiştir. Müşteriler kredi kartlarını ve bilgilerini özenle korumak ve kartla ilgili problemi derhâl bankaya bildirmek zorundalar. Kartın kaybolması, çalınması hallerinde kart hamilinin sorumluluğu 5464 sayılı yasanın 12 maddesinde şu şekilde "Kartın ya da 16 ncı maddede belirtilen bilgilerin kaybolması veya çalınması halinde kart hamili, yapacağı bildirimden önceki yirmidört saat içinde gerçekleşen hukuka aykırı kullanımdan doğan zararlardan yüzelli Yeni Türk Lirası ile sınırlı olmak üzere sorumludur. Hukuka aykırı kullanımın, hamilin ağır ihmaline veya kastına dayanması veya bildirimin yapılmaması hallerinde bu sınır uygulanmaz[14]"

Banka kartlarının haksız kullanımı ile ilgili sorumlu olan tarafı her ne kadar kanunlar belirlemiş olsa da kanunla ilgili maddelerin eksiklerinden kaynaklanan ve bankaların sorumluluktan kaçmasından kaynaklanan mağduriyetlerin önüne geçilememektedir. Elektronik kimlik kartlarının sahip olduğu altyapı bize bu kartların banka kartı olarak da kullanılabileceğini göstermektedir. Kart içerisinde yer alan elektronik veriler, kriptografik anahtarlar ile korumalı olarak saklanabilmektedir. Kartın sahip olduğu temaslı yonga sayesinde yeni nesil ödeme kaydedici cihazlarla belirli güvenlik protokolleri ile haberleşebilmekte ve kart kopyalanması ile oluşan mağduriyetlerin de önüne geçilmektedir.

3.5 TCKK ve ÖKC Entegrasyonun Başlıca Hedefleri

- Bankalararası Kart Merkezi (BKM) Şekil 3.1' de görülen 2016 yılı Haziran ayı kartlı ödeme verilerine göre; Türkiye'de 115 milyon banka kartı ve 59 milyon kredi kartı bulunmaktadır [23]. 2015 yılı Haziran ayı ile kıyaslandığında banka kartındaki %5' lik artışa karşın kredi kartı sayısında %2 lik bir artma görülmektedir [23]. Bu rakamlar bize sürekli artan bir banka kartı sayısını göstermektedir. Artan banka kart sayısı ile birlikte banka kartlarının kopyalanması ile oluşacak mağduriyetlerinde artacağı öngörülmektedir. TCKK' nın taklit ve tahrif edilememesi özelliği ile banka kartlarının kopyalanması sonucu oluşan mağduriyetlerin önüne geçilmekte, hizmet veren kurum hizmeti alan vatandaştan emin olmakta ayrıca, gereksiz yere banka kartı taşımanın önüne geçilmekte, banka aidat ücretleri gibi vatandaşların üzerine oluşan külfet kalkmakta ve bankalara olan bağımlılık azalmaktadır.

Kart Sayıları (Milyon Adet)	2015	2016	Değişim
Banka Kartı	110.4	115.4	%5
Kredi Kartı	57.8	59	%2

Şekil 3.1: BKM Verilerine Göre 2015-2016 Banka Kartı ve Kredi Kartı Sayısı

- TCKK, vatandaşa ait nüfus, fotoğraf ve parmak izi bilgilerini temaslı yonga üzerinde güvenli bir şekilde sakladığı için ödeme işlemlerinde kimlik doğrulama, biyometrik veriler ile de gerçekleştirilebilmektedir. ÖKC' ler mevcut durumda biyometrik veri alma ve o veri ile doğrulama yapabilecek donanımsal ve yazılımsal altyapıyı sunmaktadır.

- Kimlik kartının temaslı ara yüzü için tasarlanan yonga, tamamen özgün, ulusal kaynaklı ve uluslararası standartları destekleyecek özellikler taşımaktadır. Sahip olduğu Ortak Kriter EAL 5 + güvenlik seviyesi ve işlevsellik, performans, fiyat açılarından rekabet gücüyle,e-devlet, bankacılık gibi uygulamalar için güvenilir bir seçenek oluşturmaktadır. E-Kimlik Projesi kapsamında kazanılan akıllı kart çip tasarımı ve üretimi konusundaki bilgi birikimi ciddi bir yurtdışı bağımlılığını ortadan kaldırmaktadır.

- Kimlik kartındaki temaslı yonga, kart sahibine ait nitelikli elektronik sertifikanın (NES) yüklenebilmesine olanak sağlamaktadır. Kart sahibi, Bilgi Teknolojileri ve

İletişim Kurumu tarafından yetkilendirilmiş ve elektronik imza konusunda faaliyet gösteren herhangi bir özel Elektronik Sertifika Hizmet Sağlayıcı' dan (ESHS) kimlik kartına elektronik imza sertifikası yükletebilmektedir. Kişi, sahip olduğu bu kart üzerindeki elektronik imza fonksiyonu sayesinde elektronik ortamda gerçekleştirilen işlemlerde ıslak imzası gibi birebir olarak hukuksal bağlayıcılığı olan elektronik imzasını da atabilmektedir. Vatandaşların, başka bir akıllı kart olmaksızın, elektronik ortamlarda nitelikli elektronik imzasının atılmasına imkân sağladığı için büyük miktarda ödeme işlemlerinde ve para transferlerinde, başka bir onay koduna gerek kalmadan işlemi gerçekleştirerek, hizmeti veren kuruma ve hizmeti alan vatandaşa kolaylık sağlayabilmektedir. Ayrıca, Yeni Nesil Ödeme Kaydedici Cihazlar' da mevcut olan sanal pos işlemleri ile online olarak para transferi ve alışveriş yapılabilmektedir.

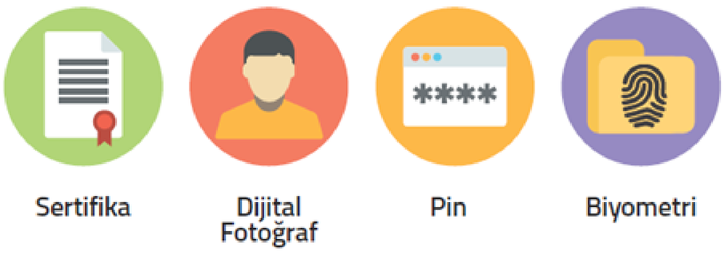
- Bankalararası Kart Merkezi (BKM) Şekil 3.2' de görülen 2016 yılı Haziran ayı kartlı ödeme verilerine göre; Haziran ayı sonunda Türkiye'de banka kartları ile yapılan alışveriş miktarı bir önceki yıla göre %32 artarak 4.07 milyar TL, nakit çekim ise bir önceki yıla göre %19 artarak 44.53 milyar TL olmuştur [23] [24]. Toplam tutar ise bir önceki yıla göre %20 artarak 48.60 milyar TL olmuştur. Bu veriler bize göstermektedir ki banka kartı kullanımı her geçen gün artarak devasa rakamlara ulaşmaktadır. Bu entegrasyon ile birlikte toplam da 115 milyon banka kartının yapmış olduğu ortalama 50 milyar TL tutar kişi bazında kayıt altına tutulabilecektir.

Banka Kartı Kullanım Tutarı (Milyar TL)	2015	2016	Değişim
Alışveriş	3.07	4.07	%32
Nakit Çekim	37.32	44.53	%19
Toplam	40.39	48.60	%20

Şekil 3.2: BKM Verilerine Göre 2015-2016 Banka Kartı ve Kredi Kartı Satış Kullanım Tutarları

- ÖKC ve TCKK' nın entegre çalışması kimlik doğrulama ile ödeme gerektiren (sağlık, finans, e-devlet, e-ticaret, sigorta vb.) gibi yerlerde vatandaşa kolaylık sağlamakta, bürokrasi azaltılmakta aynı zamanda kâğıt israfı da önlenmektedir.

- Kimlik kartı şifresi girilerek veya biyometrik veri (parmak, parmak damar veya el aya izi) okutularak hesaba erişilebildiği için PIN kodu hatırlanmadığı durumlar için kullanım kolaylığı sağlamaktadır.
- Elektronik kimlik kartları çoklu kimlik doğrulama faktörlerini desteklediği için ödeme işlemlerindeki güvenlik seviyesi kullanıcı tarafından belirlenebilmektedir.
- Bu entegrasyon sayesinde kurumların sunduğu online ödeme işlemlerinin nitelikleri ve sayıları artmaktadır ve ödeme gerektiren elektronik hizmetlerde internetin bulunduğu her yeden iş gücü harcamadan 7/24 erişilebilmektedir.
- Kurumlar tarafından sunulan farklı hizmetlerde, hizmetin niteliğine göre kimlik doğrulama faktörleri seçilebilmektedir.
- Elektronik Kimlik Kartları çoklu kimlik doğrulamayı desteklediği için ödeme tutarı bazında kimlik doğrulama yöntemi belirlenebilmektedir. Şekil 3.3' de Elektronik Kimlik Kartları' nın desteklediği kimlik doğrulama faktörleri görülmektedir.



Şekil 3.3: TCKK' nın Desteklediği Kimlik Doğrulama Faktörleri

- Bankalar vatandaşa yönelik hizmetlerde elektronik iş süreçleri destekleyen elektronik kimlik kartları ile entegre çalışarak bürokrasi azaltılmakta ve uzaktan ödeme ile (kurumun uç noktasına gitmeden ve başka bir ödeme sistemi veya uygulaması kullanmadan) aynı kart ile hem ödeme hem de kimlik doğrulama işini elektronik ortam da daha hızlı çözebilmektedir.
- Vatandaş, üzerinde hem kimlik doğrulama hem de ödeme işlemini yapan kartları taşımak yerine bu işlemlerin her ikisini de içeren akıllı kimlik kartı taşıyacaktır. Bulunmasını istediği banka hesaplarını birleştirerek tek kart, tek şifre ile işlem yapma kolaylığı sağlamaktadır.
- Banka hizmetlerinden yararlanan kişilerin hak sahipliği denetimi kolay ve güvenli bir şekilde yapılabilmektedir.

Bölüm 4

Ticarette Ödeme Kaydedici Cihazlar (ÖKC) ve Kullanımı

4.1 Gelir İdaresi Başkanlığı (GİB)

Yeni Nesil ÖKC' ler, çevre birimleri, ÖKC TSM Merkezi ve GİB Bilgi Sistemi arasındaki güvenli haberleşmeyi ve mesajlaşma yapısını tanımlayan, haberleşme protokollerini değiştiren, güncelleyen ve bununla ilgili tebliğler ve teknik kılavuzlar yayınlayan kurumdur. GİB ÖKC' ler ile mükelleflerin vergiye uyumunu kolaylaştırmakta, mükellefi vergi mevzuatından doğan hakları ve ödevleri konusunda bilgilendirmekte, mükellefin haklarını korumakta ve devlet ile mükellef arasında, her iki tarafın çıkarlarını gözetmektedir.

4.2 Trusted Service Manager(TSM): Güvenli Servis Sağlayıcı

Yeni Nesil ÖKC' lere yazılım yükleme, parametre yükleme, yazılım güncelleme, bu cihazları ve bu cihazlar ile birlikte veya üzerinde gerçekleştirilen kartlı işlemleri yönetme, cihazlar ile ilgili güvenli anahtar yönetimini gerçekleştirme, ön kontrol işlemlerini yapma, banka uygulaması yazılım ve parametrelerini cihaza yükleme, cihaz yaşam döngüsünü kontrol etme ve yönetme, ÖKC mesajlarının GİB Bilgi Sistemine ve üye işyeri anlaşması yapan kuruluşlara GMP' lerde belirlenen iletişim protokolleri çerçevesinde aktarılmasını sağlama amacıyla ÖKC üreticileri tarafından veya bir Dış Hizmet Sağlayıcısı tarafından kurulmuş terminal yönetim merkezini ifade eder. ÖKC TSM Merkezleri ÖKC Üreticileri için münhasıran kurulmuş donanım, yazılım ve işletimi içermeli ve sunulacak olan sertifikalar bu sistem için alınmış olmalıdır [15].

4.3 Yeni Nesil Ödeme Kaydedici Cihaz Teknik Özellikleri

Yeni nesil ödeme kaydedici cihazların; uzaktan yönetim, şifreleme, I/O, fiş düzenleme vb. işlemlerini aynı anda çoklu işlem yapabilme (multiprocess) özellikleri vardır. İşletim sistemi IPv4 ve IPv6 protokollerini ve NTP protokolünü desteklemektedir. Veri kaydetme, düzenleme, sorgulama ve raporlama özellikleri ile beraber yapılan satışlara ait ayrıntılı istatistiklerin çıkarılabilmesi için ana ürün grubu (gıda, giyim, tekel, elektronik vb.) ve alt ürün grubu (süt, sigara, meyve, pantolon) satış kayıtlarını tutabilmektedir. Uygulama programında yapılan ayarlarla, veritabanından istenilen sorgular yapılarak sonuçlar Gelir İdaresi Mesajlaşma Protokolü(GMP)'nün belirttiği mesaj formatlarında gönderebilmektedir. GİB Bilgi Sistemleri istenilen verileri Yeni Nesil ÖKC' lere, ÖKC Üreticisi Güvenli Servis Sağlayıcıları (TSM) aracılığı ile gönderebilmektedir[15].

ÖKC ile TSM arasında SSL güvenli haberleşme alt yapısı mevcuttur. TSM ile GİB arasında ise iletişim güvenli kiralık hatlar üzerinden yapılmaktadır. TSM ile GİB-Bilgi Sistemi arasında yer alan kiralık hatlardaki şifreleme ve imzalama alt yapısında asgari 128 bitlik AES şifreleme/çözme, 2048 bit DSA ya da RSA imzalama/doğrulama ve SHA256 özetleme muadili bir yapı bulunmaktadır[16].

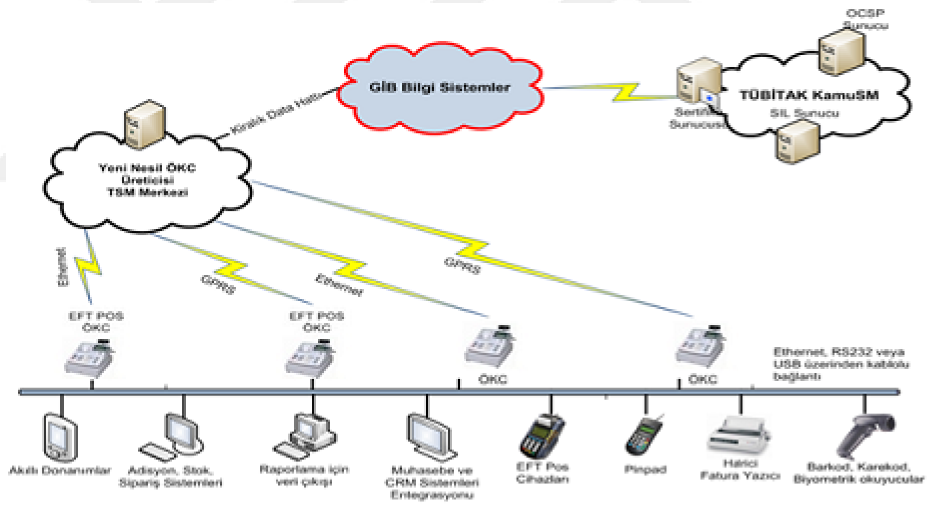
Yeni Nesil ÖKC' lere ilk kurulum sırasında ITU X.509 v3 formatı ile uyumlu sayısal sertifika yüklenmektedir. Bu sertifika temel olarak kimlik doğrulama, Yeni Nesil ÖKC' nin onaylanmış saha kullanım süresi ve GİB ile güvenli haberleşme için kullanılmaktadır [28]. Bu sertifika açık anahtar altyapısı sisteminin bir parçasıdır. Mali sertifika (Yeni Nesil ÖKC SSL Sertifikası) ve ilgili özel anahtarı cihaz içerisindeki elektronik ve fiziksel olarak korunmuş (mesh cover ile kaplı) güvenli alanda (TPM, Secure IC/Element) veya akıllı kart içerisinde saklanmaktadır. Bu sertifika, GİB tarafından yetkilendirilmiş ESHS tarafından cihaza özel üretilmektedir. Sertifika, ESHS tarafından ÖKC üretici merkezine elektronik ortamda şifreli olarak veya akıllı kart içerisinde verilmekte ve üretim esnasında ÖKC üreticisi tarafından cihaza yüklenmektedir[15].

Sistemde kullanılan anahtarların üretimleri ÖKC, TSM, GİB ve Kamu SM tarafından yapılmaktadır. TSM' ler bu anahtar ve sertifikaları sahip oldukları HSM (Hardware Security Module)' ler üzerinde ÖKC' ler ise cihazın elektronik mühür ile korunmuş güvenli alanındaki Secure IC üzerinde üretmekte ve saklamaktadır. ÖKC tarafından üretilen TRMK anahtarı GIB ve TSM ile güvenli haberleşebilmek için kullanılmaktadır. ÖKC eğer EFT-POS özelliğine sahip bir cihaz ise bu cihaz PCI-PTS (PIN Transaction Security) onayını almış olmalıdır. Bu sayede cihazın ürettiği rastgele sayıların NIST standartlarına uygunluğu belgelenmiş olmaktadır. EFT-POS özelliği bulunmayan ÖKC' ler tarafından üretilen rastgele sayılar, PCI-PTS standardı ile uyumlu olarak TÜBİTAK OKTEM Laboratuvarı tarafından kontrol edilmektedir.[16]

GİB ve TSM üzerinde üretilen anahtarlar ise HSM kullanılarak üretilmektedir. GİB HSM' de; TREK, TRAK ve LMK simetrik anahtarları üretilir. Tüm simetrik şifreleme işlemleri için AES-256 algoritması CBC çalışma modunda kullanılmaktadır. HSM' ler güvenlik testlerinden geçmiş ve FIPS 140-2 güvenlik onaylı donanımlardır [30]. HSM üzerinde üretilen bu anahtarlar için belirtilen üretilme şekli FIPS 140-2 (asgari level-2) uyumlu olmalıdır. HSM' ler ve anahtar üretme yöntemleri güvenlik için gerekli standartları sağlayacaklardır. Kamu SM ya da GİB tarafından yetkilendirilmiş başka bir sertifika otoritesi üzerinden GIB Bilgi Sistemi için, her bir TSM için ve her bir ÖKC için asimetrik kriptografi anahtar çiftleri (açık anahtar ve özel anahtar) üretilecek, yenilenecek ve SİL kontrolleri yapılacaktır. GIB Bilgi Sistemi için imzalama/doğrulama (SGIB-SIGN/PGIB-SIGN) ve şifreleme/çözme (SGIB/PGIB) amaçlı kullanılmak üzere 2-çift anahtar gerekmektedir. Aynı şekilde ÖKC' ler için imzalama/doğrulama amaçlı tek anahtar çifti bulunmaktadır. Anahtarları üreten sertifika otoritesi her public key için sertifika vererek anahtar yönetimini yapmaktadır. Aynı zamanda, düzenli periyotlarda Sertifika İptal Listesi (SİL) yayınlanmaktadır. Bu periyotlar da yayınlanacak SİL listesi GİB ve TSM üzerinde oluşturulacak zamanlanmış bir görev ile otomatik olarak indirilmektedir. Bu indirme işlemlerinden sonra; GİB 'in bilgisi haricinde iptal edilmiş geçersiz anahtarlar ile yapılan işlemler tespit edilebilmektedir. Normal şartlarda cihazlar kalıcı olarak kullanımdan kaldırılacak ise sertifikaları GİB iptal ettirmektedir. Geçici kapatma durumları GİB Bilgi Sistemi tarafından yönetilecek olup sertifika iptaline ihtiyaç duyulmamaktadır [16].

4.4 Ödeme Kaydedici Cihaz Haberleşme Topolojisi

Yeni nesil ÖKC' ler ile GİB arasında Şekil 4.1' de görüldüğü gibi online bir veri akışı olmaktadır. Yeni nesil ÖKC' ler düzenli olarak GİB' e bilgi aktarmaktadır ve Gelir İdaresi Başkanlığı istediği zaman bir ÖKC' den veri alabilmektedir. İletilen bu veriler GİB' in isteğine bağlı olarak şifreli veya şifresiz olarak iletilmektedir. Yeni nesil ÖKC' ye yapılacak tüm müdahaleler (yetkili, yetkisiz) kayıt altına alınmakta ve GİB' e iletilmektedir. GİB Bilgi Sistemleri, Yeni Nesil ÖKC ve ÖKC Üretici TSM merkezleri arasındaki Şekil 4.1' de görülen haberleşmede GMP protokolüne uygun olarak yapılmaktadır. Yeni Nesil ÖKC' lardan GİB Bilgi Sistemleri' ne gönderilecek veriler, ilgili ÖKC üreticisinin TSM merkezi üzerinden yönlendirilerek GİB' e iletilmektedir. Yeni Nesil ÖKC' den GİB Bilgi Sistemlerine iletilen verilerde uçtan uca güvenlik sağlanmaktadır, GİB Bilgi Sistemleri dışında herhangi bir yerde veri depolama, farklı yere veri yönlendirme işlemi yapılmamaktadır [16].



Şekil 4.1: GİB, TSM ve ÖKC Haberleşme Topolojisi

TSM ile GİB arasında iki yönlü bir haberleşme bulunmaktadır. GİB Bilgi Sistemlerinde bulunan sunucu devamlı olarak dinleme durumunda olmakta ve TSM GİB sunucusu tarafından sağlanacak olan IP ve Port üzerinden sisteme bağlı kalmaktadır. Bu bağlantı üzerinden; GİB tarafından gönderilecek olan parametre veya kur belirleme mesajı ile TSM' ye ulaşabilmekte ve TSM tarafından bu bilgilerin Yeni Nesil ÖKC' lere indirilmesi istenebilmektedir. ÖKC ile TSM arasında SSL güvenli haberleşme alt yapısı mevcuttur. TSM ile GİB arasında ise iletişim güvenli kiralık hatlar üzerinden yapılmaktadır.

GİB tarafından belirlenen gizlilik ve bütünlüğü korunarak iletilmesi gereken veriler şifreli olarak iletilecektir. Diğer veriler açık olarak iletilebilecektir [16].

Yeni Nesil ÖKC GMP Mesajı Ağ (network) iletim Seviyesi, ÖKC TSM Merkezinde sonlandırılacak olup, GMP Mesajı üzerinde gerekli kontroller yapıldıktan sonra GİB Bilgi Sistemleri' ne iletilebilmektedir. Yeni Nesil ÖKC' lere parametre ve ihtiyaç duyulan diğer işlemler, algoritma ve protokollerle güvenli kanallar üzerinden yüklenmektedir. Ayrıca Yeni Nesil ÖKC' lere network üzerinden yazılım yükleme işlemi güvenli kanallar aracılığı ile yapılmaktadır [15].

Yeni Nesil ÖKC' ler üzerinde çalışan tüm uygulamalar ÖKC TSM üzerinden Yeni Nesil ÖKC' lere bağlanacaktır. Üye işyeri Anlaşması Yapan Kuruluşun yetkilendireceği kişi veya kurumlar EFT-POS özelliği olan Yeni Nesil ÖKC' lere, bankacılık uygulamaları ve bunlara ilişkin parametre, anahtar yazılım yükleme ve ihtiyaç duyulan diğer işlemleri yerine getirmek için taleplerini ÖKC TSM Merkezlerine bildireceklerdir. Bu işlemler ÖKC TSM Merkezleri aracılığıyla gerçekleştirilecektir. Yeni Nesil ÖKC' lerde oluşabilecek sorunlardan (sahada yaşanacak cihaz ya da tüm uygulamalardaki manipülasyonlar, alınan ödeme ile kesilen mali fiş mutabakatsızlıkları, fonksiyonel arızalar, usulsüz banka/sadakat uygulama anahtar yüklemeleri, saha operasyonel sıkıntılar vb.) ÖKC üreticileri sorumludur [15].

Bölüm 5

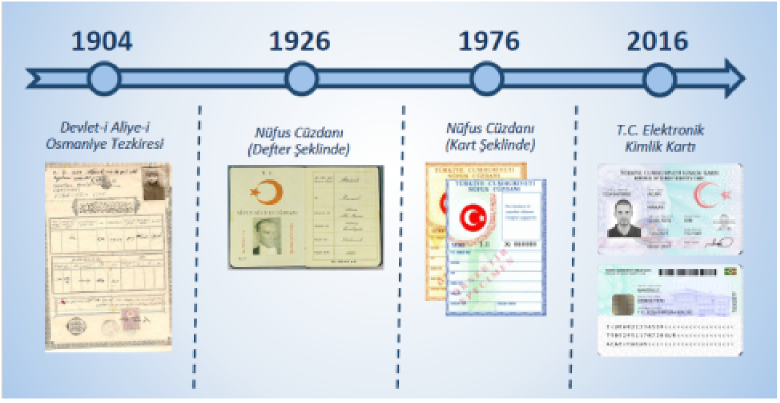
Türkiye Cumhuriyeti Kimlik Kartları (TCKK) ve Elektronik Kimlik Doğrulama Sistemi (EKDS)

5.1 Elektronik kimlik Kartı

5.1.1 Kimlik Tarihçesi

Osmanlı devletinde nüfus hizmetlerini yürütmek üzere ilk olarak Ekim 1884 yılında "Nüfusu Umumiye Müdüriyeti" kurulmuştur. Genel Müdürlüğe 1889 yılında "Sicilli Nüfus Ahali İdare-i Umumiyesi" adı verilmiş ve asıl hizmetin yanında Pasaport Kalemi, Murur Kalemi, Vilayet Kalemi, Dersaadet Kalemi gibi alt kademelere ayrılarak yapılanmıştır. Bu yapı gereğince Osmanlı halkının ilk nüfus tezkeresi 1889 yılında kurulan Sicilli Nüfus Ahali İdare-i Umumiyesi tarafından dağıtılmaya başlanmıştır. Ancak bu nüfus teskerelerinin herhangi bir nüfus kaydına dayanmaması ve tezkereyi taşıyan kişinin nüfus kütüğüne kayıtlı olmaması nedeniyle özel ve resmi işlemlerde pek yararlı olamamıştır. Zamanla nüfus tezkireleri yerini defterlere bırakmıştır. Defterler Cumhuriyet döneminde de kullanılmıştır ve kayıtlar harf inkılâbına kadar Osmanlıca tutulmuştur. 1928'den itibaren, donemin imkânları ölçüsünde, cüzdanlarda yer yer fotoğraf da konulmuştur. 01 Kasım 1928 tarihinde harf inkılâbı ile kayıtlar yeni harflerle tutulmaya başlanmıştır. Cumhuriyet dönemi defterlerin ön kapağında Türkiye "Cumhuriyet" alt kısımda "Hüviyet

Cüzdanı“ ibaresi yer almıştır. Farklı tip uygulamalar ve sistemler denenerek 01.06.1976 tarihinden itibaren çok yapraklı cüzdanlar kalkmış ve kart şeklindeki haliyle kullanılmaya başlamıştır. Şekil 5.1' de nüfus belgelerinin zamanla değişimi görülmektedir [1].



Şekil 5.1: Kimlik Tarihçesi

Ülkemizde mevcut durumda, her vatandaş için nüfus cüzdanında tekil T.C. Kimlik Numarası vardır. Bu uygulama, kamu/özel kurumlarda oluşabilecek zafiyetleri de beraberinde getirmektedir. Örneğin vatandaşın T.C. Kimlik Numarasına ulaşan biri, onun birçok mahrem bilgisine hakkı olamadığı halde erişmektedir. Gelişen teknoloji günümüzde kimlik kartının nüfus cüzdanından farklı, diğer bir deyişle “akıllı olmasını zorunlu hale getirmiştir [1].

28 Temmuz 2006 tarih ve 26242 sayılı Resmi Gazete'de yayımlanan Yüksek Planlama Kurulu'nun 11.07.2006 tarih ve 2006/38 karar no' lu kararı ile Bilgi Toplumu Stratejisi Eylem Planı kabul edilmiştir. Planın 46 no' lu eyleminde “Vatandaşlık Kartı; Pilot Uygulaması ve Yaygınlaştırılması ile biyometrik unsurlar da içeren elektronik vatandaşlık kartının kimlik doğrulama için kullanımının sağlanması ve tüm kimlik doğrulama fonksiyonlarının tek bir elektronik kartta toplanması” öngörülmüştür [1].

Vatandaşlık Kartı projesinin pilot uygulamasının yürütüldüğü, TUBİTAK destekli “Akıllı Kart Tabanlı Güvenli Sosyal Güvenlik Sistemi Geliştirimi” adlı projeye Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (NVİ), Sağlık Bakanlığı (SB) ve Sosyal Güvenlik Kurumu'nun (SGK) taraf olarak katılımı sağlanmıştır. Böylece kartın dağıtımı, sosyal güvenlik ve sağlık hizmetlerinde kullanımına yönelik süreçlerin de test edilmesi sağlanmıştır. Yeni kimlik kartının, pilot uygulama için, şeklini ve kapsamını belirlemek amacıyla İçişleri Bakanlığı, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, TUBİTAK UEKAE ve Plas kart ile birlikte çalışmalar yapılmış, son hali Bolu uygulamasında kullanılmıştır.

Bu çerçevede AB ve üye ülkeler başta olmak üzere, diğer ülkelerin kimlik kartlarına ilişkin çalışma ve uygulamalar da (İtalya, Belçika, İsveç, Estonya, Finlandiya, Avusturya, İspanya, Portekiz, Birleşik Krallık, Almanya, Fransa, Hollanda, Danimarka, İrlanda, ABD, Japonya, Avustralya, Kanada ve Pakistan) incelenerek onlardan yararlanılmıştır. Yapılan araştırmada, Avrupa Birliği (AB) düzeyinde ortak karara varılmış kimlik kartı standartları (ISO 7816, 14443) kullanılmıştır [1].

5.1.2 Elektronik Kimlik Kart İçindeki Bilgiler

- *Kimlik Bilgileri*: T.C. Kimlik Numarası, Adı, Soyadı, Anne Adı, Baba Adı, Doğum Yeri ve Tarihi, Cinsiyeti, Medeni Hali, Önceki Soyadı, Kart Seri Numarası ve Geçerlilik Tarihi, Dini. Şekil 5.2' de Türkiye Cumhuriyeti Kimlik Kartı ön cephe, Şekil 5.3' de Türkiye Cumhuriyeti Kimlik Kartı Arka Cephe görülmektedir.

ŞEKIL 5.2: Türkiye Cumhuriyeti Kimlik Kartı Ön Cephe

- *Kişiye Ait Diğer Bilgiler*: Sayısal Yüz Resmi (ISO 19794-5), Parmak İzi Verisi (ISO 19794-2),Parmak Damar Verisi (Morpho Template),El Ayası Damar İzi (Fujitsu Template)

- *Acil Sağlık Bilgisi Uygulaması (Boş Alan)*: Sağlık bilgisi 1 (Kan Grubu), Sağlık bilgisi 2, Sağlık bilgisi 3, Sağlık bilgisi 4

- *Kart Durum Bilgisi*: Kişisel Mesaj, Rüşt Mesajı [1].

Şekil 5.3: Türkiye Cumhuriyeti Kimlik Kartı Arka Cephe

5.1.3 Elektronik Kimlik Kartı e-Hizmetlerdeki Rolü

Günümüzde bilişim teknolojilerindeki gelişmeler, birçok alanda olduğu gibi kamu uygulamalarında da yeni bir anlayışı ortaya çıkarmıştır. Elektronik devlet (e-devlet) diye adlandırılan bu oluşum kapsamında, kamunun elindeki bilgiler elektronik ortamda, çevrimiçi olarak vatandaş ve kurumlarla paylaşılmaktadır. Bu yaklaşım, bir taraftan kurumların hizmet sunumunda ihtiyaç duyduğu bilgileri diğer kurumlardan anında alabilmesini, diğer yandan da vatandaşın kamu kurumlarındaki işlerini elektronik ortamda yapabilmesini sağlamaktadır. Elektronik Kimlik Kartı Şekil 5.4' de görüldüğü gibi e-bankacılık, e-devlet, e-ticaret, e-imza, e-hizmet gibi birçok alanda hizmet alımını kolaylaştıracaktır. Ayrıca vatandaşı hizmetin odağına koyarak, vatandaş ağırlıklı bir sistemin giriş kapısı olmaktadır. Vergi toplanmasından sahteciliğin önlenmesine, kimlik taşıma kolaylığından, devlete başvuruların hızlanmasına kadar birçok amaca hizmet edecek olan bu projenin, yaygınlaştırılması ile birlikte e-devlet sureci kolaylaşacaktır [1].

5.1.4 Elektronik Kimlik Kartı Özellikleri

Türkiye'de e-devlet anlayışının yerleşmesinde temel rol oynayacak olan Elektronik Kimlik Doğrulama Sistemi (EKDS) projesi kapsamında vatandaşlara dağıtılmakta olan, Şekil 5.5'de görsel özellikleri detaylı olarak görülen kimlik kartları, aşağıdaki fiziksel ve işlevsel güvenlik özelliklerine sahiptir.

Şekil 5.4: Türkiye Cumhuriyeti Kimlik Kartı e-Hizmetlerdeki Rolü

- Vatandaşın rahatlıkla taşımasına olanak sağlayan standart bir akıllı kart (kredi kartı) boyutundadır.
- 10 yıllık dayanıklılık ömrüne sahip polikarbon malzemeden üretilmiş kart gövdesine sahiptir.
- Taklit edilemeyen görsel ve elektronik güvenlik özelliklerine sahiptir.
- Temaslı ve temassız ara yüz özelliklerine sahip fiziksel olarak ayrı iki yongaya sahiptir.
- Ortak kriter EAL 5+ güvenlik seviyesinde temaslı ve temassız yongaya, Ortak kriter EAL 4+ güvenlik seviyesinde milli akıllı kart işletim sistemine sahiptir.
- Cinsiyet ayrımı olmaksızın tek tip kart tasarımına sahip olacaktır.
- Ön ve arka yüzünde yer alan kısımlar ve bu kısımların içerisindeki bilgiler uluslararası standartlara (ICAO 9303) uyumludur.
- Mevcut nüfus cüzdanın yerine kullanılmak üzere tasarlanan kimlik kartı farklı uygulamalara(kimlik, e-imza ve seyahat belgesi) sahiptir.
- Kimlik kartı ID-1 ve ISO 7810 standartlarına uygundur.
- Kimlik kartının gövdesi aşınmaya ve kırılmaya dayanıklı malzemedendir.
- Kimlik kartı, üzerinde sahteciliği önlemek üzere güvenlik öğeleri içermektedir.
- Kimlik kartı, üzerinde taşıdığı görsel elemanlar ve kişisel bilgiler bakımından tamamen alenidir (acık, seçik ve net).

- Karttaki yonga içindeki bilgilere sadece yetkili kimseler erişilebilir.
- Kimlik kartında, üzerine güvenlik, bilgi saklama, her turlu sahteciliği önleme ve e-devlet anlayışı kapsamında elektronik sertifikalar gibi uygulamaları da içerebilecek kapasitede bir yonga vardır.
- Kimlik kartının her iki yüzeyine de bilgi yazılabilir.
- Kimlik kartı taklit, tahrifat ve sahteciliğe imkan vermeyecek niteliktedir.
- Kimlik kartının üzerine işlenen görsel öğeler, karta zarar vermeden hiç bir şekilde değiştirilememektedir.
- Kimlik kartının kişiselleştirilmesi için gerekli olan tüm grafik elemanları kolaylıkla programlanabilir. (Görüntüler, imzalar, kodlar, alfa nümerik veriler vs.)
- Kimlik kartının üzerinde vatandaşa ait siyah-beyaz bir fotoğraf bulunmaktadır.
- Kimlik kartında fotoğraf, lazer baskı tekniğiyle basılır.
- Kartın üzerine T.C. kimlik no' su barkod olarak da yazılabilir.
- Kartın on ve arka yüzüne vatandaşa ait bilgiler silinmez, bozulmaz, karta zarar vermeden değiştirilemez şekilde yazılarak kişiselleştirilir.
- Bilgiler yonga içine de güvenli bir şekilde yazılmaktadır.
- Kadın ve erkek tek tip kart kullanılıp kart üzerine cinsiyet alanı bulunmamaktadır
- Kimlik Kartı Ara yüzleri Kontaklı Yonga, Barkod (T.C. Kimlik Numarası), MRZ ve Kontaksız yongadan oluşmaktadır.
- Kimlik kartı için kullanılan yonga çeşitleri CC EAL5+1 onaylı NXP, INFINION ve TUBİTAK-UEKAE tasarımı olarak belirlenmiştir.
- Kimlik kartı için yonga işletim sistemi EAL4+ sertifikasına sahip TUBİTAK UEKAE ürünüdür (AKİS 2.2.8, UKİS 2.2.9).
- Kimlik kartı üzerindeki çeşitli görsel güvenlik öğeleri görsel doğrulamada yardımcı araçlar olarak kullanılır. 3 seviyede doğrulama yapılabilir:
- Kart on yıl kullanıma olanak sağlayan Polikarbon (PC) malzemeden üretilmiş olacaktır [1].

Şekil 5.5: Türkiye Cumhuriyeti Kimlik Kartı Fiziksel Özellikleri

Kimlik kartının diğer bilgi saklama ortamı ise kartla bütünleşik olarak üretilen ve içinde kart sahibine ait nüfus bilgilerinin tutulduğu temaslı yongasının olmasıdır. Bunun yanı sıra içinde tuttuğu özel kriptografik anahtarları ve bu anahtarlarla ilişkili olan sayısal sertifikaları sayesinde ataklara karşı dirençli bir belleği de içermektedir. Kimlik kartındaki veri alanları içindeki bilgiye erişim açısından 3 kısımdan oluşmaktadır.

- Acık veya Rol Tabanlı Erişim (Fotoğraf, Kimlik Doğrulama Sertifikası)
- PIN ile erişim (Elektronik İmza, Kimlik bilgileri)
- PIN ve simetrik asıllama ile erişim: Koruma faktörü en yüksek alandır ve içinde parmak ve damar izini içeren biometrik veri bulunur. Bu alana erişebilmek için özel geliştirilen Kimlik Erişim Cihazı ve Kimlik Erişim Cihazı' nın simetrik anahtarının bulunduğu GEM (Güvenli Erişim Modülü) kartı gerekir. Kimlik kartı yongasındaki veri alanları, kullanım sırasında oluşabilecek güvenlik açıkları analiz edilerek tasarlanmıştır [13].

5.1.5 Elektronik Kimlik Kartının Açık Anahtar Altyapısı (PKI):

E-Kimlik ve e-devlet uygulamalarında ana unsur bilgiye güvenli erişimdir. İnternet üzerinde hizmet veren kurumların uygulamalarında, hizmet gerçekleştirilirken hizmete katılan görevli ve hizmetten yararlanmak isteyen vatandaşın kimliğinin belirlenmesi, yasalar önünde delil niteliği taşımaktadır. Bu nedenle e-kimlik altyapısında sertifika sistemi oluşturulmuştur. EKDS projesinde milli olarak geliştirilen Açık Anahtar Altyapısı

(PKI2, 'Public Key Infrastructure) kullanılmıştır. Bu yapıda sertifika tanzim eden ve sertifika dağıtımı konusunda yetkili kurumlar ile kullanıcıların/kişilerin bulunduğu güvene dayalı bir düzen mevcuttur [1].

Sertifika, bir varlığa ait kimlik bilgisi ile bu varlığın kullanımı için atanan açık anahtar bilgisini bir arada tutan belgedir. Açık Anahtar Altyapısı, veri iletişiminde açık anahtarlı kriptografinin yaygın ve güvenli olarak kullanılabilmesini sağlayan ve birbirleriyle eşgüdüm içinde çalışan anahtar üretimi, anahtar yönetimi, onay kurumu, sayısal noterlik, zaman damgası gibi hizmetlerin tümünü kapsamaktadır[25]. Açık Anahtar Altyapısı modellerine göre;

- Simetrik (Tek Anahtarlı): Bu şifreleme sistemlerinde, veriyi şifrelemek için ve şifrelenmiş veriyi okuyabilmek için aynı anahtar kullanılır. Karşılıklı olarak şifreli haberleşebilmek için her iki taraf simetrik anahtarları başka birinin eline geçmeden birbirleriyle paylaşmak zorundadırlar [25].

- Açık anahtarlı şifreleme (Çift Anahtarlı), şifre ve deşifre işlemleri için farklı anahtarların kullanıldığı bir şifreleme sistemidir. Haberleşen taraflardan her birinde birer çift anahtar bulunur. Bu anahtar çiftlerini oluşturan anahtarlardan biri gizli anahtar diğeri açık (gizli olmayan) anahtardır. Bu anahtarlardan bir tanesiyle şifreleme yapılırken diğeriyle de şifre çözme işlemi gerçekleştirilir. Bu iki anahtar çifti matematiksel olarak birbirleriyle bağlantılıdır.Gizli anahtarın sadece bir sahibi vardır. Gizli anahtara sahip olan taraf gizli anahtar aracılığıyla, kendi açık anahtarıyla şifrelenmiş bilgilerin şifresini çözebilir, kendisine ait sayısal imzaları oluşturabilir ya da kendi kimliğini ispat edebilir. Açık anahtar herkesin erişimine açıktır. Anahtarlar birbirlerinden farklı olsalar da, matematiksel olarak birbirleriyle ilişkilidirler. Açık anahtarla, bilgiler sadece gizli anahtarın sahibi tarafından çözülebilecek şekilde şifrelenebilir ya da gizli anahtar sahibinin dijital imzasının ve dolayısıyla kimliğinin doğruluğu kontrol edilebilir [32].

Açık Anahtar Altyapısı; gizlilik, bütünlük ve kimlik kontrolü fonksiyonlarını kullanıcıların elektronik sertifika kullanması yolu ile sağlamaktadır. Sertifika elektronik bir kimlik olduğu gibi aynı zamanda sahibine ait bilgiler ile gerekli algoritma anahtarlarını da üzerinde bulundurmaktadır .Şekil 5.6' da Türkiye Cumhuriyeti Kimlik Kartı Açık Anahtar

Şekil 5.6: Türkiye Cumhuriyeti Kimlik Kartı Açık Anahtar ve Gizli Anahtar Örneği

ve Gizli Anahtar Örneği görülmektedir. Sertifikalar kişiye özeldirler.Sertifikalar, akıllı kimlik kartları ile güvenli bir şekilde güvenli ortamlarda muhafaza edilmektedir [1].

Açık Anahtar Sertifikalarının Ortak Özellikleri;

- Sayısaldır (X.509 standardı)
- Sahibi hakkında gerekli bilgileri içerir
- Yayın ve son kullanma tarihini içerir.
- Yayıncısının adını içerir ve onun sayısal imzasıyla doğrulanması yapılır.
- Yayıncı adı ve sertifika seri numarası sertifikanın tekil olmasını sağlar [1].

5.2 Elektronik Kimlik Doğrulama Sistemi (EKDS)

Kimlik Doğrulama; bir kişinin kimliğinin geçerliğinin kanıtlanmasıdır. Elektronik Kimlik Doğrulama; bir cihaz veya yazılımın bir kişiyi veya bir cihazı elektronik olarak doğrulamasıdır. Elektronik Kimlik Doğrulama Sistemi ise; hizmet gerçekleştirilirken hizmete katılan kişilerin ve hizmetten yararlanmak isteyen kişilerin gerçekten öne sürdüğü kişi olduğunu ve kimliği çalan ya da taklit eden başka biri olmadığının doğrulanmasını gerçekleştiren sistemdir. EKDS' de Sertifika (Açık Anahtar Altyapısı), PIN ve Biyometrik veriler (Parmak izi, avuç izi ve parmak damar izi) ile elektronik kimlik doğrulama yapılmaktadır. EKDS, TUBİTAK UEKAE' nin geliştiricisi olduğu e-kimlik süreçleri ve buna uygun bileşenlerin tasarlandığı bir projedir. Elektronik Kimlik Doğrulama Sistemi elektronik ortamda verilen hizmetlerde;

- Kimlik kartının yetkili kurum tarafından verildiğini,
- Vatandaşın kartın sahibi olduğunu ve kimlik doğrulama sırasında hizmet verilen yerde olduğunu,
- Kimlik doğrulama işleminin nerede, ne zaman, kim tarafından ve niçin gerçekleştirildiğini garanti eder [13].

5.2.1 Elektronik Kimlik Doğrulama Sistemi Bileşenleri

EKDS; TCKK, Kart Okuyucu, Kimlik Doğrulama Sunucusu, Kimlik Doğrulama Politika Sunucusu ve Arabirim Yazılımlar' dan oluşmaktadır.

- *Kimlik Doğrulama Sunucusu: (KDS)*: Kimlik doğrulama sonuçlarını Kurum Hizmet Sunucuları için değerlendiren ve doğrulayan merkezi sunucudur. EKDS' de kimlik doğrulama sonucunda üretilen bildirime Kimlik Doğrulama Bildirimi denir. Hizmet alınan kurum adına Kimlik Doğrulama Bildirimi'ni (KDB) doğrulayarak imzalı doğrulama sonucunu (başarılı/ başarısız) Kimlik Doğrulama Başarım Onayı (KDBO) olarak dönmektedir. Kimlik doğrulama bildiriminin onaylanmasından sonra elektronik kimlik doğrulama başarı ile tamamlanmış olur. Doğrulama yaptığı KDB' leri saklayıp sonradan sorgulama yapılmasına, arşivlenmesi istendiği durumlarda arşiv imza ile arşivlenmesine imkân sağlamaktadır. İmzalamada kullanılmak üzere HSM donanımına ihtiyacı vardır. Şekil 5.7' de Temsili Kimlik Doğrulama Sunucuları görülmektedir. KDS elektronik kimlik doğrulama sisteminde zorunlu tutulmaktadır [13].

Şekil 5.7: Kimlik Doğrulama Sunucusu Temsili

- *Kimlik Doğrulama Politika Sunucusu:(KDPS)*: Kimlik doğrulama sırasında kart okuyucu tarafından kullanılacak kimlik doğrulama yöntemi, güvenlik seviyesi, kimlik doğrulama süresi kimlik doğrulama geçerlilik süreleri gibi parametrelerden oluşan imzalı Kimlik Doğrulama Politikası'nı (KDP) belirleyen sunucudur. Kurumların uygulama veya vatandaş bazlı Kimlik Doğrulama Politikası' nı belirlemesine imkân sağlar. İmzalamada kullanmak üzere HSM donanımına ihtiyacı vardır. KPDS, Elektronik Kimlik Doğrulama Sistemi'nde opsiyonel ve kuruma özeldir [13].

- *Online Certificate Status Protocol (OCSP):Çevrimiçi Sertifika Durum Protokolü)*: Sertifika iptallerini SİL(Sertifika İptal Listesi) yayın periyoduna bağlı kalmaksızın öğrenebilmek için Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP) kullanılmaktadır. Çalışma şekli kullanıcının X Seri no' lu sertifikanın durumu nedir sorusuna aşağıdaki gibi bir yanıt alınmaktadır [13].

  – İyi iptal edilmemiş

  – Kötü iptal edilmiş; İptal nedeni, iptal zamanı

  – Bilinmiyor

  Her SM 'ye ait bir veya birden fazla OCSP sunucusu olabilir. OCSP sunucusu bağlı olduğu SM' nin yayınladığı sertifikaların iptal edilip edilmediği bilgisine ulaşır ve kendisine gelen kullanıcı isteklerini cevaplar. OCSP cevap mesajlarını elektronik imza ile imzalayarak güvenliği sağlamaktadır [13].

- *Rol Doğrulama Sunucusu (RS)*: Rol doğrulama protokollerini kullanarak rol doğrulama yapan ve TCKK üzerinde ki rol doğrulama ile erişilebilen nüfus verilerine erişebilen sunucudur. Standart Kart Okuyucu veya Kimlik Erişim Cihazı (KEC) üzerinden rol doğrulama yapar. Güvenli İletişimde ve Rol Doğrulamada kullanmak üzere HSM donanımına ihtiyacı vardır. RS Elektronik Kimlik Doğrulama Sistemi' nde opsiyonel ve kuruma özeldir [13].

- *Kart Erişim Cihazı (KEC)*:EKDS, doğrudan merkezi kimlik doğrulama yapmaz. Uç birimde yer alan, güvenilir aracı olarak Kart Erişim Cihazını (KEC) kullanır. KEC' ler sistemin bir parçasıdır ve doğrulamanın hizmetin sağlandığı yerlerde yapılmasını sağlar. KEC kimlik doğrulamayı gerçekleştirir ve sonucu güvenli, yanıltılamaz bir şekilde elektronik olarak Kimlik Doğrulama Sunucusu' na bildirir [13].

- *Arabirim Uygumaları*: EKDS sistemindeki bileşenler arası iletişimi sağlayan yazılımlardır. EKDS ile kurumların kullandıkları elektronik uygulamalara entegrasyonu, Arabirim Uygulamaları aracılığıyla gerçekleştirilmektedir. Arabirim Uygulamaları, masaüstü uygulaması veya sunucu üzerinde çalışan bir uygulama olabilir [13].
- *APDU*: Uygulama katmanında, kart ve kart okuyucu arasındaki tüm iletişim, uygulama protokolü veri birimleri (APDU, Application Protocol Data Unit) adı verilen yapılarla gerçekleşmektedir. Uygulamalar bunlarla, protokollerden bağımsız olarak kartla iletişim kurabilir [17].

5.2.2 Elektronik Kimlik Doğrulama Sistemi Genel İşleyişi

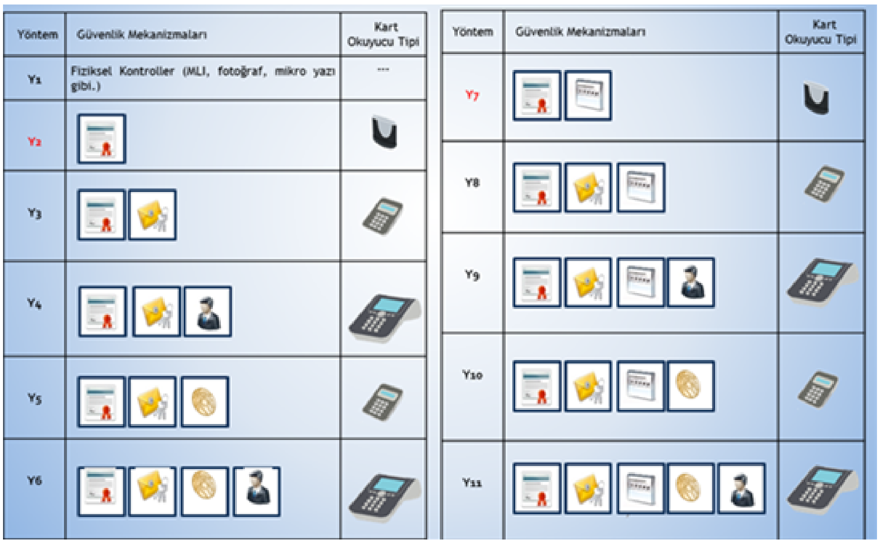
Kimlik doğrulama kullanım vakaları 3 ana başlık altında toplanabilir. Bu başlıklar;

1. Kimlik kartının doğrulanması:
    - Kimlik doğrulama talebi,
    - KDS' nın ve tüm sertifika zincirinin kontrol edilmesi,
    - KDB' nin doğrulanması ve KDB onayının üretilmesi [13].
2. Kimlik tanıma ve doğrulama Bu işlemde,
    - TCKK' nın NVİ tarafından verilmiş geçerli bir TCKK olup olmadığının yanında vatandaşın kimliği de tanımlanmaktadır.
    - Standart kart okuyucu ile çevrimiçi kimlik tanıma, standart kart okuyucu ile çevrimiçi kimlik doğrulama, KEC ile çevrimiçi kimlik doğrulama, hizmet isteyenin aracısının kimliğini KEC ile çevrimiçi doğrulama, KEC ile hizmete katılan şartlı ve çevrimiçi olarak kimlik doğrulama senaryoları ile yapılmaktadır.
    - Biyometrik verinin, PIN, dijital fotoğrafın nasıl doğrulandığı anlatılmaktadır [13].
3. Nüfus verisine erişme
    - NVİ tarafından verilmiş geçerli bir TCKK içindeki bir dosyaya erişimin nasıl yapılacağı ve yapılırken gerekli yetkilere sahip olunup olunmadığı sınanmaktadır.

- Standart kart okuyucu ile TCKK veri alanlarına rol tabanlı erişim, KEC ile TCKK içindeki veri alanlarına rol tabanlı erişim olmak üzere iki şekildedir.
- TCKK' nın rol tabanlı olma özelliğinden faydalanılmaktadır. NVİ tarafından yetkilendirilmiş kurumlar rol sertifikalarını TCKK' ya doğrulatarak, NVİ' nin izin verdiği dosyalara erişebilirler [13].

5.2.3 Elektronik Kimlik Doğrulama Sistemi'nde Kimlik Doğrulama Yöntemleri

Aşağıda Türkiye Cumhuriyeti Kimlik Kartı doğrulama yöntemleri, kimlik doğrulamada kullanılan güvenlik unsurları, gerekli olan bileşenler ve yöntemin uygulanması detaylı olarak açıklanmıştır. Hangi kimlik doğrulama tekniklerinin kullanılacağına, yapılacak risk değerlendirmesi sonucuna göre karar verilmektedir. Risk değerlendirmesi, TCKK üzerinden gerçekleştirilmesi planlanan işlemlerin türü (tipi, niteliği, varsa doğuracağı finansal ve finansal olmayan etkilerinin büyüklüğü gibi), işlem yapılan verinin hassaslık derecesi ve kimlik kartını kullanan kişiye göre değişebilen doğrulama tekniğinin kullanım kolaylığı da dikkate alınarak gerçekleştirilir. Şekil 5.8' de Türkiye Cumhuriyeti Kimlik Kartı doğrulama yöntemleri, kimlik doğrulamada kullanılan güvenlik unsurları ve gerekli olan bileşenler görülmektedir.



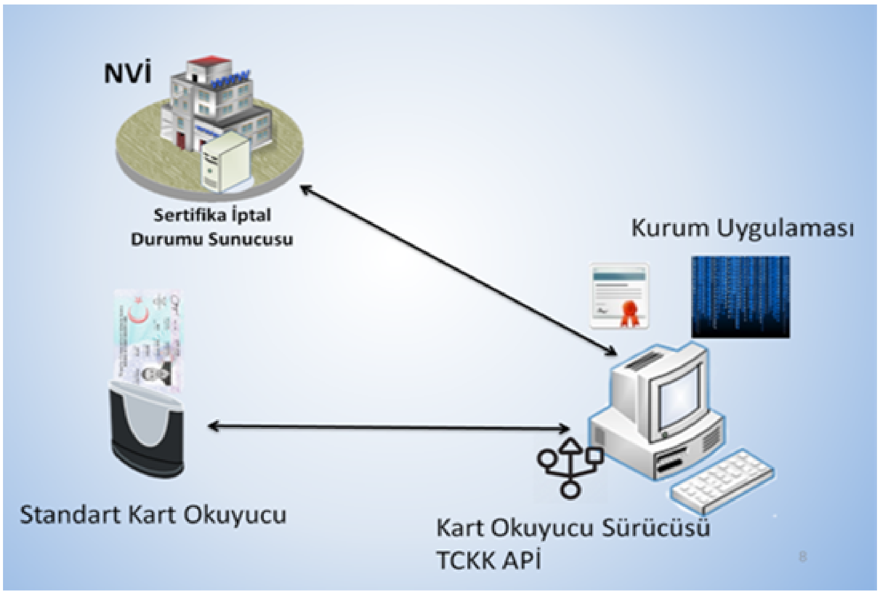
Şekil 5.8: Türkiye Cumhuriyeti Kimlik Kartı Doğrulanma Yöntemleri

1. Fiziksel Tanıma ve Doğrulama:

   Görsel güvenlik unsurları kullanılmaktadır. Gerekli olan bileşen olarak TCKK yeterlidir. Elektronik ortamın kullanılamadığı durumlarda geleneksel olarak kimlik doğrulama yapılmasını sağlamaktadır. Yöntemin Uygulanması: Bu kimlik tanıma ve doğrulama yöntemi elektronik değildir. KEC veya herhangi bir standart kart okuyucu kullanılmamaktadır. Kart gövdesi üzerinde bulunan güvenlik öznitelikleri kullanılarak fiziksel Kimlik Tanıma ve Doğrulama yapılmaktadır. Kişinin kimlik kartı üzerinde bulunan yonga (akıllı kart) Kimlik Tanıma ve Doğrulama sürecinde kullanılmamaktadır [13].

2. Standart Kart Okuyucu İle Kimlik Tanıma

   Güvenlik unsuru olarak Kimlik doğrulama sertifikası (KDS) kullanılmaktadır. Gerekli olan bileşenler TCKK ve standart kart okuyucudur. Hızlı şekilde KDS' den okunmuş bilgilerin NVİ kayıtlarında olup olmadığını ve sertifikanın geçerli olup olmadığını doğrulamaktadır. Yöntemin Uygulanması: Kimlik tanıma isteyen uygulama sunucusu, arabirim yazılımı vasıtasıyla TCKK' dan Kimlik Doğrulama Sertifikası'nı okur. Uygulama sunucusu, Kimlik Doğrulama Sertifikası' nın NVİ sunucusu tarafından imzalı olup olmadığını, sertifikanın son geçerlilik tarihini ve OCSP sorgusu ile sertifikanın aktif olduğunu kontrol eder. Şekil 5.9' da Standart Kart Okuyucu ile Kimlik Tanıma akış diyagramı verilmiştir [13].



Şekil 5.9: Standart Kart Okuyucu İle Kimlik Tanıma Genel Akışı

3. KEC ile Kimlik Tanıma:

Güvenlik unsuru olarak Kimlik doğrulama sertifikası (KDS), kişisel mesaj ve güvenli mesajlaşma kullanılmaktadır. Gerekli olan bileşenler TCKK ve KEC' dir. Kimlik Doğrulama Sertifikası' nın NVİ tarafından verilmiş bir TCKK içinden okunduğunu, sertifikada belirtilen kişinin NVİ kayıtlarında yer alıp almadığını ve sertifikanın geçerli olup olmadığı doğrulanmaktadır. Yöntemin Uygulanması: TCKK' nın KEC' e takılması ile KEC ve TCKK arasında güvenli mesajlaşma oturumu kurulur. Vatandaş KEC üzerinden kişisel mesajını kontrol ederek doğruluk onayı verir veya yanlış ise işlemi iptal eder. KEC, kişisel mesajın onaylanmasından sonra, TCKK içinden Kimlik Doğrulama Sertifikası' nı okur. KEC, Sertifikanın' nin NVİ sunucusu tarafından imzalı olup olmadığını, sertifikanın son geçerlilik tarihini ve OCSP sorgusu ile sertifikanın aktif olduğunu kontrol eder [13].

4. KKEC ve Fotoğraflı Kimlik Tanıma ve Doğrulama:

   Güvenlik unsuru olarak Kimlik doğrulama sertifikası (KDS), kişisel mesaj, güvenli mesajlaşma ve dijital fotoğraf kullanılmaktadır. Gerekli olan bileşenler TCKK, kurumsal KEC, hizmet isteyen, hizmete katılandır. KEC ile kimlik tanıma avantajlarına ek olarak, TCKK sahibinin veya benzerinin hizmet yerinde olup olmadığı anlaşılmaktadır. Yöntemin Uygulanması: KEC ile kimlik tanıma yöntemi uygulandıktan sonra TCKK yongası içinden okunan ve Kurumsal KEC ekranı üzerinden gösterilen dijital fotoğrafın, hizmet isteyene benzeyip benzemediği hizmete katılan tarafından kontrol edilmektedir. [13]

5. KEC Üzerinden Biyometrik Veri ile Elektronik Kimlik Doğrulama ve Tanıma:

   Güvenlik unsuru olarak Kimlik Doğrulama Sertifikası (KDS), kişisel mesaj, güvenli mesajlaşma ve biyometrik veri kullanılmaktadır. Gerekli olan bileşenler TCKK, KEC, hizmet isteyendir. KEC ile kimlik tanıma avantajlarına ek olarak, biyometrik veri ile doğrulama yapılmaktadır. Yöntemin Uygulanması: KEC ile kimlik tanıma yöntemi uygulandıktan sonra KEC' e girilen biyometri verisi ile TCKK içindeki biyometrik verinin aynı olup olmadığı kontrol edilmektedir. [13]

6. KKEC Üzerinden Biometrik Veri ve Fotoğraflı Elektronik Kimlik Doğrulama ve Tanıma:

   Güvenlik unsuru olarak Kimlik doğrulama sertifikası (KDS), kişisel mesaj, güvenli mesajlaşma, biyometrik veri ve dijital resim kullanılmaktadır. Gerekli olan bileşenler TCKK, kurumsal KEC, hizmet isteyendir. Kurumsal KEC ile kimlik tanıma ve doğrulama avantajlarına ek olarak, biyometrik veri ile doğrulama yapılmaktadır. Yöntemin Uygulanması: Kurumsal KEC ile kimlik tanıma ve doğrulama yöntemi uygulandıktan sonra KEC' e girilen biyometri verisi ile TCKK içindeki biyometrik verinin aynı olup olmadığı kontrol edilmektedir [13].

7. Standart Kart Okuyucu ve PIN ile Elektronik Kimlik Doğrulama ve Tanıma:

   Güvenlik unsuru olarak Kimlik Doğrulama Sertifikası (KDS) ve PIN kullanılmaktadır. Gerekli olan bileşenler TCKK, standart kart okuyucu, hizmet isteyen TCKK yongasının NVİ tarafından verildiği, Kimlik Doğrulama Sertifikası' nın TCKK' dan okunduğu, sertifikadaki kişinin NVİ kayıtlarında ve Sertifika' nın geçerli olduğu, PIN doğrulamasıyla kimlik doğrulama yapılmaktadır. Yöntemin Uygulanması: Kimlik tanıma isteyen uygulama sunucusu, arabirim yazılımı vasıtasıyla TCKK' dan Kimlik Doğrulama Sertifikası' nı okur. Uygulama sunucusu, sertifikanın NVİ sunucusu tarafından imzalı olup olmadığını, sertifikanın son geçerlilik tarihini ve OCSP sorgusu ile sertifikanın aktif olduğunu kontrol eder. Daha sonra hizmet isteyeninden PIN bilgisi istenir, PIN doğrulaması yapılarak kimlik doğrulama gerçekleştirilir [13].

8. KEC ve PIN ile Elektronik Kimlik Doğrulama ve Tanıma:

   Güvenlik unsuru olarak Kimlik doğrulama sertifikası (KDS), kişisel mesaj, güvenli mesajlaşma ve PIN kullanılmaktadır. Gerekli olan bileşenler TCKK, KEC, hizmet isteyendir. TCKK yongasının NVİ tarafından verildiği, Kimlik doğrulama sertifikası' nın TCKK' dan okunduğu, sertifikada belirtilen kişinin NVİ kayıtlarında yer alıp almadığı, sertifikanın geçerli olup olmadığının yanında PIN doğrulaması ile kimlik doğrulama yapılmaktadır. Yöntemin Uygulanması: Kurumsal KEC ile kimlik tanıma ve doğrulama yöntemi uygulandıktan sonra KEC 'e girilen biyometri verisi ile TCKK içindeki biyometrik verinin aynı olup olmadığı kontrol edilmektedir [13].

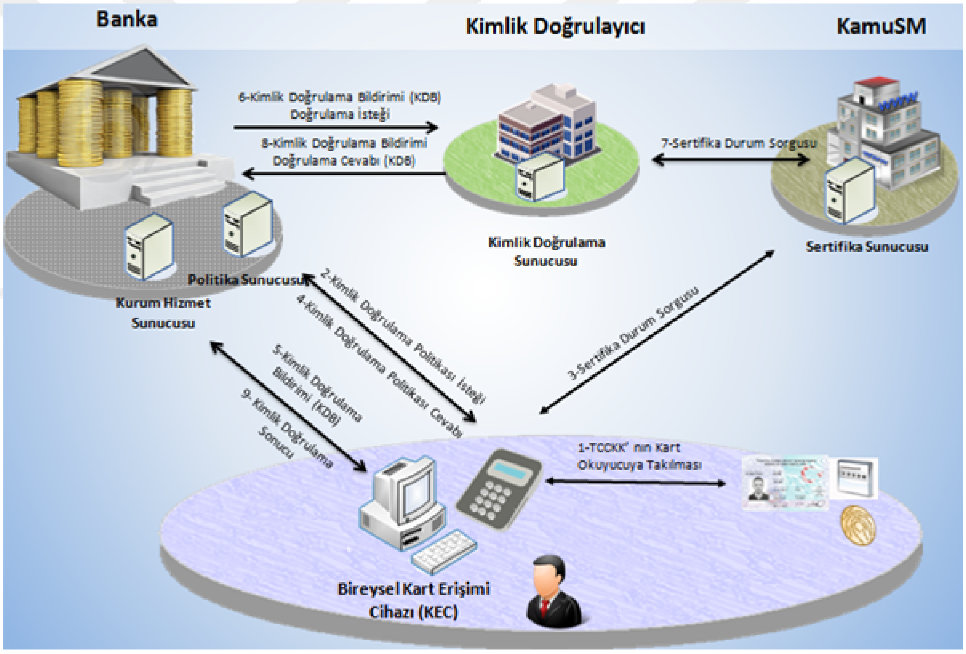
9. KKEC ile PIN ve Fotoğraflı Elektronik Kimlik Doğrulama ve Tanıma:

   Güvenlik unsuru olarak Kimlik doğrulama sertifikası (KDS), kişisel mesaj, güvenli mesajlaşma, PIN ve dijital resim kullanılmaktadır. Gerekli olan bileşenler TCKK, KEC, hizmet isteyen, hizmete katılandır. Kurumsal KEC ile Kimlik Tanıma avantajlarına ek olarak PIN doğrulaması ile kimlik doğrulama yapılmaktadır. Yöntemin

Uygulanması: Kurumsal KEC ile kimlik tanıma ve doğrulama yöntemi uygulandıktan sonra KEC' e girilen PIN ile kimlik doğrulama yapılmaktadır [13].

10. KEC, Biyometrik Veri ve PIN ile Elektronik Kimlik Doğrulama ve Tanıma:

    Güvenli unsuru olarak Kimlik doğrulama sertifikası (KDS), kişisel mesaj, güvenli mesajlaşma, PIN, biyometrik veri kullanılmaktadır. Gerekli olan bileşenler TCKK, KEC, hizmet isteyendir. KEC ile Kimlik Tanıma avantajlarına ek olarak PIN ve biyometrik veri doğrulaması ile kimlik doğrulama yapılmaktadır. Yöntemin Uygulanması: KEC ile kimlik tanıma ve doğrulama yöntemi uygulandıktan sonra KEC 'e girilen PIN ve Biyometrik veri ile kimlik doğrulama yapılmaktadır. Şekil 5.10' da KEC, Biyometrik Veri ve PIN ile Elektronik Kimlik Doğrulama ve Tanıma akış diyagramı verilmiştir [13].



Şekil 5.10: Biyometrik Veri ve PIN ile Kimlik Doğrulama ve Tanıma Genel Akışı

Kimlik doğrulama talebinin süreci başlatması ile birlikte;

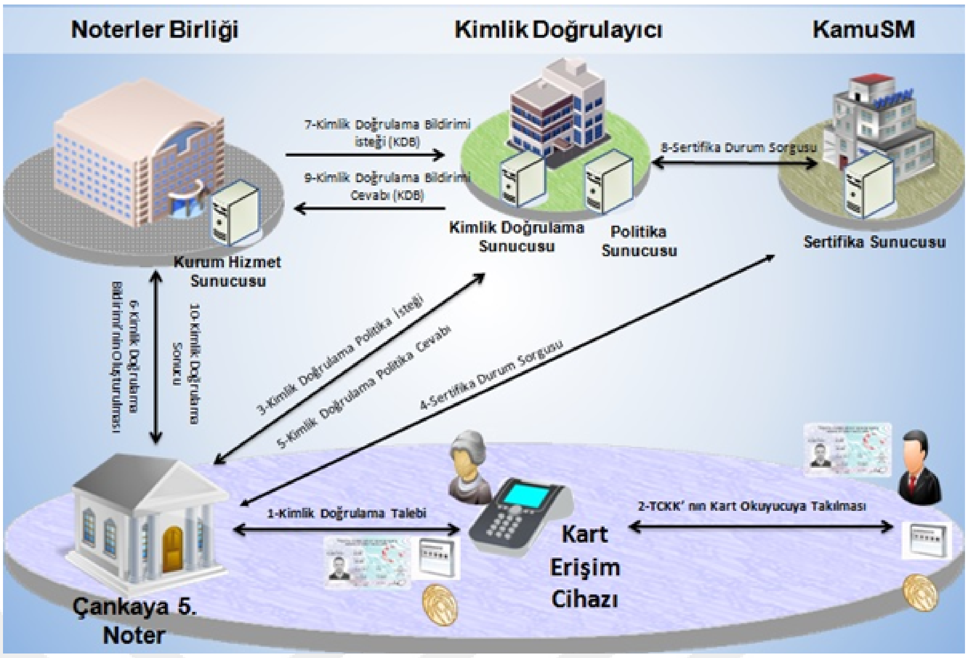
- *Adım1*:TCKK' nın Kart Okuyucuya takılması
- *Adım2*:Kimlik Doğrulama Politikası' nın belirlenmesi (Politika İsteği)
- *Adım3*:TCKK' nın geçerliliğinin doğrulanması (Çevrimiçi Sertifika Durum Sorgusu)
- *Adım4*:Politikaya uygun vatandaş verilerinin alınması (PIN, Biyometri vs)

- *Adım5*:Vatandaş verisinin doğrulanması Kimlik Doğrulama Bildirimi' nin oluşturulması
- *Adım6*:Kimlik Doğrulama Bildirimi' nin Kimlik Doğrulama Sunucusu tarafından doğrulanması (İsteği)
- *Adım7*:Kimlik Doğrulama Sunucusunun Sertifikayı Sertifika Sunucu' na çevrimiçi doğrulatması
- *Adım8*:Kimlik Doğrulama Bildirimi onayının hizmet veren kurum sunucusuna ulaştırılması (Cevabı)
- *Adım9*:Hizmetin talep eden vatandaşa verilmesi

11. KKEC, Biyometrik Veri, PIN ve Fotoğrafla Elektronik Kimlik Doğrulama ve Tanıma

Güvenlik unsuru olarak Kimlik doğrulama sertifikası (KDS), kişisel mesaj, güvenli mesajlaşma, PIN, biyometrik veri ve dijital resim kullanılmaktadır. Gerekli olan bileşenler TCKK, KEC, hizmet isteyen, hizmete katılandır. Kurumsal KEC ile Kimlik Tanıma avantajlarına ek olarak PIN ve biyometrik veri doğrulaması ile kimlik doğrulama yapılmaktadır. Yöntemin Uygulanması: Kurumsal KEC ile kimlik tanıma ve doğrulama yöntemi uygulandıktan sonra KEC' e girilen PIN ve Biyometrik veri ile kimlik doğrulama yapılmaktadır. Şekil 5.11' de KKEC, Biyometrik Veri ve PIN ve Fotoğraf ile Elektronik Kimlik Doğrulama ve Tanıma akış diyagramı verilmiştir [13].

- *Adım1*:Hizmet Veren Kurum, Kimlik Erişim Cihazından Kimlik doğrulama talebinde bulunur.
- *Adım2*:TCKK' nın Kart Okuyucuya takılması
- *Adım3*:Kimlik Doğrulama Politikası' nın belirlenmesi(Politika İsteği)
- *Adım4*:TCKK' nın geçerliliğinin doğrulanması (Çevrimiçi Sertifika Durum Sorgusu)
- *Adım5*:Politikaya uygun vatandaş verilerinin alınması (Politika Cevabı PIN, Biyometri vs)
- *Adım6*:Vatandaş verisinin doğrulanması Kimlik Doğrulama Bildirimi' nin oluşturulması



Şekil 5.11: KKEC, Biyometrik Veri, PIN ve Fotoğrafla Elektronik Kimlik Doğrulama ve Tanıma Genel Akışı

- *Adım7*:Kimlik Doğrulama Bildirimi' nin Kimlik Doğrulama Sunucusu tarafından doğrulanması (İsteği)
- *Adım8*:Kimlik Doğrulama Sunucusunun TCKK Sertifikasını, Sertifika Sunucusu' na çevrimiçi doğrulatması
- *Adım9*:Kimlik Doğrulama Bildirimi onayının hizmet veren kurum sunucusuna ulaştırılması (Cevabı)
- *Adım9*:Kimlik Doğrulama Sonucunun iletilmesi

5.2.4 Elektronik Kimlik Doğrulama Sistemi' nin Amaçları

- *Vatandaş Yönünden*
  - Nüfus işlemlerini hızlandırmak,
  - Kamu hizmetlerinin tek bir noktadan ve güvenli alınabilmesini sağlamak (e-Devlet dönüşümüyle kamu kurum ve kuruluşlarının T.C. kimlik kartı vasıtasıyla tam entegrasyonu sonucu vatandaşın, askerlik, pasaport ve iş başvurusu işlemleri, noterlik işlemleri gibi birçok hizmeti alırken kamu kurumlarını dolaşmak zorunda kalmaması),

- Hizmet alımı giderlerini azaltmak

- *Devlet Yönünden*
  - Vergi tâhsilatı ve denetimini kolaylaştırmak,
  - Kayıt dışı ekonomiyi kontrol altına alabilmek.

- *Güvenlik Yönünden*
  - Suçlu takibi ve yakalanmasında kolaylık,
  - Hızlı kimlik tespit imkânı sağlamak ve sahteciliği engellemek,

- *Askerlik Yönünden*
  - Askere alma işlemlerinde asker kaçaklarının takibini kolaylaştırmak.

- *Sağlık Yönünden*
  - T.C. Kimlik Numarası sayesinde kişinin birden fazla sağlık dosyası olmasını engellemek,
  - Sağlık bilgilerinin birleştirilmesini kolaylaştırmak ve doğru kişinin hizmetlerden yararlanmasını sağlamak

- *Eğitim Yönünden*
  - Eğitimle ilgi kayıt ve sınav gibi işlemlerde doğru kişinin hizmetlerden yararlanmasını sağlamak.

- *Sosyal Güvenlik Yönünden*
  - Tek numara ve güvenli kimlik kartı ile sosyal güvenlik kurumları arası bilgi takibi ve hizmet birleştirilmesini kolaylaştırmak.

- *Adalet Yönünden*
  - Davalarda kimlik tespitlerinin daha hızlı ve doğru bir şekilde yapılmasını sağlamak [1].

5.2.5 Elektronik Kimlik Doğrulama Sistemi' nin Hedefleri

- Türk vatandaşlarının sahip oldukları nüfus cüzdanlarını Avrupa ve dünya standartlarına uygun, her çeşit taklit, tahrif ve sahteciliği ortadan kaldıracak özelliklerde yeni ve güvenli kimlik kartlarıyla değiştirmek,
- Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün yükümlülüğünde olan kimlik kartı düzenleme süreçlerinin yeni teknolojik altyapıya uyumunu sağlamak,
- Uluslararası standartlara uyum sağlamak,
- İhtiyaç duyulan verilere elektronik ortamda ulaşılmasını kolaylaştırmak,
- Kamu kurum ve kuruluşları arasındaki bilgi akışını hızlandırmak,
- İşlem zorluklarının yarattığı savurganlık, zaman ve iş gücü kaybını önlemek, vatandaşlara kaliteli ve hızlı hizmet vermek,
- Kimlik kartı işlemlerini, hukuki ve teknik olarak merkezden denetlenebilir hale getirmek,
- Özel ve resmi işlemlerde sahteciliği en aza indirerek "mal güvenliği" ve "kişi haklarını" sağlamak,
- Kart materyalinin isterler çerçevesinde gerçekleştirmek,
- Milli bir kart ve yonga işletim sistemi kullanmak,
- Yeni teknolojilere uyum sağlayabilen kart üretim ve kişiselleştirme sistemi oluşturmak

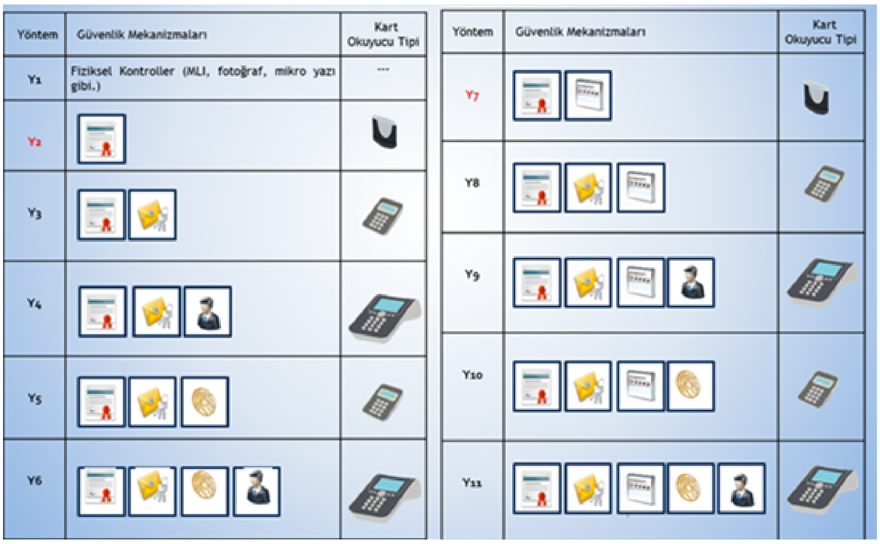
Bölüm 6

Türkiye Cumhuriyeti Kimlik Kartı'nın Ticarette Kullanım Analizi

Kimlik kartları vatandaşların sahip oldukları ve yalnızca kendilerinin bileceği PIN kodları sayesinde kamu ve özel sektör uygulamalarında Chip&PIN doğrulaması yapılmasına imkan verebilmekte; ayrıca bünyesinde barındırdığı biyometrik özellikleri ile (parmak izi, parmak damar izi, avuç içi izi) de gerekli görüldüğü durumlarda vatandaşların biyometrik doğrulamalarının da yapılmasını sağlayabilmektedir. Hâlihazırda 11 farklı doğrulama yöntemi ile doğrulanabilecek e-kimlik kartlarının doğrulama yöntemleri incelendiğinde; "Chip&PIN" doğrulama yönteminin gerek ihtiyaç duyulan asgari güvenlik şartlarını sağlaması gerekse geniş sektörel kullanım yaygınlığına ulaşabilmesi açısından en ideal olan yöntem olduğu görülmektedir [26].

Aşağıda Şekil 6.1' de Türkiye Cumhuriyeti Kimlik Kartı doğrulama yöntemleri, kimlik doğrulamada kullanılan güvenlik unsurları ve gerekli olan bileşenler görülmektedir.

Chip&PIN doğrulama yönteminin üzerine ek bir güvenlik seviyesine ihtiyaç duyulan özel uygulamalarda ise biyometrik doğrulama yönteminin kullanımı sektörel oyuncuların kendi tercihleri olması önerilmektedir [4]. E-Kimlikler üzerinde sunulacak Chip&PIN doğrulama yöntemi bugün itibariyle tüm banka ve kredi kartları için kullanılan EMV standardı olan Chip&PIN doğrulama yöntemleri ile güvenlik açısından aynı seviyede bir güvenlik sunduğu görülmektedir. E-Kimlikler üzerindeki Chip&PIN hizmetini sunan ve



Şekil 6.1: Türkiye Cumhuriyeti Kimlik Kartı Doğrulanma Yöntemleri

TÜBİTAK tarafından geliştirilen Elektronik Kimlik Doğrulama Sistemi (EKDS) bileşenleri incelendiğinde, aşağıdaki konularda bankacılık sektörünün ihtiyaç duyduğu çift faktörlü doğrulamayı sağladığı görülmektedir [4].

- Kart Geçerlilik Doğrulama (Sahip Olunan Faktör): e-Kimlik kartlarının üzerindeki kart sertifikaları online ve gerçek zamanlı olarak NVİ Kimlik Doğrulama Sunucuları üzerinden kontrol edilebilmekte; bu sayede sahte veya iptal edilmiş kartların sektörel kullanımının önüne anlık olarak geçilebilmektedir.
- PIN Doğrulama (Bilinen Faktör): Kart okuyucularda tuşlanan PIN' in doğruluğu e-Kimlik kartlarının üzerindeki yonga üzerinde anlık olarak kontrol edilebilmekte ve kartı taşıyan kişinin kart sahibi olan kişi olduğu teyit edilebilmektedir [4].

Bu sebeple e-kimlik kartları üzerinde bulunan EKDS sisteminin:

- Vatandaşın taşıdığı kimlik kartının yetkili kurum tarafından verildiği ve işlem anında geçerli olduğunu,
- Vatandaşın kartın gerçek sahibi olduğunu ve kimlik doğrulama sırasında hizmet verilen yerde olduğunu,
- Kimlik doğrulama işleminin nerede, ne zaman, kim tarafından ve ne için gerçekleştirildiğini garanti eden bir sistem olduğu görülmektedir [13].

Bu değerlendirmeler çerçevesinde, e-kimliklerin Chip&PIN doğrulaması ile kullanılabilmesi sayesinde gerek yüz yüze bankacılık kanallarında (şube) gerekse mesafeli bankacılık kanallarında (Internet Bankacılığı, Mobil Bankacılık, ATM, vb.)finansal tüketicilerin kolaylıkla ve güvenli bir şekilde doğrulanabilmeleri mümkün olacaktır. Bu vesile ile gerek sürekli iş ilişkilerinin ilk tesisi süreçlerinde, gerekse de mevcut müşterilerin şube ve mesafeli bankacılık arayüzlerine erişiminde e-kimlik kullanılabilir hale gelecektir [4]

Bölüm 7

TCKK'nın ÖKC İle Entegrasyon Çözümü ve Örnek Senaryo

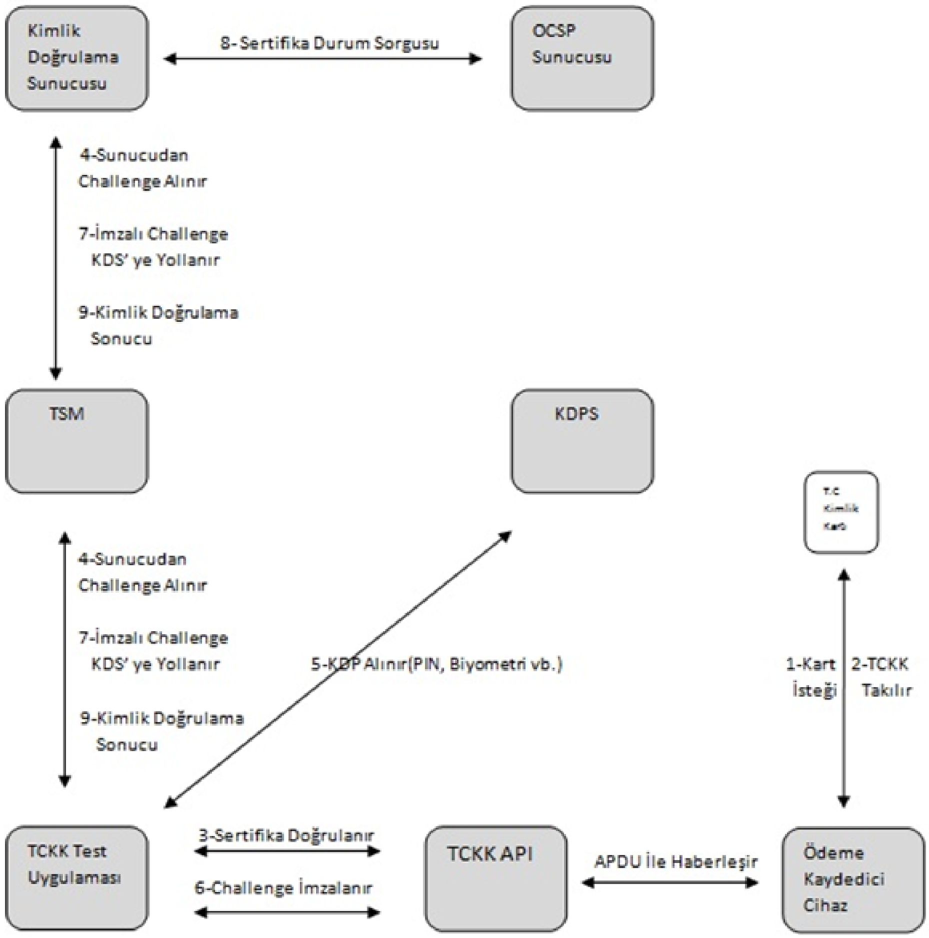
Yeni Nesil Ödeme Kaydedici Cihaz'larda ödeme işlemlerini yapan Banka Uygulamaları ve Yemek Kartı Uygulamaları (Sodexo, Ticket vb.) 3. Parti Uygulama olarak çalışmaktadır. Cihaz sahibi mükellef, hangi banka ile çalışmak isterse o bankanın sunucularına o cihazı tanımlatmaktadır. Cihazlara banka uygulaması gibi 3. Parti uygulamaları yükleme işlemi ise Ödeme Kaydedici Cihaz üreten firmalar aracılığıyla güvenli odalarda veya TSM' ler üzerinden güvenli iletişim kanallarıyla yapılmaktadır.

Ödeme Kaydedici Cihazlar da mevcut durumda ana işlemci üzerinde çalışan mali bir uygulama bulunmaktadır. Bu uygulama cihaz içerisindeki donanımların birbiri ile iletişimini sağlamakta, TSM ile veri alışverişini yapmakta ve cihaz üzerinde bulunan 3. Parti yazılımlarla senkronize olarak çalışmaktadır. Bu entegrasyon kapsamında yazmış olduğum uygulama(TCKK Test Uygulaması), Ödeme Kaydedici Cihazlar' da 3. Parti uygulama olarak çalışmaktadır.

TCKK Test Uygulaması yüklü Ödeme Kaydedici Cihaz' da vatandaş alışverişini tamamlayıp ödeme işlemine geçtikten sonra cihaz üzerinde mali uygulama tutar bilgisini TCKK Test Uygulaması' na gönderip kendini beklemeye almaktadır. Uygulamam ilk olarak TCKK' nın NVİ tarafından verilmiş geçerli bir TCKK olup olmadığını kontrol etmektedir. Kontrol başarılı olursa ödeme işlemine geçilmektedir. Kimlik doğrulama süreci Bölüm 7.1' de akış diyagramı ile birlikte detaylı olarak açıklanmaktadır.

7.1 Kimlik Kartı Doğrulanma İşlemi

Şekil 7.1' dekii akış diyagramı verilen kimlik doğrulama süreci, akış diyagramının altında detaylı olarak açıklanmaktadır.



Şekil 7.1: Kimlik Doğrulama Süreci Akış Diyagramı

Ödeme Kaydedici Cihaz' da satış işlemi yapılır ve ödeme seçeneği olarak TCKK seçilir.

- *Adım1*: Ödeme Kaydedici Cihaz içerisindeki TCKK Test Uygulaması, TCKK' nın ilgili dosyasından read record komutu ile kart kullanıcısının bilgilerini okur. Bu bilgiler kartla ilgili (TC Kimlik Numarası, kartın son kullanım tarihi, Kart Unit ID' si vb.)' dir.
- *Adım2*:TCKK Ödeme Kaydedici Cihaz'a takılır.
- *Adım3*:TCKK Test Uygulaması, Kimlik Doğrulama talebini TCKK' ya gönderir. TCKK API ile "Kimlik Doğrulama Sertifikası" offline olarak doğrulanır. İstenirse

online doğrulama da yapılabilir. Fakat ileriki aşamalarda KDS' de sertifikayı online olarak doğrulayacağı için fazladan işlem yapılmış olur.

Ödeme Kaydedici Cihaz üzerinde çalışan TCKK Test Uygulaması, Kimlik Doğrulama talebini TCKK API' den alır. Ödeme Kaydedici Cihaz, TCKK API ile APDU aracılığıyla haberleşir. Uygulama katmanında, kart ve okuyucu arasındaki tüm iletişim, uygulama protokolü veri birimleri (APDU, Application Protocol Data Unit) adı verilen yapılarla gerçekleşir.

- *Adım4*: TCKK Test Uygulaması, TSM aracılığıyla Kimlik Doğrulama Sunucusuna giderek Challenge değerini alır.

- *Adım5*: Uygulama bu aşamada isterse Kimlik Doğrulama Politika Sunucusu' dan (KDPS) Kimlik Doğrulama Politikasını(KPS) alabilir. KDPS, kimlik doğrulama sırasında kart okuyucu tarafından kullanılacak kimlik doğrulama yöntemi, güvenlik seviyesi, kimlik doğrulama süresi kimlik doğrulama geçerlilik süreleri gibi parametrelerden oluşan imzalı Kimlik Doğrulama Politikası'nı (KDP) belirleyen sunucudur.

- *Adım6*: Challenge değeri, kullanıcıdan alınan PIN değeri ile TCKK API kullanılarak TCKK' ya imzalatılır.

- *Adım7*:TCKK API tarafından imzalan challenge değeri KDS' ye yollanır. Kimlik Doğrulama Sunucusu kendisine gelen challenge değerini kontrol eder. KDS kimlik doğrulama sonuçlarını Kurum Hizmet Sunucuları için değerlendiren ve doğrulayan merkezi sunucudur.

- *Adım8*: Kimlik Doğrulama Sunucusu (KDS) , OCSP den online olarak sertifika sorgusunu yapar. OCSP sunucusu bağlı olduğu SM' nin yayınladığı sertifikaların iptal edilip edilmediği bilgisine online olarak ulaşmakta ve kendisine gelen kullanıcı isteklerini cevaplamaktadır.

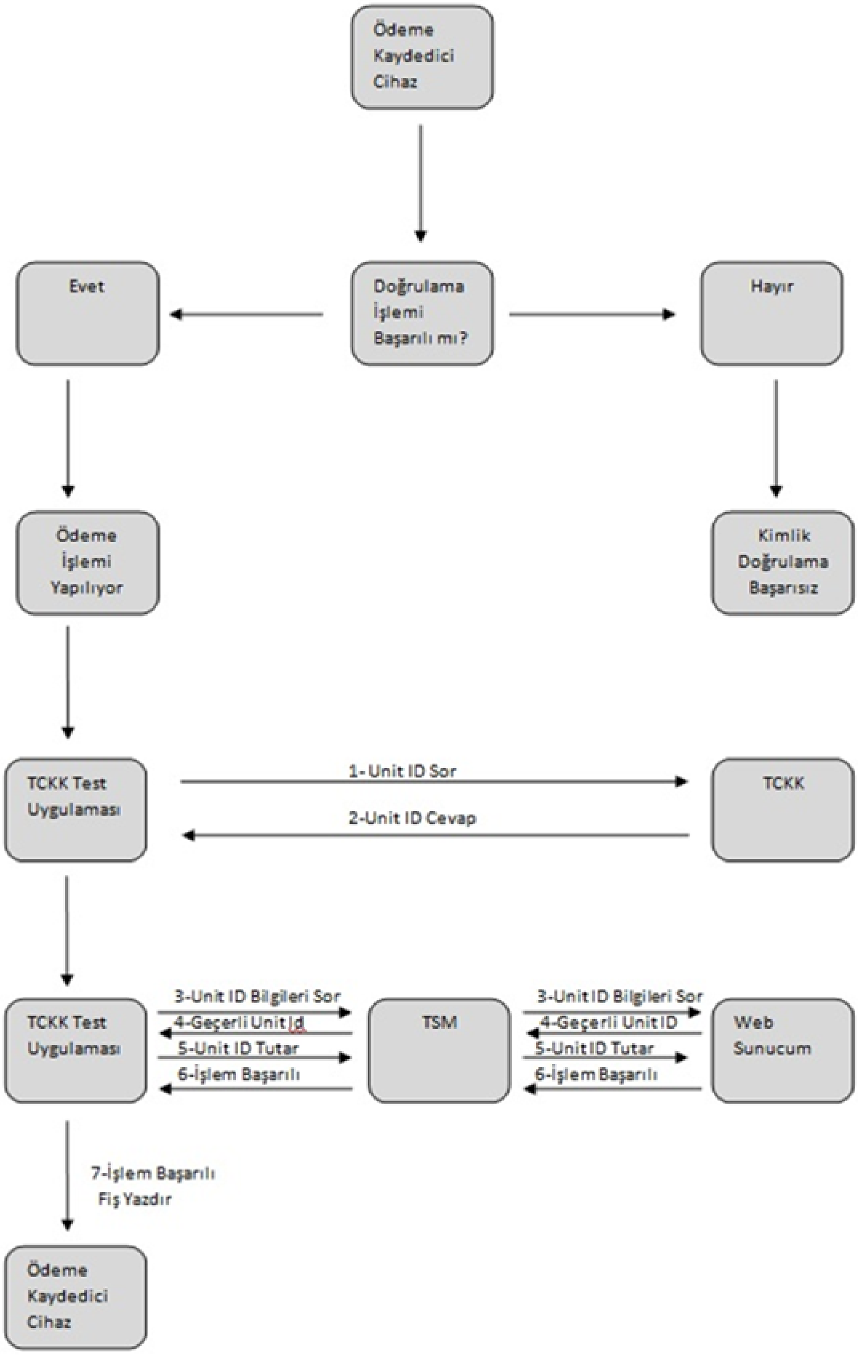
- *Adım9*: Doğrulama sonucu başarılı ise Kimlik Doğrulama Sunucusu başarılı cevabı ile birlikte kullanıcının TCKN ve Ad Soyad bilgisini döner. Başarısız ise hata mesajı döner.

Kimlik doğrulama sonucu başarılı olursa TCKK Test Uygulaması işleme devam edip ödeme işlemini başlatır.

7.2 Kimlik Kartı Ödeme Alma İşlemi

TCKK, Yeni Nesil Ödeme Kaydedici Cihaz üzerinden kimlik doğrulama işlemi yapıp sonucu başarılı döndükten sonra ödeme işlemi başlatılır. Ödeme İşleminde TCKK Test Uygulaması TCKK' ya ait bilgileri ve işlem tutarını alarak yazmış olduğum Web Sunuya gidip bu bilgilere ait bir TCKK' nın, sunucu veritabanında kayıtlı olup olmadığını ve bakiyesini kontrol etmektedir. Web Sunucudan başarılı olarak cevap almasının ardından işlem tutarı kart bakiyesinden düşmektedir. Şekil 7.2' de akış diyagramı verilen ödeme alma işlemi aşağıdaki detay olarak açıklanmıştır.

- *Adım1*:Ödeme Kaydedici Cihaz üzerinde 3. Parti yazılım olarak çalışan TCKK Test Uygulaması, Ödeme Kaydedici Cihaz aracılığıyla vatandaş' dan kart isteğinde bulunur.
- *Adım2*: TCKK' dan Unit ID Cevabı alınır.
- *Adım3*:TCKK' dan bilgileri alan TCKK Test Uygulaması, TSM üzerinden kartın Unit ID' si ile, İlgili kartın Web Sunucuya tanımlı olup olmadığını sorar. Web Sunucudan cevap alınır ve verinin bütünlüğü kontrol edilir.ÖKC üzerinde çalışan TCKK Test Uygulaması, kimlik doğrulama talebini TCKK API' den alır. ÖKC, TCKK API ile APDU aracılığıyla haberleşir. Uygulama katmanında, kart ve okuyucu arasındaki tüm iletişim, uygulama protokolü veri birimleri (APDU, Application Protocol Data Unit) adı verilen yapılarla gerçekleşir.
- *Adım4*: Web sunucudan geçerli Unit ID cevabı alınır.
- *Adım5*: Web sunucudan geçerli Unit ID cevabı alınması ile birlikte, TCKK Test Uygulaması Ödeme Kaydedici Cihaz üzerindeki yapılmış olan işlem tutarını, işlemi tanımlayan sayaç değerini (ATC Application transaction counter), Geçerli Unit ID ile birlikte TSM üzerinden Web Sunucuya gönderir.
- *Adım6*: Gönderilen İşlem tutarı, işlemi yapan TCKK Bakiyesinden düşülür. Web Sunucu, İşlem Başarılı cevabını TSM Üzerinden TCKK Test Uygulaması' na gönderir.
- *Adım7*: İşlem başarılı cevabını alan TCKK Test Uygulaması Ödeme Kaydedici Cihaz' a fiş kesme işlemi ile ilgili komutu göndererek yazıcıdan fiş kesilmesi sağlanır.

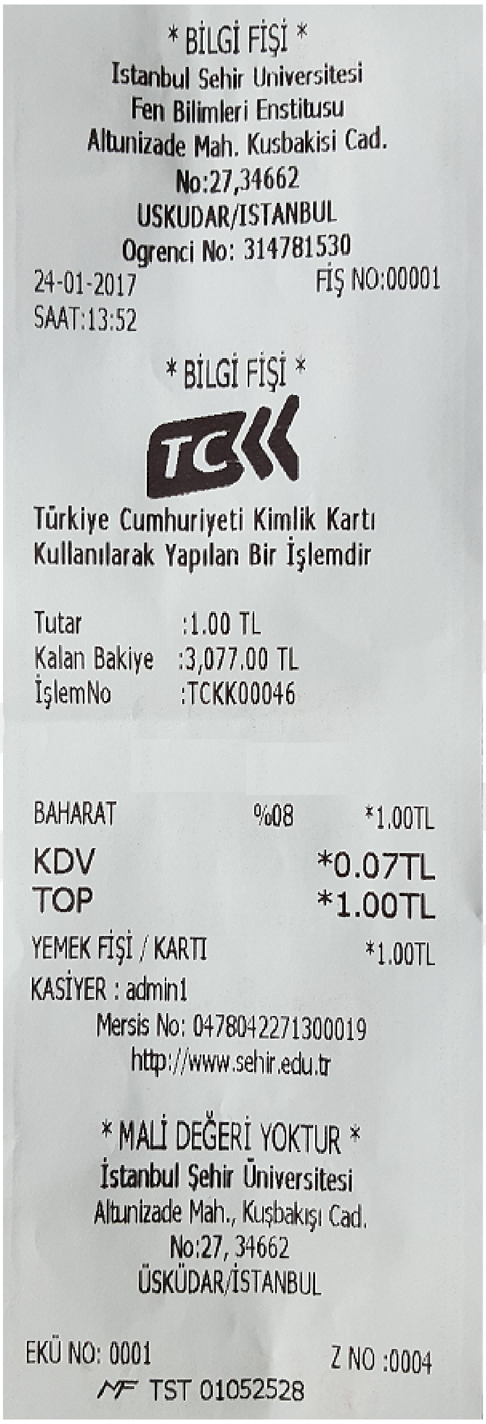


Şekil 7.2: Ödeme İşlemi Süreci Akış Diyagramı

Eğer Web Sunucu işleme izin verirse başarılı komutu ile dönüş yapacak, izin vermezse işlemi yarıda kesecek olan işlem başarısız komutu ile dönecektir. (Bu işlemde Başarılı cevabı dönmesi için Kartın daha önce Web Sunucuya tanınmış olması, kart bakiyesinin yeterli olması, kartın iptal edilmemiş olması gerekir).

Bu kullanım vakasında, vatandaş alışverişini yapmış, Ödeme işlemi için banka kartı yerine TCKK' nı kullanmıştır. TCKK' nın NVİ tarafından verilmiş geçerli bir TCKK olup olmadığı kontrol edilmiş, Kimlik kartının doğrulanma işlemi, Ödeme Kaydedici Cihaz ile çevrimiçi ve TCKK 'nın fiziksel özellikleri ile yapılmıştır. Kimlik doğrulama talebi gönderilmiş KDS' nın ve tüm sertifika zinciri kontrol edilmiş KDB' nin doğrulanması ve KDB onayının üretilmesi sağlanmıştır. NVİ tarafından verilmiş geçerli bir TCKK içindeki bir dosyaya erişimin nasıl yapılacağı ve yapılırken gerekli yetkilere sahip olunup olunmadığı sınanmıştır. Bu entegrasyon kapsamında Ödeme Kaydedici Cihaz ile TCKK veri alanlarına rol tabanlı erişim yapılmış, TCKK' nın rol tabanlı olma özelliğinden faydalanılmıştır.

Kimlik doğrulama işlemi başarılı bir şekilde gelmesi ile TCKK Test uygulaması tarafından TCKK' nın kart bilgileri okunmuş ve bu kart bilgileri ile web sunucuya gidilmiş kartın web sunucuda tanımlı olup olmadığına bakılmıştır. Web Sunucum tanımlı komutu gönderilmesi ile birlikte vatandaşın yaptığı alışveriş tutarı web sunucuya tekrar gönderilmiş ve kart bakiyesinden düşülmüştür. Ödeme Kaydedici Cihaz üzerinde çalışan TCKK Test Uygulaması bu işlem sonucunda vatandaşa yaptığı işlemin detaylarını (tarih, saat, fiş numarası, Z numarası kalan bakiye bilgisi, işlem iptal numarası vb.) gösteren Şekil 7.3'deki fiş çıktısını vermiştir.



* BİLGİ FİŞİ *
Istanbul Sehir Universitesi
Fen Bilimleri Enstitusu
Altunizade Mah. Kusbakisi Cad.
No:27,34662
USKUDAR/ISTANBUL
Ogrenci No: 314781530
24-01-2017 FİŞ NO:00001
SAAT:13:52

* BİLGİ FİŞİ *

Türkiye Cumhuriyeti Kimlik Kartı
Kullanılarak Yapılan Bir İşlemdir

Tutar :1.00 TL
Kalan Bakiye :3,077.00 TL
İşlemNo :TCKK00046

BAHARAT %08 *1.00TL
KDV *0.07TL
TOP *1.00TL
YEMEK FİŞİ / KARTI *1.00TL
KASİYER : admin1
Mersis No: 0478042271300019
http://www.sehir.edu.tr

* MALİ DEĞERİ YOKTUR *
İstanbul Şehir Üniversitesi
Altunizade Mah., Kuşbakışı Cad.
No:27, 34662
ÜSKÜDAR/İSTANBUL

EKÜ NO: 0001 Z NO :0004
TST 01052528

Şekil 7.3: TCKK ile Yapılan Ödemenin Fiş Çıktısı

7.3 TCKK Test Uygulaması

C# programlama dilini kullanarak yazmış olduğum TCKK Test Uygulaması aşağıda Şekil 7.4 ' de görülen Microsoft Windows CE 6.0 R3 işletim sistemli Ödeme Kaydedici

Cihaz' da 3. Parti Uygulama olarak çalışmaktadır.

Şekil 7.4: Windows İşletim Sistemi Bulunan Ödeme Kaydedici Cihaz

Manyetik Kart Okuyucu, ICC Kart Okuyucu ve RFID bulunan cihaz' ın TCKK ile haberleşmesi ICC Kart Okuyucu aracılıyla olmaktadır. Ödeme Kaydedici Cihaz' ın diğer teknik özellikleri aşağıdaki gibidir.

- Microsoft Windows CE 6.0 R3 işletim sistemi
- 1GHZ A8 CORTEX CPU işlemci
- 56 MB bellek
- 3.5 inch 240 X 320 Piksels / 262,000 Color ekran çözünürlüğü
- 7mm Font Color LCD arka ekran
- 1 USB (OTG type, Host port, Client port), 1 USB(RS232port) arayüzü
- High speed, high resolution, thermal printer
- GSM/GPRS/EDGE /CDMA/3G modem
- SiRFstarIII GSC3e/LP GPS
- Dokunmatik ve tuşlu klavye
- 2000 veya 2300 mah. şarj edilebilir batarya
- MAXQ1850 işlemci
- Parmak izi okuyucu
- PCI 3.1 Online/Offline onayı

- EMV L1&L2 Certified Smart Card Reader, 2 SAMs slot akıllı kart
- Triple Track (track 1,2, & 3) manyetik kart okuyucu
- QR Kod BARKOD: 3.1 MP kamera
- 1D ve 2D barkod okuyucu

Vatandaş Şekil 7.5' de görüldüğü gibi İçecek, Şarküteri, Ekmek gibi günlük alışverişini yaptıktan sonra satış ekranından Şekil 7.5' de görülen ekrandan, ödeme türü olarak TCKK seçip daha sonra Ödeme Kaydedici Cihaz' ın ICC Kartı Okuyucu bölümüne kimlik kartını okutmaktadır. TCKK Test Uygulaması ilk olarak kimlik kartı doğrulaması daha sonra ise ödeme alma işlemini gerçekleştirmektedir.

Şekil 7.5: Ödeme Kaydedici Cihaz Ürün Eklenmiş Satış Ekranı

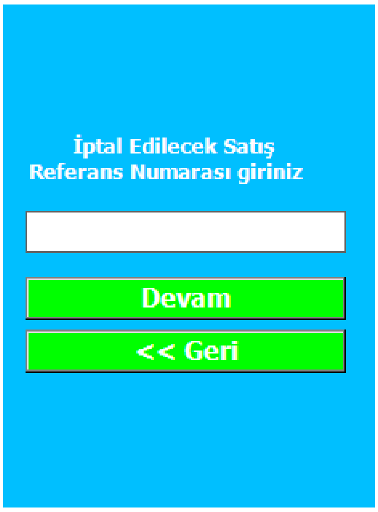
Şekil 7.6' da görülen TCKK Test Uygulamasında, Kart Bilgilerini Göster bölümüne basıldığında aşağıdaki Şekil 7.7' de görülen kart sorgulama ekranı gelmektedir. Bu ekrandan, T.C Kimlik Numarası veya Kart ID' si girilerek sorgulama işlemi yapıldığında karta ait bakiye bilgisi öğrenilmektedir.Son Fiş kopyası bölümüne basıldığında ise TCKK ile yapılmış olan son fişin kopyası Ödeme Kaydedici Cihaz tarafından basılmaktadır.

Şekil 7.6' de ana menüde yer alan satış iptal tuşuna basıldığında ise o TCKK ile daha önce yapılmış satışın, satış fişindeki iptal referans numarası Şekil 7.8' da görülen ekrandaki bölüme girilerek satış iptali yapılıp bakiye iadesi yapılabilmektedir.

Aşaıdaki Şekil 7.9' de ve Şekil 7.10' de TCKK Test uygulaması sertifika doğrulama ve PIN sorgulama adımları görülmektedir.

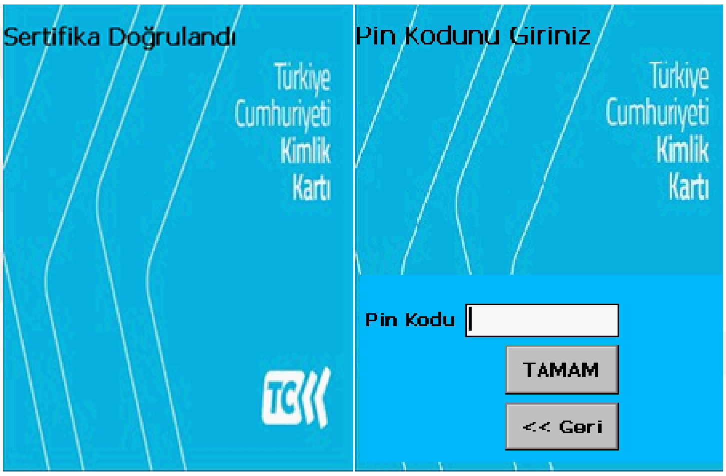
Şekil 7.6: TCKK Test Uygulaması Ana Menü

Şekil 7.7: TCKK Test Uygulaması Kart Sorgulama Ekranı



Şekil 7.8: TCKK Test Uygulaması Satış İptal Ekranı

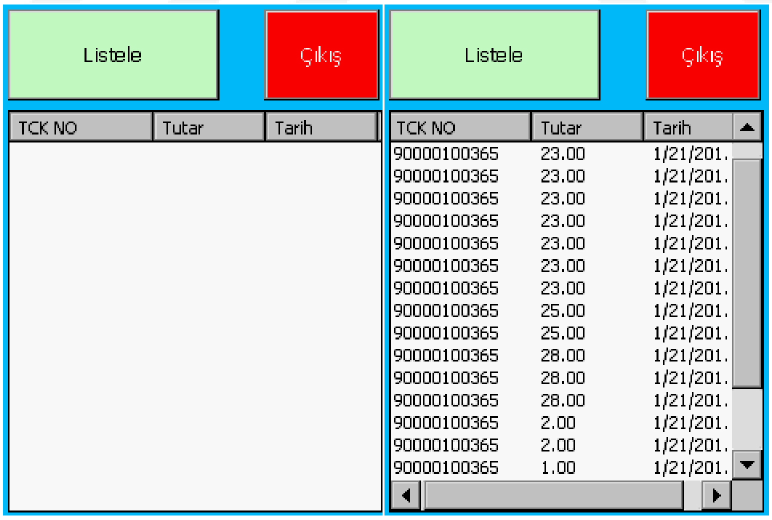
Şekil 7.9: TCKK Doğrulanma İşlemi 1



Şekil 7.10: TCKK Doğrulanma İşlemi 2

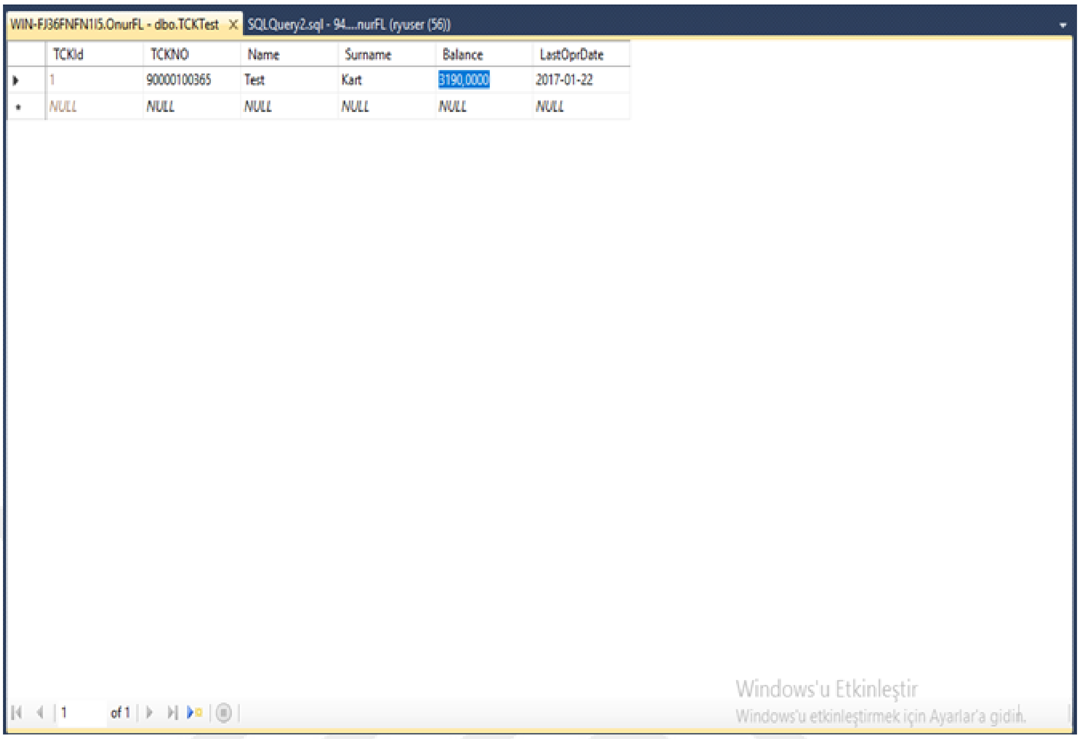
Şekil 7.6' de TCKK Test Uygulaması ana menüsünde görülen TCKK İşlemleri bölümüne girilerek, daha önce yapılmış satışlara ait Şekil 7.11' de görülen Satış Kopyası, Özet Raporu, Ayrıntılı Rapor, Gün Sonu Raporu, Aylık Rapor gibi bilgilere ulaşılabilir. Bu menü Ödeme Kaydedici Cihaz sahibinin isteklerine göre daha detaylı bilgiler içerecek şekilde geliştirilebilir.Ayrıntılı rapora basıldığında ise Şekil 7.12' de daha önce TCKK ile yapılmış satışlar listelenmektedir.

Şekil 7.11: TCKK Test Uygulaması TCKK İşlemleri Ekranı

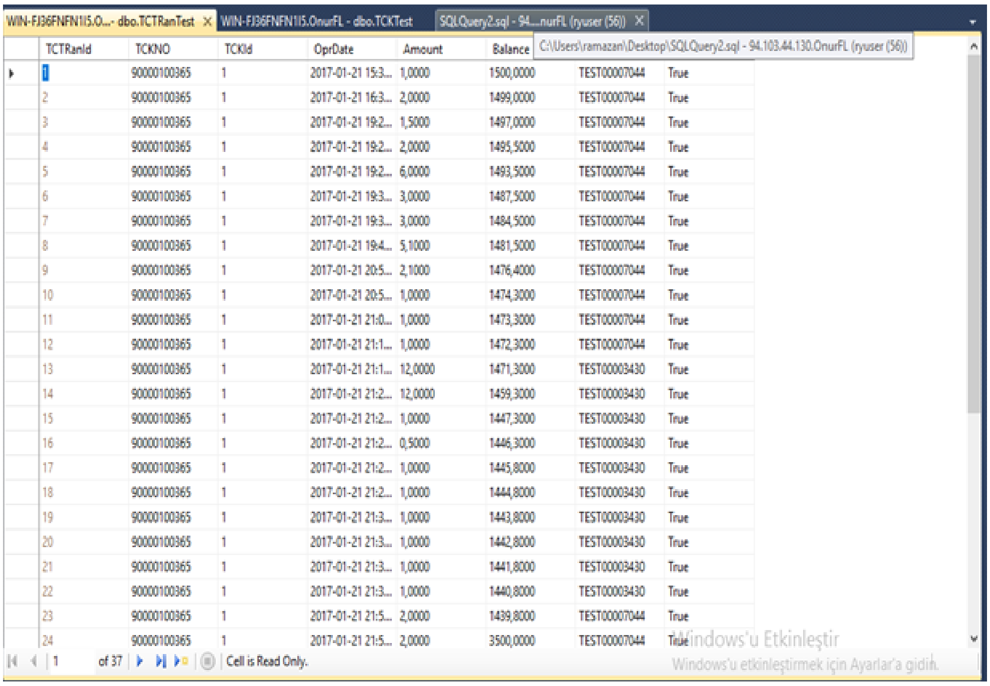


Şekil 7.12: TCKK Satış Detayları

Şekil 7.13' de web sunucudan bakiye bilgileri değiştirilebilir.Şekil 7.14' den de TCKK ile daha önce yapılmış olan işlemler TCKK Seri Numarası, TCKK Numarası, işlem yapılan cihazın seri numarasına göre yapılan satışlar ve kalan bakiye miktarları görülebilir.



Şekil 7.13: Web Sunucu TCKK Bakiye Kontrol Ekranı



Şekil 7.14: TCKK İşlemleri Detay Ekranı

Bölüm 8

TCKK'nın ÖKC İle Kullanımında Tamamlanması Gereken İdari Süreçler

3100 sayılı Kanunun 10 uncu maddesinde "Maliye Bakanlığı, ödeme kaydedici cihazların kullanılmalarıyla ilgili olarak, bu Kanunla belli edilen hususlar dışında uyulması gereken usul ve esasları belirlemeye ve bunlarda değişiklik yapmaya yetkilidir "[18]hükmü yer almaktadır 5490 sayılı kanunun 41 inci maddesinde "Kimlik kartında yer alacak bilgiler ile kartın tasarımı, temini, basımı, dağıtım ve teslim yöntemi ile üretim ve kişiselleştirilmesinde kullanılacak sistemi belirlemeye İçişleri Bakanlığı yetkilidir" [19].

Yukarıdaki Kanunların Maddeleri çerçevesinde ilgili iki bakanlığın bu entegrasyon için ortak bir tebliğ yayınlaması gerekmektedir. Bakanlıklar gerekli gördükleri zamanlarda paydaşlara bildirmek şartı ile teknik kılavuzlarda ve tebliğlerde değişiklik yapabilme hakkına sahip olmalıdır. Yayınlanan teknik kılavuzlar ve tebliğlere uyumluluk sağlayan bankalar, onay için bakanlığa veya bakanlığın belirlediği üçüncü bir otoriteye entegre edilmiş uygulamayı teslim etmeli ve teknik ve idari yeterlilik onayı almalıdırlar. Üçüncü otorite tarafından Ödeme kaydedici cihazlar ile entegre edilmiş olan uygulamalarında teknik kılavuzlarda ve tebliğlerde belirtilen şartlar aranmalı, şartları sağlamayan cihazlara onay verilmemelidir.

Yeni nesil ödeme kaydedici cihazların, öngörülen amaca uygun olarak kullanılmasının sağlanması bakımından, ödeme kaydedici cihaz firmaları, satış ve bakım onarım servisleri aracılığıyla gerekli tedbirleri almalıdırlar.

Yeni nesil ödeme kaydedici cihazlar, Maliye Bakanlığı ve İçişleri Bakanlığının belirlediği kıstaslara göre ilgili kimlik kartının limit bilgilerini, harcama bilgilerini anlık ya da dönemsel olarak elektronik yolla, belirlen Bilgi İşlem Merkezlerine göndermelidir.

Türkiye Cumhuriyeti kimlik kartlarının Yeni Nesil Ödeme Kaydedici Cihaz' larda kullanılmasına ilişkin kademeli bir geçiş öngörülmektedir. Bu geçiş için kurumların tamamlaması gereken idari ve mevzuatsal süreçler bulunmaktadır.

8.1 İlgili Bakanlıklar Tarafından

- Yasal düzenlemeler yapılmalı
- Yetkili otoritenin belirlenmeli
- İdari ve mevzuatsal süreçleri içeren teknik kılavuzlar, tebliğler yayınlanıp bunlarla ile ilgili standartların oluşturulmalı ve bu standartlara uygunluk kontrolü yapılmalı.
- Projede yer alacak olan paydaşların belirlenmeli, paydaşların görev ve sorumlulukları tanımlanmalı

8.2 Bankalar Tarafından

- Bankalar kendi mevzuat ve yönetmeliklerini gözden geçirerek gerekli düzenlemeleri yapmalıdır.
- Bankalar ve işletmeler verdikleri hizmetlerde iş süreçlerini gözden geçirerek maddi ve manevi kayıplarını ve risklerini öngörerek elektronik kimlik kartları ile yapılacak ödeme işlemlerinde ne tür kimlik doğrulama yöntemlerini kullanacaklarına karar vermelidir.
- Bankalar ve işletmeler elektronik ortamdaki bütün uygulamalarını e-kimliği entegre etmelidir.

- Bankalar ve işletmeler kurumsal alt yapılarını Elektronik Doğrulama ve Ödeme Sistemine geçirmek için yatırım planlarını yapmalıdır.

Bankaların sürekli iş ilişkisi tesisinde gerek yüz yüze gerekse mesafeli kanallarda Chip&PIN yöntemi ile kimlik doğrulaması yapabilmesi için MASAK ve NVİ tarafında aşağıda belirtilen mevzuat ve entegrasyon geliştirmelerinin yapılması ve teyidi gerekli olacaktır:

8.3 Mali Suçları Araştırma Kurulu (MASAK) Hususları

Mevcut "Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik" kapsamında bulunan 6. Madde gerçek kişilerde kimlik tespitini düzenlemektedir [4].

8.3.1 Doğum Yeri, Doğum Tarihi, Anne ve Baba Adı, Uyruğu ve Kimlik Belgesinin Türü ve Numarasına İlişkin Bilgilerin Alınması

İlgili madde 6-(2) içinde "İlgilinin adı, soyadı, doğum yeri ve tarihi, anne ve baba adı, uyruğu ve kimlik belgesinin türü ve numarasına ilişkin bilgilerin doğruluğu; a) Türk uyruklular için T.C. nüfus cüzdanı, T.C. sürücü belgesi veya pasaport üzerinden teyit edilir." ifadesi bulunmaktadır [4].

Chip&PIN yöntemi ile e-Kimlik kartları üzerinden elde edilecek verilerin TCKN, Ad, Soyad ile kısıtlı olmasından dolayı bu doğrulama ihtiyacının e-Kimlik kartları için revize edilmesi ihtiyacı bulunmaktadır. E-Kimlik kartları üzerinden Chip&PIN doğrulaması, doğrulanan TCKN için alınan veriler arasında bulunmayan "doğum yeri, doğum tarihi, anne adı, baba adı, uyruğu ve kimlik belgesinin türü ve numarasına ilişkin bilgilerin doğrululuğu" Kimlik Paylaşım Sistemi (KPS) üzerinden gerçek zamanlı olarak doğrulanabildiğinden, bu bilgilerin doğrudan e-kimlik kartları üzerinden doğrulanma zorunluluğunun kaldırılması uygun olacaktır [4].

8.3.2 İmza Örneğinin Alınması

İlgili madde 6-(1) içinde "Gerçek kişilerin kimlik tespitinde; ilgilinin adı, soyadı, doğum yeri ve tarihi, uyruğu, kimlik belgesinin türü ve numarası, adresi ve imza örneği, varsa telefon numarası, faks numarası, elektronik posta adresi, iş ve mesleğine ilişkin bilgiler ile Türk vatandaşları için bu bilgilere ilave olarak anne, baba adı ve T.C. kimlik numarası alınır." İfadesi bulunmaktadır [4].

Internet Bankacılığı, Mobil Bankacılık gibi mesafeli kanallar açısından düşünüldüğünde, gerek imza örneği alımının mümkün olmaması, gerek Chip&PIN yöntemi ile e-Kimlik kartları üzerinden elde edilecek verilerin TCKN, Ad, Soyad ile kısıtlı olması, gerekse de müşterilerin onay işlemlerini imza yerine Chip&PIN ile yapıyor olmalarından dolayı, ilgili madde içerisinde bulunan "imza örneği alınır" ifadesinin e-Kimlik kartları için uygulanmamasının uygunluğu değerlendirilmelidir [4].

8.3.3 Kimlik Belgelerinin Fotokopi veya Elektronik Görüntüsünün Alınması

İlgili madde 6-(2) içinde "Yetkililerce istenildiğinde sunulmak üzere teyide esas kimlik belgelerinin asıllarının veya noterce onaylanmış suretlerinin ibrazı sonrası okunabilir fotokopisi veya elektronik görüntüsü alınır yahut kimliğe ilişkin bilgiler kaydedilir." İfadesi bulunmaktadır [4].

Internet Bankacılığı, Mobil Bankacılık gibi mesafeli kanallar açısından düşünüldüğünde e-Kimlik kartlarının elektronik olarak görsel görüntüsünün veya fotokopisinin alınması pratik olarak mümkün değildir. Ancak e-Kimlik kartları üzerinde geçekleştirilen işlemlerin Chip&PIN yöntemi ile doğrulanabilmesi ile elektronik olarak imzalanarak loglanabilmesi mümkündür. Bu açıdan yukarıda sayılan "yahut kimliğe ilişkin bilgiler kaydedilir" ifadesinin bu loglama yöntemi ile karşılandığı düşünülmekte ve teyide ihtiyaç duyulmaktadır [4].

8.4 Nüfus ve Vatandaşlık İdaresi (NVİ) Tarafından

E-Kimlik kartlarının doğrulanması için gerekli Elektronik Kimlik Doğrulama Sistemi (EKDS) entegrasyonlarını sunacak olan Nüfus ve Vatandaşlık İdaresi (NVİ) tarafından aşağıdaki hususların teyit edilmesi gerekmektedir [4].

- Kimlik tespitinin 2-faktörlü doğrulamasının önemli bir unsuru olan kart sertifikası doğrulama hizmetlerinin online olarak tüm bankacılık sektörünün kullanımına sunulacağının teyidine ihtiyaç duyulmaktadır.

- E-kimlik yongaları içerisindeki bilgilerin okunması ve/veya kaydedilmesi yetkisinin verileceği sektörler ya da roller değişiklik göstermektedir. Bankacılık sektörü için yonga üzerindeki bilgilerden hangilerine ne kadar yetki verileceğinin netleştirilmesine ihtiyaç duyulmaktadır.

- E-kimlik üzerindeki sayısal yüz resmi ve ıslak imza örneği bilgilerine bankaların "müşterini tanı" tedbirleri kapsamında Chip&PIN yöntemi dâhilinde erişilebilir ve kaydedilebilir olmasına ihtiyaç duyulmaktadır.

- Mevcutta Kimlik Paylaşım Sistemi'nden alınan bilgiler ile ileride e-Kimliğin yongasından alınabilecek olan bilgilerin ne ölçüde örtüştüğünün netleştirilmesine ihtiyaç duyulmaktadır

- Mevcut kimliklerde yer alan seri/sıra no bilgilerinin e-Kimlik üzerinde yer alıp almayacağı, yer almazsa bile bu bilgilerin KPS veritabanında yer alıp almayacağı konusunun netleştirilmesine, söz konusu bilgilerin e-kimlik kartında veya KPS' de bulunması durumunda, bu bilgilerin bankalar tarafından teyit ve kontrol amacıyla kullanılabilmesine imkân tanınmasına ihtiyaç bulunulmaktadır.

- E-kimlikte nüfus cüzdanlarına göre yeni/ek bilgilerin olup olmayacağının teyidine ihtiyaç duyulmaktadır.

- E-Kimlikler üzerindeki seri/sıra no algoritması benzer yapıda mı yoksa farklı bir yapıda mı olacaktır teyit edilmelidir. Şayet yapısal farklılıklar olacak ise geçiş döneminde KPS uygulaması açısından hem Nüfus Cüzdanındaki Seri / Sıra No hem de yeni çipli kimlikteki Seri / Sıra No' yu sorgulayabilecek ikili yapı olacak mıdır teyit edilmelidir.

- E-Kimlik yongaları üzerindeki kimlik bilgilerinin (PIN de dâhil olmak üzere) daha sonradan fiziki veya mesafeli kanallar ile ve hangi yetkili kurum ve arayüzler üzerinden güncellenip güncellenmeyeceğinin netleştirilmesine ihtiyaç duyulmaktadır

- Belirli bir süre boyunca vatandaşların hem mevcut kimliği hem de yeni kimlikleri geçerli olmaya devam edecek midir netleştirilmelidir. Geçiş sürecine yönelik planlama (pilot iller, pilot süresi, yaygınlaşmanın başlayacağı iller ve tarihler gibi) netleşmiş ve paylaşılması gerekmektedir [4].

Bölüm 9

Çözümün Endüstride Uygulanma Fizibilitesi

Yeni Nesil Ödeme Kaydedici Cihazlar' da mevcut durumda çalışan banka yazılımları, ÖKC mali yazılımından ayrı, 3.Parti bir yazılım olarak çalışmaktadır. Dolayısıyla Kimlik Kartları ile entegre çalışacak ödeme uygulamaları, ÖKC mali yazılımların değiştirmeden TSM' ler üzerinden mevcut banka yazılımları güncellenerek veya güncellenen banka yazılımlarını ÖKC üretici firmalara teslim elden ederek çözülebilir. Cihazlara banka uygulaması gibi 3. Parti uygulamaları yükleme işlemi ise Ödeme Kaydedici Cihaz üreten firmalar aracılığıyla güvenli odalarda veya TSM' ler üzerinden güvenli kanallarla yapılmaktadır.

Güvenli Oda, Yeni Nesil ÖKC' lere PIN güvenlik kuralları ile anahtar ve sertifika yükleme yapılacak olan ve kural koyucular ile TÜBİTAK tarafından denetlenen güvenlik seviyesi belirlenmiş özel yerlerdir. Bu entegrasyonlar ile güvenli odaların kurulması, denetimi ve yönetimi daha da önemli hale gelmektedir. Anahtar ve sertifika yüklemesi yapılacak olan güvenli odaların, TÜBİTAK Güvenli Oda Kriterlerine ve bankacılık sektörüne özel anahtarlar da yüklenecek ise "PCI – PIN Security Requirements" dokümanın ilgili bölümlerinde yer alan kriterlere uygun olması zorunludur [20]. Güvenli Odaların denetimi yılda bir kere yaptırılarak, denetimlerinin belgeleri ÖKC Üreticisi tarafından GİB' e ve İçişleri Bakanlığının yetkili olarak gördüğü bir otoriteye teslim edilir. Güvenli Oda yönetimi ve sorumluluğu tamamen ÖKC üreticisindedir. Bu entegrasyonun saha da uygulanabilir olması için aşağıdaki hususlara dikkat edilmelidir.

9.1 TSM Merkezleri İle İlgili Dikkat Edilecek Hususlar

ÖKC' ler üzerinde çalışan tüm uygulamalar ÖKC TSM Merkezi üzerinden ÖKC' lere bağlanmaktadır. Yeni Nesil ÖKC ile birlikte çalışacak bankacılık uygulamaları ve bunlara ilişkin parametre, anahtar yazılım yükleme ve ihtiyaç duyulan diğer işlemleri yerine getirmek için taleplerini ÖKC TSM Merkezleri'ne bildirmektedirler. Bu işlemler ÖKC TSM Merkezleri aracılığıyla gerçekleşleşmektedir. ÖKC' lerde oluşabilecek sorunlardan (sahada yaşanacak cihaz ya da tüm uygulamalardaki manipülasyonlar, alınan ödeme ile kesilen mali fiş mutabakatsızlıkları, fonksiyonel arızalar, usulsüz banka/sadakat uygulama anahtar yüklemeleri, saha operasyonel sıkıntıları vb.) ÖKC üreticileri sorumlu olmalıdır [20].

ÖKC TSM Merkezleri, ÖKC' leri yönetme, ayakta tutma, her işlemde cihazdan gelen mesaj bilgilerinin format ve doğruluğunu değerlendirme, bu mesaj bilgilerinin içerisindeki hassas mali verilerin kaynağını, doğruluğunu, değişmezliğini ve bütünlüğünü kontrol etmekle yükümlüdür. Bu kontrol işlemi sırasında NVİ' ye ait hassas verilerin ÖKC TSM Merkezi tarafından açılmaması ve saklanmaması gerekmektedir. Bu konuda sorumluluk ÖKC Üretici firmalarındadır. Ayrıca NVİ, TCKK ile Ödeme Kaydedici Cihazlar üzerinden yapılan tüm işlemler depolamak ve yedek olarak saklamak isteyebilir. Yeni Nesil ÖKC' lerin sahada bulunduğu süre içerisinde belirlenen kurallar dâhilinde tüm saha ve bakım hizmetlerinin sorumlusu ÖKC üreticisidir. Banka uygulamalarının Yeni Nesil ÖKC üzerinde çalışması için sahada yapılması gereken tüm kurulum, servis ve operasyonların sorumlusu ÖKC üreticisidir. ÖKC 'ye bağlı olarak çalışacak olan bütün çevre birimlerinin ve buralarda çalışan yazılımların belirlenen kurallara uygun olarak çalışmasına yönelik saha ve servis hizmetlerinin verilmesinin sorumlusu ÖKC üreticisidir. ÖKC TSM Merkezi'nin sistem güvenliğinin oluşturulması, gerçeklenmesi, bakımının yaptırılması ve sürekli geliştirilmesi için ISO 27001 sertifikasını alması gerekmektedir. Sistemin iş sürekliliğini ve felaketten kurtarma gereksinimlerinin standardizasyonunu sağlamak için ISO 22301 sertifikalarının alınması işlemi ÖKC Üretici firmalar tarafından yapılmalıdır. ÖKC TSM Merkezi, bünyesindeki bilgi sistemleri üzerinde gerçekleştirilen ve ÖKC Mesajlarını yöneten donanım ve yazılımlara ilişkin her türlü bakım, yama ve değişikliğin uygun bir şekilde planlanmasını, yetkilendirilmesini, test edilmesini, gerçekleştirilmesini, belgelendirilmesini ve sonrasında denetlenebilirliğini sağlayacak yazılı ve etkin bir değişiklik yönetimi süreci işletilmelidir. Tutarsızlık ve atak içeren mesajlar ÖKC

TSM Merkezleri tarafından geçersiz mesaj kabul edilecek olup bu mesajlar gerekli araştırmaya tabi tutulmadan ve ÖKC Üreticilerince ÖKC TSM Merkezleri tarafından yapılan mesaj kontrolleri sırasında karşılaşılan tüm tutarsızlıklar ve ataklar raporlanmalıdır.[20].

ÖKC Üretici firmalar, ÖKC TSM Merkezleri' nin sistem güvenliğinde ve sisteminin düzgün işlemesinde önemli ve dikkat edilmesi gereken temel hususları, sistemde var olan ve ifşa olması veya değişikliğe uğraması durumunda sistemin gizliliğini, bütünlüğünü, kaynak/kimlik doğruluğunu ve erişilebilirliğini olumsuz yönde etkileyecek, Yetkili Kullanıcılar(İç personel), Yetkisiz Kullanıcılar(Hacker, Siber Terörist, vb.), Teçhizat ve Yazılımlar, Çevresel Koşullar gibi varlıklarla ilgili riskler belirlenerek, risk analizleri oluşturulmalı ve gerekli önlemler alınmalıdır [20].

ÖKC TSM Merkezleri, NVİ, GİB Yeni Nesil ÖKC Mesajlarının yönetildiği Kimlik Doğrulamanın gerçekleştiği sistemlere ve yazılımlara gerçekleştirilen mantıksal veya fiziksel erişimlere, işlem altyapısını kullanan yetkisiz erişim teşebbüslerine ilişkin etkin bir denetim izi mekanizması tesis edilmelidir. Denetim izi, kullanıcılara sorumluluk atayan, yeterli detay içeren ve şüpheli bir olayı izleme imkânı sunan nitelikte tutulmalıdır [20].

- İşlemi gerçekleştiren uygulama,
- İşlemi gerçekleştiren ve varsa onaylayan kişiler,
- İşlemin açıklaması,
- Yapılan işlemin zaman bilgisi,
- İşlemin olumlu veya olumsuz sonucu,
- Etkilenen veri ve sistemlerin bilgisi [20].

9.2 Kimlik Doğrulama, Şifreleme ve Güvenlik İle İlgili Dikkat Edilecek Hususlar

Kimlik doğrulama ve ödeme alma işleminde kullanılan iletişim altyapısının oturumun başından sonuna kadar güvenliği garanti altına alınmalıdır.

Kimlik doğrulamada kullanılacak şifreleme teknikleri, güncel durum itibariyle literatürde kabul görmüş ve güvenilirliğini yitirmemiş algoritmalar kullanılarak oluşturulmalıdır.

Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanılabileceği zaman zarfında kırılamayacak şekilde uzun seçilmelidir. Geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılması engellenmelidir [21].

Ödeme işlemlerinde Ödeme Kaydedici Cihazlar' da kullanılacak olan kimlik doğrulama tekniklerine yapılacak risk değerlendirmesi sonucuna göre karar verilmelidir. Risk değerlendirmesi, TCKK üzerinden gerçekleştirilmesi planlanan işlemlerin türü (tipi, niteliği, varsa doğuracağı finansal ve finansal olmayan etkilerinin büyüklüğü gibi) dikkate alınırak oluşturulmalıdır.

ÖKC TSM Merkezi GİB Bilgi Sistemleri ve ÖKC ile haberleşmek için kriptografik anahtarlar kullanılması ve bu anahtarların ÖKC TSM Merkezler' inde FIPS 140-2 level 3 ve üzeri sertifikası almış HSM' ler ile saklanması gerekmektedir [30]. Güvenlik denetimi yılda bir kez GİB, NVİ ve ÖKC Üreticisi mutabakatıyla belirlenecek tarihlerde bağımsız firmalar tarafından gerçekleştirilecek sızma testleri ile proje genelinde hedeflenen bilgi güvenliği standardına ulaşılıp ulaşılmadığı sınanmalı, tespit edilen açıklıkların kapatılmasına yönelik tavsiyeler detaylı bir şekilde bu firmalar tarafından NVİ' ye ve GİB Bilgi Sistemleri' ne raporlanmalıdır. PIN güvenlik kuralları ile anahtarın ve başlangıç vektörleri, sayaçlar gibi ilgili diğer güvenlik parametrelerinin oluşturulması, dağıtımı, saklanması, yüklenmesi ve kullanılması, ömrünü tamamlamasının ardından veya güvenliği zedelendiğinde yeni bir anahtar oluşturularak eski anahtarın imhası veya arşivlenmesinin yazılı ve etkin bir biçimde yönetilmesi süreci olan Kriptografik Anahtar Yönetim Süreci ÖKC firmalarının kontrolünde yürütülmelidir [21].

Bu entegrasyon kapsamında yapmış olduğum uygulama da veriler TSM üzerinden gideceği için ÖKC ile TSM arasında SSL güvenli haberleşme alt yapısı ile güvenlik sağlanmaktadır.

9.3 Risk Analizinin Oluşturulması

Bilgi sistemleri ve içerdiği verilerin güvenliği konusunda gerekli kontrollerin ve yapıların oluşturulması çalışmaları kapsamında; risk değerlemesi yapılması, bilgi güvenliği politikası oluşturulması ve uygulanması, bilgi güvenliği testlerinin uygulanması, işlemlerin takip edilip raporlanması ve kontrollerin ve oluşturulan yapıların teknolojik gelişmelere göre güncellenmesi faaliyetlerini içeren bir sürecin yetkili otoriteler (NVİ, GİB vb.)

tarafından oluşturulması gerekmektedir. Bu çerçevede güvenlik ile ilgili hükümlerin gereklerinin yerine getirilmesi hususunda herhangi bir icrai görevi bulunmayan bağımsız ekiplere, düzenli aralıklarla sızma testleri yaptırılmalıdır. Güvenlik alanındaki güncel gelişmeler ve yeni açıklar takip edilmeli, gerekli yazılım güncellemeleri yapılmalı, gerekli yamalar uygulanmalıdır [21].

Bilgi sistemlerine ilişkin risk analizleri, hizmetleri etkileyen önemli güvenlik olayları sonrasında, önemli bir değişiklik öncesinde ve yeni tehditlerin tespiti halinde gözden geçirilmeli ve yılda en az bir defa olmak üzere güncellenmelidir. Mevcut planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa bir günlük operasyonlarının tamamını İkincil Merkez üzerinden gerçekleştirecek şekilde testler yapmalı, test sonuçlarını ve hizmet sürekliliğini etkileyen olayları üst yönetime raporlamalıdır [21].

9.4 Sertifikaların Üretimi, Teslimi, Yeniden Üretilmesi, İptal Edilmesi ve Amacı Dışında Kullanılması İle İlgili Dikkat Edilecek Hususlar

Yetkili otoriteler tarafından, bankaların Türkiye Cumhuriyeti Kimlik Kartları' nı kendi bankacılık sistemlerine entegre etmeleri için kimlik tespitinin 2-faktörlü doğrulamasının önemli bir unsuru olan kart sertifikası doğrulama hizmetlerini, online olarak tüm bankacılık sektörünün kullanımına sunmaları gerekmektedir.

Yeni Nesil ÖKC' lere, ÖKC TSM Merkezlerine ve GİB Bilgi Sistemleri' ne NVİ sunucularına yüklenecek sertifikaların üretimi, dağıtımı ve sonrasında yönetimini ve denetimini gerçekleştirecek kurum (TÜBİTAK Kamu SM) ya da NVİ tarafından yetkilendirilmiş bir sertifika otoritesi olmalıdır.

Yeni Nesil Ödeme Kaydedici Cihazlar 2 türlü Sertifika bulundurmaktadır. Bunlar SAM Kart dediğimiz akıllı kartlarda bulunan sertifikalar ve soft sertifika olarak elektronik ortam da temin edilen sertifikalardır. Güvenilir Sertifika Otoritesi ile anlaşma yapılması, sertifika temini, sertifikaların yüklenmesi, bunun için uygun yapıların kurulması ve işletilmesi sorumluluğu ÖKC üreticisine ait olmalıdır. Bu entegrasyon kapsamında kulanılacak sertifika ile ilgili aşağıdaki hususlara dikkat edilmelidir.

9.4.1 Soft Sertifika Üretimi ve Elektronik Ortamda Teslimi

Cihaz'lar için üretilen sertifikalar, akıllı kartlara yüklenmediği durumda pfx (PKCS#12) formatında üretilmektedir. Her bir cihaz için bir adet pfx dosyası oluşturulmalı ve pfx dosya içeriğinde özel-açık anahtar çifti ve sertifika bulunmalıdır. Pfx dosya adı <Üretici-FirmaKodu><Cihaz SeriNo><Üretici FirmaAdı>_<pfxParola>.pfx şeklinde olmalıdır. Oluşturulan pfx dosyalarının her biri ayrı ayrı Sertifika Yükleme Yetkilisi/Yetkilileri Şifreleme Sertifikası ile şifrelenerek sftp protokolü ile cihaz üreticisine gönderilmelidir. Sertifika Yükleme Yetkilisi/Yetkilileri, cihaz sertifikalarını cihaza yüklemeden önce şifreli olan pfx dosyasının şifresini çözecek ve sonra pfx dosyasını cihaz'a yüklemelidir. Pfx dosyalarının her biri, ilgili Sertifika Yükleme Yetkilisi'nin/Yetkilileri'nin şifreleme sertifikası kullanılarak RFC 3852'de belirtilen CMS Envelope formatında şifrelenmelidir. Şifreli dosyaların şifresinin çözülebilmesi için cihaz üreticilerine ücretsiz yazılım ve/veya API, Sertifika Otoritesi tarafından sağlamalıdır [22].

9.4.2 Akıllı Kartta Üretim ve Teslim

Cihaz'lar için üretilen sertifikalar akıllı kartlara yüklendikten sonra, akıllı kartlar ilgili üretici firmaya kurye aracılığıyla teslim edilmelidir.

ÖKC' lerin NVİ Kimlik Doğrulama Sunucuları bağlanmasında aktarılacak verilerin güvenliğinin sağlanması ve veriyi üreten/gönderen ÖKC' nin NVİ sunucuları tarafından tanınabilmesi amaçları ile şifreleme işlemi için şifreleme açık (PNVİ) ve şifreleme özel (SÖKC) anahtarlarını içeren iki adet sertifikanın ÖKC üreticisi tarafından güvenli odada yüklenmesi gerekmektedir. Saha da bulunan bütün cihazların bu işlemler için toplatılıp güvenli oda da sertifika yükleme işlemi maliyetli olacağı düşünülüyorsa bu işlem yerine bir defa ya mahsus olarak Trusted Service Manager (TSM) dediğimiz güvenli servisler aracılığıyla uzaktan yükleme işlemi yapılabilir [22].

NVİ' e ait şifreleme açık anahtarı (PNVİ),bu entegrasyon kapsamında kullanılaca Ödeme Kaydedici Cihaz' ların ilk kayıt işleminde kullanılmaktadır. Doğrulama amacı ile kullanılacak olan simetrik master anahtarın (TRMK) NVİ' e iletilmesi esnasında, TRMK anahtarını şifrelemek amacıyla kullanılmaktadır. ÖKC 'ye ait şifreleme özel anahtarı (SÖKC) ise, ÖKC tarafından oluşturulan verilerin imzalanması amacı ile kullanılmaktadır [22].

9.4.3 Aynı Cihaz İçin Yeniden Sertifika Üretilmesi

Cihaz sertifikasının silinmesi/bozulması gibi sertifikanın kullanılamaz hale geldiği durumlarda Cihaz'a yeni bir sertifikanın yüklenmesi gerekmektedir. Sertifikanın akıllı karta yüklü olarak verildiği bir cihaza yeni bir sertifikanın yüklenmesi söz konusu olduğunda, yetkili otorite tarafından cihaz için yeni bir sertifika üretilmeli ve yeni bir akıllı karta yüklenerek üretici firmaya kurye ile gönderilmelidir. Sertifikanın soft olarak yüklendiği bir cihaza sertifikanın yeniden yüklenmesi söz konusu olduğunda ise cihaz için yeni bir sertifika üretilmeli ve üretici firmaya sftp ortamında iletilmelidir. Soft ya da akıllı karta basılı olarak cihaz üretici firmaya ulaştırılan yeni sertifika cihaza güvenli alanda yüklenmelidir. Sertifika, güvenli alan dışında cihaza yüklenmemelidir [22].

9.4.4 Sertifikaların İptal Edilmesi

Cihaz'lar için üretilecek sertifikanın geçerlilik süresi cihazın geçerlilik süresi ile aynı olmalıdır. Fakat bir mükellefin ticari faaliyetlerini sonlandırması, cihazın tamir edilemeyecek şekilde arızalanması, sertifikanın herhangi bir sebepten ötürü silinmesi ya da kullanılamayacak hale gelmesi, sertifikanın güvenilirliğinin yitirilmesi gibi durumlarda sertifikanın kötüye kullanılmasının engellenmesi için ivedi olarak iptal edilmesi gerekmektedir. Cihaz sertifikasının iptal edilmesi gerektiği durumlarda, bu cihazın seri numarasını, GİB ve NVİ' ye ya da üretici firma tarafından Sertifika Otoritesine bildirilmeli ve sertifika derhal iptal edilmelidir. Böylelikle bu sertifika, sertifika iptal listesine girecektir ve bilinçli veya bilinçsiz olarak kötüye kullanımın önüne geçilecektir. Sertifika Otoritesine bildirim, e-imzalı olabileceği gibi sağlanacak bir arayüzle de gerçekleştirilebilmelidir. Bu bildirimlerde gerekli kimlik doğrulama işlemleri yapıldıktan sonra sertifika iptal edilmelidir [22].

9.4.5 Sertifikaların Amacı Dışında Kullanılması

Üreticilere teslim edilen sertifikaların amacı dışında kullanılması durumunda oluşacak olumsuz duruma neden olan kişi veya kurumun tespit edilebilmesi amacıyla Sertifika Otoritesi ve NVİ sertifikalara ait kayıtları tutulmalıdır. Gerektiği durumda bu bilgileri bakanlıklara ve adli kurumlarla paylaşmalıdır. Cihaz üreticileri, aldıkları sertifikaların güvenli olarak kullanılmasından sorumlu olmalıdır [22].

Bölüm 10

Sonuç ve Gelecek Çalışmalar

Bu çalışma kapsamında Türkiye Cumhuriyeti Kimlik Kartları ile IP Tabanlı Yeni Nesil Ödeme Kaydedici Cihazlarının entegrasyonu için çözüm sunulmuş, prototip seviyesinde uygulama geliştirilmesi yapılmış ve çalışırlılığı doğrulanmıştır.

Ödeme işlemlerinde tüm dünyada nakit ödeme işlemlerinden, nakit olmayan ödeme işlemlerine doğru bir yönelim olmaktadır. Bu durumun en önemli sebepleri, nakit olmayan ödeme işlemlerinin hizmeti alan ve hizmet veren için kullanım kolaylığının olması, gelişen teknolojinin bu konuda ödeme alternatifleri sunması, en önemlisi artan tüketici ihtiyaçlarını karşılamak amacıyla her kurumun kullandığı sisteme uyum sağlayabilecek pratik ödeme araçlarının gerekliliğinin ortaya çıkmasıdır.

Dünya da birçok ülke elektronik kimliğe geçiş yapmıştır bunlardan birkaçı kimlik kartlarını kısıtlı olarak banka işlemlerinde kullanmaktadır. Örnek verecek olursak; Estonya' da kullanıma geçen kimlik kartı fiziksel kimlik ve elektronik kimlik olarak işlev görecek şekilde oluşturulmuştur. Gömülü bir PKI uygulaması içeren bu Elektronik Kimlik Kartı elektronik sertifikalarla çevrimiçi kimlik doğrulama ve dijital imza sağlamaktadır. Çevrimiçi banka işlemlerine yetki vermek, sözleşmeleri ve vergi beyannamelerini imzalamak, kablosuz ağlara kimlik doğrulaması yapmak, devlet veritabanlarına erişmek, sağlık hizmetlerine erişebilmek için kullanılmaktadır. Portekiz kimlik kartlarının elektronik ortamda kimlik doğrulama, tanıma ve imza atma fonksiyonlarına sahiptir. Elektronik imzadan dolayı birkaç banka ve kamu uygulamalarında sınırlı olarak kullanılmaktadır.Almanya'da 2010 yılında biyometrik veriyi destekleyen kimlik kartının dağıtımına başlanması planlanmış, çevrimiçi e-kimlik ve biyometrik veri kullanımı vatandaşın isteğine bırakılmıştır. Kimlik kartının; elektronik ortamda kimlik doğrulama, elektronik imza atma, seyahatlerde kimlik doğrulama amaçlı olmak üzere 3 temel fonksiyona sahip olması hedeflenmiştir.Avusturya' da ise, kimlik kartı tek bir elektronik kimlik türünün aksine, birçok biçime sahip olabilmektedir. İlk planda hükümet vatandaşlara tek bir kart çıkarmayı planlamasına rağmen daha sonraki süreçte başta alternatif belirteçlerinde (Sağlık sigortası kartları, banka kartları) elektronik tanıma için kullanılmasına izin vermiştir. Örneğin, Mart 2005' ten bu yana, Avusturya bankaları tarafından yayınlanan tüm banka (ATM) kartlarının, Avusturya yasalarına göre bir kimlik kartı olarak kullanımı ve elektronik imza atma yetkileri olmaktadır. Bütün vatandaşlık kartları, kişinin adı ve doğum tarihi de dâhil olmak üzere temel kişisel bilgileri saklamaktadır.

Ülkemiz de bu entegrasyonun diğer ülkelerden en önemli farklarından biri de; bileşenlerinin Kimlik Doğrulama Sunucusu, Kimlik Doğrulama Politika Sunucusu, yüksek güvenlik seviyesinde kimlik doğrulama yapan Kart Erişim Cihazı içeren özgün bir Elektronik Kimlik Doğrulama Sistemi' nin olmasıdır. Bu sistemde; hizmet gerçekleştirilirken hizmete katılan kişilerin ve hizmetten yararlanmak isteyen kişilerin gerçekten öne sürdüğü kişi olduğunu ve kimliği çalan ya da taklit eden başka biri olmadığının doğrulanmasının ardından ödeme işlemine geçiş yapılmaktadır. EKDS' de Sertifika (Açık Anahtar Altyapısı), PIN ve Biyometrik veriler(Parmak izi, avuç izi ve parmak damar izi) ile elektronik kimlik doğrulama yapılmaktadır. EKDS' de vatandaş ile ilgili kayıtlar kurumların kendi sunucularında bilmesi gereken prensibi çerçevesinde tutulduğu için güvenlik ve mahremiyet büyük orada korunmaktadır.

Elektronik Doğrulama Sistemi;

- Kimlik kartının yetkili kurum tarafından verildiğini,
- Vatandaşın kartın sahibi olduğunu ve kimlik doğrulama sırasında hizmet verilen yerde olduğunu,
- Kimlik doğrulama işleminin nerede, ne zaman, kim tarafından ve niçin gerçekleştirildiğini garanti eder.

Bu sistem de; Kimlik doğrulama sonuçlarını Kurum Hizmet Sunucuları için değerlendiren, doğrulayan kimlik doğrulama sonucunda Kimlik doğrulama bildirimini üreten Hizmet alınan kurum adına Kimlik Doğrulama Bildirimi'ni (KDB) doğrulayarak imzalı doğrulama sonucunu (başarılı/ başarısız) Kimlik Doğrulama Başarım Onayı (KDBO) olarak dönen bir kimlik doğrulama sunucusu yer almaktadır. Kimlik doğrulama sırasında kart okuyucu tarafından kullanılacak kimlik doğrulama yöntemi, güvenlik seviyesi, kimlik doğrulama süresi, kimlik doğrulama geçerlilik süreleri gibi parametrelerden oluşan imzalı Kimlik Doğrulama Politikası'nı (KDP) yer almaktadır. Kurumların uygulama veya vatandaş bazlı Kimlik Doğrulama Politikası' nı belirlemesine imkân sağlanmaktadır. Sertifika iptallerini SİL(Sertifika İptal Listesi) yayın periyoduna bağlı kalmaksızın anlık olarak öğrenebilmek için Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP) kullanılmaktadır. Sertifika durum sorgusuna iptal edilip edilmediğini veya iptal edilmiş ise neden ve zamanı detaylı olarak öğrenilmektedir. Böylelikle kimlik geçerliliği güncel olarak sorgulanabilmektedir. Rol doğrulama protokollerini kullanarak rol doğrulama yapan ve TCKK üzerindeki rol doğrulama ile erişilebilen nüfus verilerine erişebilen sunucu bulunmaktadır. Kimlik doğrulama işlemini hizmetin başladığı yerde yapılmasını sağlayan ve sonucu güvenli, yanıltılamaz bir şekilde elektronik olarak Kimlik Doğrulama Sunucusuna bildiren Kart Erişim Cihazları ile Kimlik doğrulama işlemini yapılmaktadır.

Elektronik uygulamalara entegrasyonu sağlayan arabirim yazılımları ile kamu ve özel sektördeki bütün kurumların sistemlerine entegre olma avantajı sunmaktadır. Elektronik Kimlik Doğrulama Sistemi' nin Ödeme işlemi ile entegre olması, kamu kurum ve kuruluşları arasındaki bilgi akışını hızlandırmakta, ihtiyaç duyulan verilere elektronik ortamda ulaşılmasını kolaylaşmakta, yeni teknolojik altyapıya uyumunu sağlanmakta, İşlem zorluklarının yarattığı savurganlık, zaman ve iş gücü kaybını önlenmekte, vatandaşlara kaliteli ve hızlı hizmet verilmektedir.

Elektronik Kimlik Doğrulama Sisteminin içerdiği Kimlik Doğrulama Politika Sunucusu çoklu kimlik doğrulama yöntemlerini desteklediği için ödeme tutarı bazında ve kişi bazında kimlik doğrulama yöntemi belirlenebilmektedir. Aşağıda Elektronik Kimlik Doğrulama Sisteminde kullanılan çoklu kimlik doğrulama yöntemleri verilmektedir.

- Fiziksel Tanıma ve Doğrulama
- Standart Kart Okuyucu İle Kimlik Tanıma
- KEC ile Kimlik Tanıma
- KKEC ve Fotoğraflı Kimlik Tanıma ve Doğrulama

- KEC Üzerinden Biyometrik Veri ile Elektronik Kimlik Doğrulama Tanıma
- KKEC Üzerinden Biometrik Veri ve Fotoğraflı Elektronik Kimlik Doğrulama Tanıma
- Standart Kart Okuyucu ve PIN ile Elektronik Kimlik Doğrulama Tanıma
- KEC ve PIN ile Elektronik Kimlik Doğrulama ve Tanıma
- KKEC ile PIN ve Fotoğraflı Elektronik Kimlik Doğrulama ve Tanıma
- KEC, Biyometrik Veri ve PIN ile Elektronik Kimlik Doğrulama ve Tanıma
- KKEC, Biyometrik Veri, PIN ve Fotoğrafla Elektronik Kimlik Doğrulama ve Tanıma

Kimlik Kartları' nı bankacılık işlemleri içinde kullanılan Nijerya' da ise; elektronik kimlik kartları tamamen MasterCard sunduğu ödeme teknolojisi ile geliştirilmiştir. Kimlik kartlarının oluşumunda tamamen Mastercard' ın bilgi birikimi ve rehberliği kullanılmıştır. Programın mülkiyeti, kontrolü ve vatandaşlarının bilgileri ne derece devlet kontrolünde olduğu tam olarak bilinmemektedir. Ulusal Kimlik Kartında MasterCard logosunun olması özgün ve milli bir nitelik taşımamaktadır. Şekil 10.1' de MasterCard logolu Nijerya Kimlik Kartı' nın ön ve arka yüzü görünmektedir.

Şekil 10.1: MasterCard Logolu Nijerya Kimlik Kartı

Ülkemiz de ise Uluslararası standartlar, uyumluluk esasları ve güvenlik kriterlerine sahip olarak TÜBİTAK tarafından geliştirilen milli işletim sisteminin kullanıldığı kimlik kartı, bu özelliğiyle milli bir güvenliği de beraberinde getirmektedir. Kimlik bilgilerimizin hem ulusal hem de uluslararası seviyede güvenliğini sağlamak amacına hizmet eden milli işletim sistemi, uluslararası tüm güvenlik testlerinden başarıyla geçmesi ile ödeme işlemleri için de kullanıma uygun olduğunu ispatlamıştır. Vatandaşların ihtiyaçlarını karşılayacak, kolay taşınabilir, taklit, tahrif ve sahteciliğe imkân vermeyen, biyometrik unsurlar da içeren, kredi kartı boyutlarında tasarlanan TCKK' nın vatandaşlarımıza hizmet vermesi için gereken sistemler Türk Mühendisleri tarafından geliştirilmiştir. Bunun yanı sıra sistem güvenliği TÜBİTAK tarafından yapılandırılmıştır. Ülkemizin önde gelen grafik tasarımcılarının çalışmaları ve Merkez Bankası Banknot Matbaası'nın katkılarıyla tasarlanan kimlik kartı görsellerimiz, ülkemizin ulusal, kültürel ve tarihi ortak değerlerini içeren unsurlarla harmanlayan bir anlayışla seçilmiştir. Selçuklu çizgilerinden, Osmanlı motiflerine ve Cumhuriyetimizin modern çizgilerine sahip çıkılarak oluşturulan grafikler, banknot basımında kullanılan tekniklerle birleştirilerek kimlik kartına uygulanmıştır. Uluslararası kamuoyunda ülkemizin kabul görmüş rengi olarak Turkuaz rengi tercih edilmiştir [29]

Gerçekleştirilen sistem ile ödeme işlemleri Elektronik Kimlik Kartı üzerinden tek bir sisteme alınarak maliyeti azaltılmış, kullanımı kolaylaştırılıp daha güvenli ve sağlıklı yapılması sağlanmıştır. Sistem geliştirilmeye ve üzerine yeni modüller eklenmeye açıktır. Tasarlanarak geliştirilen sistemin bir model teşkil etmektedir. Geliştirilmesi devam etmekte olan bu entegrasyon çalışmasının sonraki versiyonlarında eklenecek özelliklerle beraber daha kapsamlı kullanılması amaçlanmaktadır. Bu hedef doğrultusunda aşağıdaki özelliklerin sisteme entegrasyonu düşünülmektedir.

- ÖKC' ler mevcut durumda biyometrik veri alma ve o veri ile doğrulama yapmak için gerekli donanımsal ve yazılımsal altyapıyı sunmaktadır. TCKK, vatandaşa ait nüfus, fotoğraf ve parmak izi bilgilerini temaslı yonga üzerinde güvenli bir şekilde sakladığı için ödeme işlemleri biyometrik veriler ile gerçekleştirilmesi sağlanabilir.
- Kimlik kartındaki temaslı yonga, kart sahibine ait nitelikli elektronik sertifikanın (NES) yüklenebilmesine olanak sağlamaktadır. Kişi kartına yüklettiği elektronik imza sertifikası ile sahip olduğu elektronik imza fonksiyonu sayesinde elektronik ortamda gerçekleştirilen işlemlerde ıslak imza gibi birebir olarak hukuksal bağlayıcılığı olan elektronik imzasını da atabilmektedir. Böylelikle vatandaşların, başka bir akıllı kart olmaksızın, elektronik ortamlarda ıslak imza ile eşdeğer olan nitelikli elektronik imzanın atılmasını sağlandığı için büyük miktarda ödeme işlemleri be para transferleri gerçekleştirilebilir
- Elektronik İmzayı kullanarak Yeni Nesil Ödeme Kaydedici Cihazlarda mevcut olan sanal pos işlemleri ile online olarak para transferi ve alışverişi yapılabilir.

- Elektronik Kimlik Kartının sahip olduğu temassız okuma (RFID) özelliğinin kullanılmasıyla İETT ile entegrasyonu yapılıp vatandaşların, kiosklar da, İnternette veya cep telefonundan bakiye yükleme işlemi ile İstanbul Kart olarak kullanılabilir.

Kaynaklar

[1] A.Kubilay and O.Adalıer and A.Karademir UEKAE Dergisi:Türkiye'nin E-Kimlik Yolculuğu cilt:2 sayi:4 Eylül-Aralik 2010

[2] EGM Emniyet Genel Müdürlüğü Hizmet İçi Eğitime Yönelik Çalışma Kitabı, s. 16

[3] A. Arslan Dikkat! ATM'lerde hesabınız boşaltılmasın,2010 URL http://www.finansgundem.com/haber/dikkat-atmlerde-hesabiniz-bosaltilmasin/276045.

[4] TBB. T. Bankalar Birliği Genel Sekreterliği E-kimlik yaklaşımı ve netleştirilmesi gereken hususlar (Alt çalışma grubu raporu) Mart 2015)

[5] D. Castro Explaining Internatioal IT Application Leadership: Electronic Identification Daniel Cast ro September 2011

[6] Gemalto security to be free Estonian eID card: Putting the E in Estonia April 2016 URL http://www.gemalto.com/govt/customer-cases/estonia-eid.

[7] A. Poller, U. Waldmann, S. Vowé, and S. Türpe. Fraunhofer Institute for Secure Information Technology Electronic Identity Cards for User Authentication—Promise and Practice In *Security and Privacy, January/February 2012 IEEE Symposium on*, IEEE, 1987.

[8] H. Leitold and R. Posch, Common Criteria in Austria – Overview of Experiences, 6th ICCC 2005 Tokio September 28, 2005, URL http://www.a-site.at/pdfs/20050928_CC-in-Austria-Web.pdf.

[9] Secure Information Technology Center - Austria "Citizen Cards – Data Protection and Security" Buergerkarte.at. n.d. 2006 URL http://www.buergerkarte.at/sicherheit-datenschutz.de.php.

[10] S. Arora, "National e-ID card schemes: A European overview," Information Security Technical Report 13 (2008) 50.

[11] F. Maes, Belgium Country Update, Presentation at Porvoo Group 16 (March 2010).

[12] Gemalto. The new Nigerian national eID program Gemalto: an ambitious initiative gemalto URL `http://www.gemalto.com/govt/customer-cases/nigeria-eid`.

[13] O. Adalıer and M. Selvi Türkiye Cumhuriyeti Kimlik Karti.2016 URL `www.ekds.gov.tr`.

[14] BDDK. Banka Kartları ve Kredi Kartları Kanunu, Kanun Numarası :5464 Kabul Tarihi :23/2/2006 Yayımlandığı R.Gazete : Tarih: 1/3/2006 Sayı : 26095 Yayımlandığı Düstur : Tertip : 5 Cilt : 45)

[15] GİB. Yeni Nesil Ödeme Kaydedici Cihazlar Teknik Kılavuzu TK-1 Sürüm 4.00 ,20 EKİM 2016 URL `http://www.gib.gov.tr/fileadmin/duyurular/YNOKC2.pdf`.

[16] GİB. Gelir İdaresi Başkanlığı Mesaj Protokolü Spesifikasyonları 1 Sürüm 4.00, 18MAYIS 2015

[17] W. Rankl and W. Effing, Smart Card Handbook,1997 URL `https://imcs.dvfu.ru/lib.int/docs/Hardware/Smart%20Card%20Handbook.pdf`.

[18] T.C Maliye Bakanalığı Katma Değer Vergisi Mükelleflerinin Ödeme Kaydedici Cihazları Kullanmaları Mecburiyeti Hakkında Kanun (1) Kanun Numarası: 3100 Kabul Tarihi: 6/12/1984 Yayımlandığı R. Gazete: Tarih: 15/12/1984 Sayı: 18606 Yayımlandığı Düstur: Tertip: 5 Cilt: 24 Sayfa: 130) URL `https://www.tbmm.gov.tr/tutanaklar/KANUNLAR_KARARLAR/kanuntbmmc072/kanuntbmmc072/kanuntbmmc07203482.pdf`.

[19] NVİ, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü. NÜFUS HİZMETLERİ KANUNU Kanun Numarası: 5490 Kabul Tarihi: 25/4/2006 Yayımlandığı R.Gazete: Tarih: 29/4/2006 Sayı: 26153 Yayımlandığı Düstur: Tertip: 5 Cilt: 45) URL `https://www.tbmm.gov.tr/tutanaklar/KANUNLAR_KARARLAR/kanuntbmmc072/kanuntbmmc072/kanuntbmmc07203482.pdf`.

[20] GİB. Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezi Teknik Kılavuzu Sürüm 2.0, 23 Eylül 2016

[21] BDDK. Bankacılık Düzenleme ve Denetleme Kurumu, Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere ilişkin Tebliğ URL https://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/9491ilkelerteblig.pdf.

[22] TUBİTAK Yeni Nesil ÖKC Sayısal Sertifika Yaşam Döngüsü TUBİTAK BİLGEM 01 TEMMUZ 2015 URL http://www.kamusm.gov.tr/dosyalar/rehberler/REHB-001-012_Yeni_Nesil_OKC%20Sayisal_Sertifika_Yasam_Dongusu.pdf.

[23] BKM Bankalararası Kart Merkezi (BKM) İstatistik verileri Haziran 2016. URL http://bkm.com.tr/secilen-aya-ait-istatistikler/.

[24] BKM Bankalararası Kart Merkezi (BKM) İstatistik verileri Haziran 2015. URL http://bkm.com.tr/secilen-aya-ait-istatistikler/.

[25] M. A. Wright An overview of PKI Network Security, Volume 1999, Issue 9, September 1999, Pages 14-17 URL http://www.sciencedirect.com/science/article/pii/S1353485800800318.

[26] S. J. Murdock, S. Drimmer, R. Anderson, M. Bond , Chip and PIN is Broken , 2010 IEEE Symposium on Security and Privacy. Articles URL https://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf.

[27] M. E. Peters. Emerging eCommerce Credit and Debit Card Protocols IBM Corporation 2002.

[28] E.Büyükkaya Yeni Nesil Ödeme Kaydedici Cihazlarda Güvenlik-1 Elif Büyükkaya TÜBİTAK BİLGEM, TUBİTAK/BİLGEM 18.09.2013 URL https://www.bilgiguvenligi.gov.tr/donanim-guvenligi/yeni-nesil-odeme-kaydedici-cihazlarda-guvenlik-1.html.

[29] NVİ. T.C. İÇİŞLERİ BAKANLIĞI Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü Türkiye Cumhuriyeti Kimlik Karti.Temmuz 2016 URL https://www.nvi.gov.tr/hakkimizda/projeler/tc-kimlik-karti/turkiye-cumhuriyeti-kimlik-karti.

[30] FİPS. FIPS 140-2 Levels Explained Modified on: Thu, 11 Jul, 2013 URL http://support.datalocker.com/support/solutions/articles/104685-fips-140-2-levels-explained.

[31] W. Rankl. Smart Card Applications: Design Models for Using and Programming Smart Cards 2007, URL https://books.google.com.tr/books/about/Smart_Card_Applications.html?id=40dv4nCsCGUC&source=kp_cover&redir_esc=y.

[32] The free encyclopedia Wikipedia. Açık anahtarlı şifreleme, 2015 URL https://tr.wikipedia.org/wiki/A%C3%A7%C4%B1k_anahtarl%C4%B1_%C5%9Fifreleme.