TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLAR İÇİN TÜMLEŞİK VE HİBRİT TSMMODELİNİN GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

Hasan Hüseyin SUBAŞI

Bilgisayar Mühendisliği Anabilim Dalı
Bilgi Güvenliği

Tez Danışmanı: Prof. Dr. Ali Aydın SELÇUK

ARALIK 2016

Fen Bilimleri Enstitüsü Onayı

……..
Prof. Dr. Osman EROĞUL
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

……..….
Doç. Dr. Oğuz ERGİN
Anabilim Dalı Başkan V.

TOBB ETÜ, Fen Bilimleri Enstitüsü'nün 141111045 numaralı Yüksek Lisans Öğrencisi **Hasan Hüseyin SUBAŞI**'nın ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLAR İÇİN TÜMLEŞİK VE HİBRİT TSM MODELİNİN GELİŞTİRİLMESİ"** başlıklı tezi **16 Aralık 2016** tarihinde aşağıda imzaları olan jüri tarafından kabul edilmiştir.

Tez Danışmanı : **Prof. Dr. Ali Aydın SELÇUK** .....
TOBB Ekonomi ve Teknoloji Üniversitesi

Jüri Üyeleri : **Prof. Dr. Bülent TAVLI (Başkan)** .....
TOBB Ekonomi ve Teknoloji Üniversitesi

Prof. Dr. İbrahim KÖRPEOĞLU .....
Bilkent Üniversitesi

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Hasan Hüseyin SUBAŞI

ÖZET

Yüksek Lisans Tezi

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLAR İÇİN
TÜMLEŞİK VE HİBRİT TSM MODELİNİN GELİŞTİRİLMESİ

Hasan Hüseyin SUBAŞI

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Bilgi Güvenliği

Danışman: Prof. Dr. Ali Aydın SELÇUK

Tarih: Aralık 2016

Günümüzde devletler kayıt dışı ekonomi harcamalarını kontrol etmek için çeşitli altyapılar ve teknolojiler geliştirmektedir. Bu bağlamda vergi düzenini sağlayarak güçlü bir devlet olma yönünde çalışılmaktadır.

Yeni Nesil Ödeme Kaydedici Cihazı (YN ÖKC) yazarkasa ile POS (Point Of Sale) cihazının tek bir cihazda birleştirilmiş halidir. Gelir İdaresi Başkanlığı (GİB) kurallarını ve teknik detaylarını yayınladığı bu cihazların, kullanılan tüm yazarkasalar yerine kullanılmasını istemektedir. Geleneksel POS dünyasında POS cihazları sadece bankaya bağlanmaktadır. Yeni Nesil Ödeme Kaydedici cihazları ise önce Trusted Service Manager (TSM) merkezine sonrasında bankacılık işlemleri için bankaya bağlanmaktadır. TSM merkezleri GİB adına işlem kaydını tutarak ilgili kayıtları GİB Bilgi Sistemleri sunucuları ile paylaşmaktadır. Böylelikle satış işlemlerinin online kayıt altına alma altyapısı sağlanmış olmaktadır. Bununla birlikte bankalar POS (Point of Sale) haberleşme dünyasını kendi başlarına yönetmektedirler. Ancak geçmiş teknolojilere bağımlılık ve eski banka sistemlerinden dolayı POS cihazlarında kriptografik anahtarın yönetimi basit yapıdan güçlü ve karmaşık yapıya

kadar farklılık gösterecek nitelikte olabilmektedir. Son yıllarda yapılan uluslararası düzenlemelerde POS cihazlarında güçlü bir anahtar yönetimine geçilmesi tavsiye edilmektedir. İleriki yıllarda bu tavsiyenin zorunluluk haline getirileceği de bilinmektedir.

Bu çalışma, Yeni Nesil Ödeme Kaydedici Cihaz ile Trusted Service Manager merkezlerinin güvenli iletişim altyapısını anlatacaktır ve sonrasında bankacılık uygulamaları için güçlü bir anahtar yönetim altyapısına sahip bir TSM modeli önerecektir. Bu model aynı zamanda GİB tarafından tariflenen her iki TSM çalışma modeline uyacaktır. Çalışmalarda GİB tarafından yayınlanmış teknik kılavuzların yanında uluslararası standartların isterleri de değerlendirilmiştir. Bu çalışmada önerilen sistem ile anahtar yönetimi TSM sistemi içerisinde yapılarak bütün banka yazılımlarının aynı güçlü anahtar yapısını kullanması sağlanmaktadır. Banka ile POS iletişim sisteminde hem iletişim paketinin şifreli hem de paket içerisindeki hassas verilerin ayrı ayrı şifrelenmesi PIN Security standartları kapsamında gerekmektedir. Önerilen model ile terminal ile banka arasında taşınan hassas verilerin şifrelenmesi sağlanmaktadır. Kurulan güçlü anahtar altyapısı ile GİB adına işlem kaydını tutma işlemini yapan TSM merkezlerinin bu taşınan hassas verileri görmemesi de sağlanmaktadır. Bu sayede banka kartları ile yapılan ödemede bankaya taşınan birincil hesap numarası (PAN), PIN vb. hassas verilerin uçtan uca şifreli taşınması sağlanacak ve arada TSM tarafından elde edilmesi önlenecektir. Yani YN ÖKC tarafında şifrelenmiş paketler TSM tarafından açılamadan bankaya taşınacaktır ve sadece banka tarafında açılarak ilgili işlemler gerçeklenecektir.

Anahtar Kelimeler: Finansal kriptografi, Elektronik ödeme sistemleri, Güvenli elektronik bankacılık, ISO 8583

ABSTRACT

Master of Science

DEVELOPMENT OF INTEGRATED AND HYBRID TSM MODEL FOR THE NEW GENERATION CASH REGISTERS

Hasan Hüseyin SUBAŞI

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Computer Engineering Programme
Information Security

Supervisor: Prof. Dr. Ali Aydın SELÇUK

Date: December 2016

Nowadays governments have been developing various infrastructures and technologies in order to control the unregistered economical expenditures. In this context, they have been working on becoming a strong state by means of ensuring better tax adjustments.

The New Generation Electronic Cash Register (NG ECR) is a single machine which is the combination of cash register and point of sale (POS) machines. Revenue Administration of Turkey (GIB) approves the usage of this machine of which they published the rules and technical details instead of using all different types of cash registers. In the traditional POS usage, POS machines only connect to the banks. However, the New Generation Electronic Cash Registers first connect to the Trusted Service Manager (TSM) center afterwards to the banks for banking transactions. TSM centers share the related information with Revenue Administration Information System (GIB-BS) servers while recording the transactions on behalf of GIB. Therefore, the infrastructure of online recording of sale transactions is ensured. With this being ensured, banks operate the POS communication arena on their own. However, management of cryptographic keys have characteristics that differ from

basic structure to strong and complicated structure due to dependence on traditional technologies and previous banking systems. With the recent regulations at an international scale, it is highly recommended to make the transition to a stronger key management. It is a well-known fact that this recommendation will become mandatory in the near future.

This study will examine the secure communication infrastructure of NG ECR and TSM; then, it will recommend a TSM model which has a stronger management key infrastructure for banking services. This model will, at the same time, correspond to both of the TSM working models, which were previously defined by GIB. In addition to the technical instructions published by GIB, the requirements of international standards were also examined in this study in addition to the technical guidelines published by GIB with the system proposed in this study.

Entire communications infrastructure will be supported by the same strong key management structure by doing the key management within the TSM systems through the system examined in this study. In bank and POS communication systems, both encrypted communication packets and sensitive data that is separately encrypted in the packet are necessarily made within PIN security standards. Encryption of sensitive data carried between the terminal and the bank is provided with this recommended model. With the installed powerful key infrastructure, TSM centers which hold the operation records on behalf of GIB are also assured not to see the sensitive data carried. In this way, with the payments done with credit cards, sensitive data such as the primary account number (PAN), PIN, etc. is protected by end-to-end encryption and is protected from being obtained by the TSM in the meantime. In other words, packets encrypted by the NG ECR will be carried to the bank without being seen by the TSM, and relevant transactions will be carried out by decrypting only on the bank's side.

Keywords: Financial cryptography, Electronic payment systems, Secure electronic banking, ISO 8583

TEŞEKKÜR

Çalışmalarım boyunca emeğiyle ve katkılarıyla beni yönlendiren, değerli bilgi birikimini, tecrübesini, zamanını ve her konuda desteğini esirgemeyen değerli hocam Prof. Dr. Ali Aydın SELÇUK'a, kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerine, destekleriyle her zaman yanımda olan arkadaşlarıma ve iş arkadaşlarıma, bankacılık alanında engin tecrübesiyle tezime yaptığı katkılarla vizyonerlik sağlayan Sn. Hasan Murat YAĞCI'ya, tezimi baştan sona okuyarak biçimsel hatalarımı inceleyerek tez basımı süresince yardımını esirgemeyen Sn. Nihat PİŞKİN'e,

Tez jürimde yer almayı kabul ettikleri ve zaman ayırdıkları için Prof. Dr. Bülent TAVLI'ya ve Prof. Dr. İbrahim KÖRPEOĞLU'na,

Öğrenimim süresince her türlü idari desteği sağlayan ve tezimi baştan sonra gözden geçirerek düzenlenmesinde, kaliteli ve düzgün bir çalışmanın çıkmasında emeği bulunan Sn. Ülüfer NAYIR'a,

Öğrenimim süresince ve çalışmamın her anında desteğini esirgemeyen, bu öğrenim sürecini elinden geldiğince benim için kolaylaştırmaya çalışan kıymetli eşim Naciye'ye ve güzel kızım Melike Berrin'e,

Yüksek lisans öğrenimim süresince sağladığı burs ve diğer tüm imkanlar için TOBB Ekonomi ve Teknoloji Üniversitesi'ne çok teşekkür ederim.

İÇİNDEKİLER

Sayfa

ÖZET ..... **iv**
ABSTRACT ..... **v**
TEŞEKKÜR ..... **vi**
İÇİNDEKİLER ..... **vii**
ŞEKİL LİSTESİ ..... **viii**
ÇİZELGE LİSTESİ ..... **ix**
KISALTMALAR ..... **x**
RESİM LİSTESİ ..... **xi**
1. GİRİŞ **1**
1.1 Tezin Amacı 3
1.2 Literatür Araştırması 4
2. YAZARKASA VE POS **7**
2.1 Yazarkasanın Tarihçesi 7
2.1.1 Nakit kayıt öncüsü abaküs 7
2.1.2 Nakit çekmecesi 8
2.1.3 Aldatılmaz kasiyer 8
2.2 Türkiye'de Yazarkasa 12
2.3 Dünyada Kartlı Ödeme Sistemlerin Tarihçesi 13
2.4 Banka Kartı Terminallerinin Tarihçesi 14
2.4.1 Manuel görüntüden yazıcı (Imprinter) 15
2.4.2 Elektronik yetkilendiriciler 15
2.4.3 POS terminaller 15
2.5 PCI PIN Güvenliği Standardı Açısından POS Cihazlarında PIN ve Anahtar Güvenliği 16
2.5.1 Donanımsal güvenlik modülü (HSM) cihazların temini 20
2.5.2 Anahtarların üretilmesi ve güvenli saklanması 21
2.5.3 Anahtarların kullanılması, paylaşılması ve kullanım dışına alınması 23
2.6 Güvenli İşlem Sistemleri ve Metotları 24
3. YENİ NESİL ÖDEME KAYDEDİCİ CİHAZ ve TRUSTED SERVICE MANAGER **29**
3.1 Sistem Mimarisi 30
3.2 Mesaj Yapısı 31
3.3 Yeni Nesil Ödeme Kaydedici Cihaz 32
3.3.1 Mali sertifika 34
3.3.2 Güvenli veri iletimi 35
3.4 Trusted Service Manager (TSM) 35
3.4.1 TK1 TSM 38
3.4.2 TK2 TSM 38
3.4.3 TK1 ile TK2 karşılaştırması 38
3.5 Sertifikalar ve Sertifika Mimarisi 39
3.5.1 Sertifikaların doğrulanması 42
3.6 Gelir İdaresi Başkanlığı Mesajlaşma Protokolü 42

3.7 TSM Güvenlik ve Anahtar Yönetimi 43
3.7.1 Anahtar açıklamaları ve güvenlik gereksinimleri 44
3.7.1.1 Terminal random master key (TRMK) 46
3.7.1.2 Terminal random master key for data (TRMKD) 46
3.7.1.3 Terminal data key (TDK) 46
3.7.1.4 Terminal random encryption key (TREK) 47
3.7.1.5 Terminal random authentication key (TRAK) 47
3.7.1.6 Local master key (LMK) 47
3.8 YN ÖKC, TSM ve GİB BS Online Anahtar Yükleme 48
4. TÜMLEŞİK VE HİBRİT TSM 51
4.1 H-TSM Çalışma Modeli 52
4.2 Finansal Elektronik Sertifika Hizmet Sağlayıcısı 54
4.3 Anahtar Yönetimi 56
4.3.1 İlk kurulumlar 56
4.3.2 PIN anahtar paylaşımları 59
4.3.3 Güvenli finansal işlem 59
4.3.4 Anahtarlar ve kullanım alanları 61
4.3.4.1 Gateway master key (GMK) 61
4.3.4.2 Terminal PIN key (TPK) 61
4.3.4.3 TPK key encryption key (TPKKEK) 61
4.3.4.4 Diğer anahtarlar 61
4.3.5 Sistem için önerilen uzaktan sertifika yükleme/yenileme süreci 62
4.3.5.1 YN ÖKC'ler için önerilen sertifika yükleme ve yenileme süreci 62
4.3.5.2 YN ÖKC'ler için önerilen anahtar üretimi ve sertifikalandırma süreci 64
5. SONUÇ VE ÖNERİLER 67
KAYNAKLAR 71
ÖZGEÇMİŞ 75

ŞEKİL LİSTESİ

Sayfa

Şekil 1.1 : Uygulama mimarisi olarak yeni nesil ödeme kaydedici cihazlar. 4
Şekil 2.1 : Otelde izlenecek prosedürü gösteren akış şeması 11
Şekil 4.1 : YN ÖKC – TSM arasında TSM sertifika yükleme. 57
Şekil 4.2 : TGW – Banka arasında signon mesajları. 58
Şekil 4.3 : YN ÖKC – TGW arasında veri anahtarı paylaşımı. 58
Şekil 4.4 : PIN içeren güvenli finansal işlem. 60
Şekil 4.5 : YN ÖKC için sertifikalandırma akışı. 65

ÇİZELGE LİSTESİ

Sayfa

Çizelge 3.1 : YN ÖKC temel teknik özellikleri tablosu. 33
Çizelge 3.2 : YN ÖKC-TSM paket iletişim genel yapısı. 43
Çizelge 3.3 : TSM-GIB paket iletişim genel yapısı. 43
Çizelge 3.4 : Mali haberleşme sistemi anahtar tablosu. 45
Çizelge 3.5 : Online anahtar yükleme. 49
Çizelge 4.1 : TPK üretimi 59
Çizelge 4.2 : TPKKEK üretimi. 59
Çizelge 4.3 : Güvenli finansal işleminde ilk anahtarlar. 60

KISALTMALAR

AES : Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
ATM : Automated Teller Machine
CBC : Cipher Block Chaining – Bir şifreleme modudur
CC : Common Criteria (Ortak Kriter)
CR : Cash Register (Yazarkasa)
CVM : Card Verification Method
CVV : Card Verification Value
EAL : Evaluation Assuranca Level (Değerlendirme Güvence Seviyesi)
EFT : Elektronik Fon Transferi
EMV : Europay, Mastercard ve VISA kuruluşların kısaltması olan sertifika
GİB : Gelir İdaresi Başkanlığı
GİB BS : Gelir İdaresi Başkanlığı Bilgi Sistemleri
GMP : GİB Mesajlaşma Protokolü
HSM : Hardware Security Module (Donanımsal Güvenlik Modülü)
ISO : International Organization for Standardization
JCB : Japan Credit Bureu
KCV : Key Check Value
LMK : Local Master Key
LRC : Longitudinal Redundancy Check
MAC : Message Authentication Code (Mesaj Kimlik Doğrulama Kodu)
OCSP : Online Certificate Status Protocol
PAN : Primary Account Number (Birincil Hesap Numarası)
PCI : Payment Card Industry
PCI-DSS : Payment Card Industry Data Security Standard
PIN : Personel Identification Number (Kişisel Kimlik Numarası)
POS : Point Of Sale
RSA : River Shamir Addleman Asimetrik Algoritma
SİL : Sertifika İptal Listesi
SSL : Secure Socket Layer
TLV : Tag Length Value
TMK : Terminal Master Key
TPDU : Transport Protocol Data Unit
TPM : Trusted Platform Module
TSM : Trusted Service Manager (Güvenli Servis Sağlayıcı)
VAS : Value Added Services (Katma Değerli Servisler)
ZCMK/ZMK : Zone Control Master Key, Zone Master Key

RESİM LİSTESİ

Sayfa

Resim 2.1 : Ritty'nin yazarkasası 8
Resim 2.2 : Elektronik yazarkasa kullanarak kredi kartı soruşturma sistemi 10
Resim 2.3 : Metal plakalarda ilk özgün kredi kartları 14
Resim 2.4 : MasterCard ağı üzerinde PIN paylaşımı 17
Resim 2.5 : Anahtar sertifikalandırma prosesi 18
Resim 2.6 : Ödeme sistemlerinde jeton işlem mimarisi 26
Resim 3.1 : EFT-POS genel çalışma mimarisi 29
Resim 3.2 : Genel haberleşme topolojisi 31
Resim 3.3 : YN ÖKC teknik mimarisi 32
Resim 3.4 : TSM haberleşme mimarisi 37
Resim 3.5 : Yetkilendirilmiş ESHS sertifika otoritesi yapısı 39
Resim 3.6 : GMP haberleşme mimarisi 42
Resim 3.7 : Anahtar mimarisi 48
Resim 4.1 : H-TSM mimari yapısı 51
Resim 4.2 : H-TSM haberleşme yapısı 52
Resim 4.3 : H-TSM çalışma yapısı 54
Resim 4.4 : Finansal ESHS sertifika otoritesi yapısı 55
Resim 4.5 : Hibrit ESHS sertifika otoritesi yapısı 56
Resim 4.6 : Anahtar üretme ve sertifikalandırma kronolojisi 65
Resim 5.1 : Gelecekteki tahmini TSM mimarisi 68

1. GİRİŞ

Günümüzde vergiler, devletlerin ekonomik olarak ayakta kalmasında en önemli gelir kalemlerinden biri, belki de en önemlisidir. Devletler kayıt dışı ekonomi harcamalarını kontrol etmek için çeşitli altyapılar ve teknolojiler geliştirmektedir. Bu bağlamda vergi düzenini sağlayarak güçlü bir devlet olma yönünde çalışılmaktadır. Ülkemizde hayatımıza giren bu çalışmalardan biri de Yeni Nesil Ödeme Kaydedici Cihazıdır (YN ÖKC).

Bankalar POS (Point of Sale) haberleşme dünyasını kendi başlarına yönetmektedirler. POS üzerinde koşan banka uygulamalarının yüklenmesi, parametrelerin yüklenmesi, gün sonu işlemleri ve anahtar yönetimi bankanın belirlediği kriterlere göre POS üreticileri tarafından gerçeklenmektedir. Ancak geçmiş teknolojilere bağımlılık ve eski banka sistemlerinden dolayı POS kriptografik anahtar yönetimi basit yapıdan güçlü ve karmaşık yapıya kadar farklılık gösterecek nitelikte olabilmektedir.

Ülkemizde yayınlanan düzenlenmiş bir kanunla ve ilgili genel tebliği ile Yeni Nesil Ödeme Kaydedici Cihazların (YN ÖKC) kullanımına ve zorunluluğuna ilişkin kurallar açıklanmıştır. Faaliyetlerinde seyyar POS cihazı kullanan mükelleflerin, kullandıkları bu POS ve yazarkasa yerine dünyada ilk kez birlikte kullanımına imkân veren yeni nesil ödeme kaydedici cihaz kullanma zorunluluğu getirilmiştir [1] ve o tarihten günümüze YN ÖKC kullanımı ülkemizde yaygınlaşmaya devam etmektedir.

YN ÖKC tarafından üretilen ve GİB için istenen bilgilerin iletimi, Gelir İdaresi Başkanlığınca yayınlanan “Yeni Nesil Ödeme Kaydedici Cihazlara ait ÖKC TSM Merkezi Teknik Kılavuzları” [2],[3],[4],[5] ile usul ve esasları belirlenen merkezler aracılığıyla GİB Bilgi Sistemlerine (GİB BS) gönderilecektir. İşte bu noktada hassas verilerin iletimi için kurulacak olan Trusted Service Manager – TSM merkezlerinin barındırdığı güvenli iletişim altyapısı önem arz etmektedir. Ülkemizde Başbakanlık genelgesi olarak yayınlanan, "Kayıt dışı ekonomiyle mücadele stratejisi eylem planı" ile kayıt dışı ekonomi ile mücadelede başarı kazanılması ve kayıt dışılığın azaltılması

için kayıt dışı ekonomi ile mücadelenin devlet politikası olarak benimsenmesi önerilmektedir [6]. Bunun için etkin bir izleme ve değerlendirme sisteminin oluşturulması gerektiği belirtilmektedir [6],[7]. Denetimlerin daha etkin hale getirilmesi ise, mükelleflerin beyanlarının sürekli denetim altında bulundurulması sonucunu ortaya çıkarmıştır. Bu maksatla yayınlanmış kanun ve mevzuatlarla ülkemizde kullanılan ödeme kaydedici cihazlarda yeni bir sistemi hayata geçirerek daha etkin bir biçimde kontrolün sağlanması amaçlanmıştır. Yayınlanan 466 sıra no'lu vergi usul kanunu genel tebliğ ve sonraki tebliğler ile mükelleflerin yeni nesil ödeme kaydedici cihazlara (YN ÖKC) geçiş takvimi planlanmıştır [1].

YN ÖKC'ler, bünyesinde banka POS'u da barındıran bütünleşik yazarkasalardır ve her türlü fiş çıktısını mali uygulamadan bastırarak kayıt altına alan bir cihazdır. Günümüzdeki POS cihazlar doğrudan banka sunucuları ile ISO 8583 [8] finansal mesajlaşma formatı kullanarak haberleşirken, YN ÖKC iletişiminde ise arada Trusted Service Manager (TSM) denilen merkezlerin bulunması zorunlu hale getirilmiş ve yeni nesil ödeme kaydedici cihazların dolaylı olarak bankaya bağlantı kurması yayınlanan mevzuat ve teknik kılavuzlarla tariflenmiştir [2],[3],[4],[5].

Bu çalışmanın ilk bölümünde yazarkasa hakkında bilgiler verilerek tarihsel gelişimi irdelenecektir. İkinci bölümde ise POS dünyasına değinilecek ve mevcut anahtar yönetimi hakkında bilgiler aktarılacaktır. Üçüncü bölümde Yeni Nesil Ödeme Kaydedici Cihazlar ve GİB tarafından belirlenmiş teknik isterler hakkında genel bilgiler aktarılacaktır. Son bölümde ise bu çalışmada önerilen, YN ÖKC ile TSM ve TSM ile banka arasındaki güvenli anahtar yönetimini tarifleyen tümleşik ve hibrit TSM modeli hakkında bilgiler sunulacaktır.

Bankalar, POS cihazlarında banka kartlarının hassas bilgilerini içeren track alanlarını da bankaya taşırlar. Bu alanlarda kart numarası, kart sahibinin adı, son kullanım tarihi, PIN bloğu verisi vb. hassas veriler bulunabilir. Bu alanların POS banka işlemlerinde güvenli olarak taşınması için şifreleme anahtarları kullanılır. PIN ayrı bir anahtar ile şifrelenir ve PIN bloğu olarak track verisi içinde bulunur ve track içinde tekrar şifrelenir. Kullanılan algoritmalar zayıf olduğu bilinen algoritmalardır. (Örneğin double DES, 3DES). POS cihazında çalışan bankacılık uygulamaları her cihazda aynı ve bir anahtarlarla şifreleme yapısı kadar basit şekilde olabildiği gibi cihaz içerisinde farklı olacak anahtar yapısında da çalışabilmektedir. Ancak bu anahtarlar değiştirilmez ve uzaktan anahtar yükleme henüz bu dünyada yeni ve yavaş

kullanılmaya geçilen bir özelliktir. Hatta sertifika temelli bir kriptografik yapı POS cihazlarında mevcut değildir.

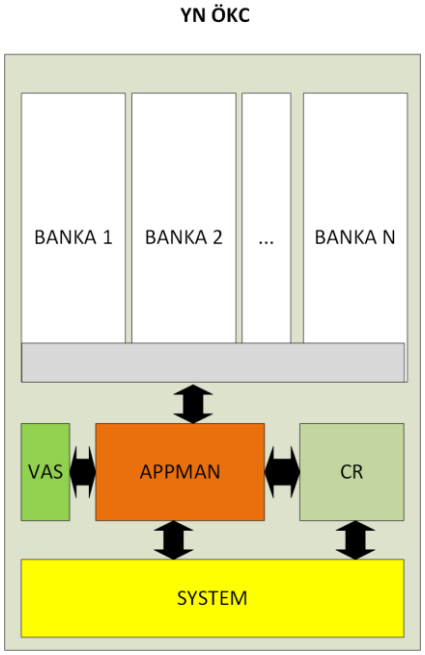
Bu çalışmada önerilen modelin özgünlüğü; (1) ödeme sistemini gerçekleyen uygulamaların banka uygulamasından bağımsız olarak anahtar yönetiminin sertifika temelli ve açık anahtar yönetim sistemine tam uyumlu olarak tasarlanması, (2) sağlanan güçlü anahtar yönetim altyapısının bütün uygulamalar (bankacılık uygulamaları ve diğer uygulamalar) için aynı seviyede güvenlik sunması, (3) böylelikle farklı ve görece zayıf anahtar yönetimine sahip bankacılık sistemlerini daha güçlü bir kriptografik seviyeye çıkaracak nitelikte olmasıdır.

1.1 Tezin Amacı

Günümüzde aynı POS cihazı üzerinden birden çok banka uygulamasının çalışmasına olanak veren ortak POS kavramı bulunmaktadır. Yeni Nesil Ödeme Kaydedici Cihazlar için de ortak POS kavramı söz konusudur. Bankacılık yazılımlarının yanında YN ÖKC içerisinde ayrıca Yazarkasa (Cash Register - CR) yazılımı ve Katma Değerli Servisler (Value Added Services - VAS) dediğimiz VAS uygulamaları da bulunabilmektedir. Birçok yazılımın birbiriyle uyumlu ve sıralı bir şekilde çalışması için genel olarak ifade edebileceğimiz Uygulama Yöneticisi (Application Manager - AppMan) yazılımı da bu cihazlarda bulunabilmektedir. Temel olarak bir YN ÖKC içerisinde bulunabilecek uygulamalar Şekil 1.1'de gösterilmiştir. Bu yapıya göre her bir bankanın kendi ekosistemiyle birlikte yazarkasa yazılımı ve başkaca katma değerli servis yazılımları çalışabilmektedir. YN ÖKC donanımı ve yazarkasa yazılımı (CR), GİB tarafından yayınlanmış mevzuatlarla yapısı ve çalışması açıkça belirlenmiştir. Yazarkasa yazılımları aynı zamanda Ortak Kriter (Common Criteria – CC) EAL 2 seviyesinde olması gereken bir yazılımdır [9]. Öte yandan bankacılık yazılımları da uluslararası standartlara göre geliştirilmiş ve anahtar güvenlikleri uluslararası kuruluşlarca belirlene uygulamalardır. Çalışmada bu kurallar gözetilerek güvenli anahtar altyapısı açıklanacaktır.

Kısaca özetlemek gerekirse bu çalışmada önerilecek model ile aşağıdakilerin geliştirilmesi mümkün hale gelecektir:

- TSM ekosisteminde her banka için uygulanabilir sertifika temelli güçlü bir anahtar yönetim altyapısı,
- Kolay entegrasyon sağlanabilecek online işlem altyapısı,
- Farklı altyapılı YN ÖKC'ler için GİB'in tariflediği her iki TSM çalışma modelini tek bir TSM altyapısında kullanabilme,
- TSM'in gelen/giden bankacılığa özgü hassas veri içeriğini görmesini engelleyecek şifreli ve güvenli mesajlaşma altyapısı.



Şekil 1.1 : Uygulama mimarisi olarak yeni nesil ödeme kaydedici cihazlar.

1.2 Literatür Araştırması

Yeni Nesil Ödeme Kaydedici Cihazlar, dünyada ilk defa Türkiye'de hayata geçirilmiş, yazarkasa ile POS cihazının bir arada kullanımına olanak veren bütünleşik bir yazarkasadır. YN ÖKC'ler; teknolojik gelişmeler çerçevesinde teknik özellikleri yeniden belirlenen Ödeme Kaydedici Cihazları ifade etmektedir. Bu yüzden bu çalışmada çoğunlukla mevzuatlar ve yayınlanmış teknik dokümanlar referans alınarak çalışma yürütülmüştür. Ayrıca banka kartlarının bu tarz cihazlarda kullanımına ilişkin güvenlik kriterleri uluslararası kuruluşlar tarafından kabul görmüş ve gerekliliği zorunlu hale getirilmiş standartlar da araştırmanın içeriğini belirlemiştir.

Bu çalışmaya esas konu olan ve GİB tarafından tanımlanmış olan TSM, YN ÖKC mesajlarının GİB Bilgi Sistemine ve üye işyeri anlaşması yapan kuruluşlara, belirlenen iletişim protokolleri çerçevesinde aktarılmasını sağlama amacıyla kurulan ve YN ÖKC üreticilerine ait terminal yönetim merkezini ifade etmektedir [2],[3]. Bu tanımla TSM merkezleri dünyadaki örneklerden farklı olarak konumlanan ve işletilen güven merkezleridir. Bankacılık sektöründe ise TSM merkezlerine kısmen benzeyen güven merkezlerine Ödeme Servis Sağlayıcıları (Payment Service Providers - PSPs) denmektedir [10].

Visa, Ödeme Servis Sağlayıcı (PSP) olarak çalışan merkezlere Third Party Agent (TPA) (veya agent, gateway, service provider) [11] olarak isimlendirirken, Mastercard ise bu merkezlere Third-Party Processors (TPP) [12] şeklinde ifade etmektedir. Türkiye'de ise servis sağlayıcılar altında bu işi yapan firmaların listesini BKM (Bankalararası Kart Merkezi) tutmaktadır [13]. TPA, doğrudan veya dolaylı olarak bir Visa müşterisine ödemeyle ilgili servisleri sunan ve/veya Visa kart sahibi verilerini depolayan, işleyen veya ileten VisaNet'e doğrudan bağlı olmayan bir servis sağlayıcıdır [11]. Bankalar müşterilerle anlaşmaları kendi yapar, ödeme sistemleriyle ilgili (kart basımı, kart bilgisi taşıma, bankacılık işlemlerini karşılama, yetkilendirme vb. işlemler) işlemler banka adına bankanın yetki verdiği ölçüde bu güvenilir ödeme servis sağlayıcılar tarafından sağlanabilir. Bu açıdan irdelendiğinde Ödeme Servis Sağlayıcılarının banka adına kredi kartı ödeme sistemlerini bankaya benzer işlettiği söylenebilir. Ancak banka hesabında para durumları vb. bilgileri sorgulamak için banka ile entegre olunduğunda bu şekilde çalışmanın Tükiye'de konumlandırılan TSM merkezleri ile benzerlik gösterdiği söylenebilir. Genel anlamda TSM merkezleri bankacılık ödeme işlemlerini işleyen taraf değil, finansal işlemleri bankaya güvenli olarak taşıyan, bankanın geri dönüşünü terminallere ileten ve bu işlemleri yaparken mali kayıtlarla eşleştiren merkezlerdir. Bu rolle çalışmasıyla bu merkezler dünyada ilk sayılırlar.

Avrupa Komisyonu (European Commission), 2013 yılında önerdiği revize Ödeme Servisleri Direktifinde (Payment Services Directive) [10], 3. Parti Ödeme Servis Sağlayıcıları (Third Party Payment Service Provider - TPP) nosyonunu tanıtmıştır. İlgili direktifte bu sağlayıcılar Ödeme Servis Sağlayıcı (PSP) olarak açıklanmış ve ödeme hesapları erişiminde iş faaliyetlerinin nasıl sürdürüleceği planlanmıştır. Avrupa Ödemeler Konseyi (European Payment Council - EPC), TPP faaliyetleriyle

ilgili önerilen yeni kurallar setinde yapılacak önemli değişikliklerin, Avrupa Birliği (AB) üyeleri, yani Avrupa Parlamentosu ve Konsey arasındaki diyalogda mutabakata varılması gerektiğine inandığını belirtmiş böylelikle direktif uyarınca banka müşterilerinin fonlarının ve verilerin ödeme hesabı erişim hizmetleri ile güvence altına alınmasının sağlanacağını söylemiştir [14]. EPC'ye göre kolaylık önceliktir; güvenlik vazgeçilmezdir. Ödeme yeniliklerini hem ödeme yapanların hem de alacaklıların yararına teşvik etmek için ise her ikisini (kolaylık ve güvenlik) birleştirmeyi gerektirdiğini vurgulamıştır [14]. Ulusal açıdan bakıldığında TSM merkezleri de bankacılık ödemeleri için güvenli bir ortamı sağlarken mali güvenceyi de sağlar nitelikte konumlanmıştır. Böylelikle ödemeler ve mali izler birbiriyle örtüştürülerek mali takibin daha etkin yapılması sağlanmıştır.

Ödeme Servis Sağlayıcılarının asıl ticari faaliyeti; ödeme başlatma veya hesap bilgileri gibi ödeme hesaplarına erişimi temel alır ancak genellikle müşteri parasını tutmayan hizmetleri sunar [14]. Müşteri hesapları ve mali bilgileri bankalarda bulunmaktadır. PSP'ler bankalara karşı sorumludur. TSM merkezleri ise GİB tarafından adı konumu, amacı belirlenmiş ve denetlettirilen oluşumlardır.

Ödeme Servis Sağlayıcıları ile ilgili yapılmış bir başka makalede önerilen bir hipotez ile, bankalar tarafından maliyet etkinliğinin sağlanmasının yanı sıra, ödeme talimatlarının ve işlemlerin bankalar yerine doğrudan ödeme servis sağlayıcılarıyla sunulmasının müşteri memnuniyetini arttırılabileceği önerilmiştir [15]. PSP kullanımının sadakat sistemleri için de önemli olduğu vurgulanmıştır.

Günümüzde ödeme sistemlerinde bölümlerin ve rollerin yasal olarak yavaş yavaş ayrıştırıldığı ve bankalarında müşterilere odaklanarak ödeme faaliyetlerini Ödeme Servis Sağlayıcılarla sağlamaya yöneldiği görülmektedir.

Türkiye'de TSM merkezleri bankacılık sistemlerinin kullandığı Ödeme Servis Sağlayıcılardan öte, bütün işlemleri mali işlemlerle örtüştüren yapısıyla dünyadaki örneklerinden bu şekilde ayrışmaktadır.

2. YAZARKASA VE POS

2.1 Yazarkasanın Tarihçesi

Dünyada ilk yazarkasanın icadı birçok şeyde olduğu gibi bir gereksinimden doğmuştur. Ancak çok daha önceleri de nakit kayıtları için farklı araçlar kullanılmıştır. Erken dönem yazarkasalar, her satış tutarını bir kâğıt rulosuna kaydetmiş, ancak işlem özetlerini kaydetme gibi sınırlı bir yardım sağlamıştır. Sonraki dönemlerde bilgisayar sistemlerinin gelişmesiyle yazarkasalar akıllanmış ve günümüzde birçok işlevi yapabilir hale gelmiştir. Bu bölümde kısaca yazarkasanın günümüze kadar gelişimi ve tarihçesi aktarılacaktır.

2.1.1 Nakit kayıt öncüsü abaküs

Ticari işlemleri izlemek için yapılan en eski icatlardan biri olan “Abaküs”, bir kişinin aritmetik hesaplamalar yapmasına yardımcı olan bir araçtır. Orta doğuda 4500 yıl önce keşfedilen bu araç Mısırlılar ve Çinliler tarafından bugünkü haline dönüştürülmüştür. Çeşitli abaküs tasarımları mevcuttur. "Abaküs" kelimesi, "sayım tahtası" anlamına gelen Yunanca “abax” kelimesinden gelir [16]. Cihazın Asya dillerinde başka isimlendirmeleri de bulunmaktadır. Günümüzde yazarkasalar abaküs işlevlerinin çoğunu mekanik olarak uygulamaktadır.

Antik zamanlarda abaküs kumun içine çakılların yerleştirildiği bir sıra oluktan oluşuyordu. Daha sonraları levha veya tahta kullanımı, Asya genelinde yaygın olarak kullanılan taşınabilir bir cihaz olmasını sağlamıştır. Günümüzde, paralel teller üzerine dikdörtgen çerçeve içerisinde dizilmiş boncuklardan oluşmaktadır ve elektrik ve pillerin kıt olduğu ya da pahalı olduğu yerlerde halen kullanılmaktadır [16].

Abaküs, yer-değeri gösterimi ilkesinde çalışır: boncuğun konumu değeri belirler. Boncuklar bir yöne kaydırılarak sayılır veya sayısal değerler verilir.

2.1.2 Nakit çekmecesi

19. yüzyılın ortalarına kadar, banknotları ve paraları tutacak bölücüleri olan para çekmecesi, tüm dünyadaki perakende işletmelerin ortak bir özelliğiydi. Ancak, endüstriyel devrimin büyümesiyle artan iş hacmi ve artan kentleşmeyle, her satış noktası için günlük işlemlerin hızlı ve doğru özetlerine ihtiyaç duyuldu. Sahtekâr kasiyerler, işlemleri kolayca denetlemenin bir yolu olmadığından ve süpervizörleri yokken nakit çekmecelerini çıkardığı için bu aletlerin kullanım amacını tam sağlayabildiği söylenemez [17].

2.1.3 Aldatılmaz kasiyer

Bir bar işletmecisi olan James Jacob Ritty 1871 yılında Dayton, Ohio'da ilk bar salonunu açmıştır [18]. Fakat James Jacob Ritty, Dayton kasabasında işlettiği barın genellikle dolu olmasına karşın, beklenen kar oranını yakalayamadığını görmekteydi [19]. O zamanlarda nakit paralar açık kutularda saklanmaktaydı ve satışlar barmenler tarafından hesap defterine kaydedildiğinden, barmenlerin kendi ceplerine para indirmesi mümkün gözüküyordu. Bu duruma bir yandan çareler düşünen Ritty, 1878 yılında gemi ile Avrupa seyahatine çıktığında yolculuk ettiği geminin makine dairesinde gemi pervane şaftının devir sayısını ölçen bir mekanizma olduğunu gördü ve bu fikri kendi barının muhasebe kayıtları için nasıl kullanılabileceğini düşündü [19]. Fikrini tatil dönüşü kardeşiyle paylaştı ve yetenekli bir mekanikçi olan kardeşi John'la beraber yazarkasayı tasarlamaya koyuldular. Birkaç başarısız denemeden sonra çalışır bir cihaz icat ettiler. Resim 2.1'de bu yazarkasanın bir örneği gösterilmiştir.

Resim 2.1 : Ritty'nin yazarkasası.

Patentini ertesi yıl aldıkları ve adını “Ritty’nin Aldatılmaz Makinesi” olarak verdikleri makinenin dairesel bir kadranı ve tuş takımı vardı [18]. Bar personeli yapılan satışın tutarını makineye girince aygıtın kadranı o günün toplam satış rakamını gösteriyordu [19]. Böylece James Ritty her günün sonunda hesapları kontrol edebiliyordu.

Aldatılamayan makine, her satış yapıldığında satışı zil sesiyle uyaran bir özelliği vardı. Dayton’da yazarkasa üretmek için küçük bir fabrika kuran Ritty’ler, iki işi birden yürütmeye çalıştı.

James Rity, yazarkasayı icat etmeyi başarmış ancak bundan kazanç sağlamayı pek başaramamıştır. Bölgede faaliyet gösteren bir iş adamı olan John H. Patterson, yazarkasaların katkısından çok etkilenerek Ritty'nin şirketinin çoğunluk hissesini satın aldı [19]. Şirketi ayağa kaldıran Patterson, şirketin ismini National Cash Register Co. (Bugün NCR olarak bilinmektedir) olarak değiştirerek ileriki yıllarda milyarder olmuştur [19].

Patterson, NCR'yi başarılı bir işyeri haline getirdi. Patterson, daha büyük, daha iyi ve daha fazla hırsızlığa dayanıklı cihazlar üretmek için bir buluş departmanı kurdu. Satış temsilcileri için bir eğitim programı başlattı [16].

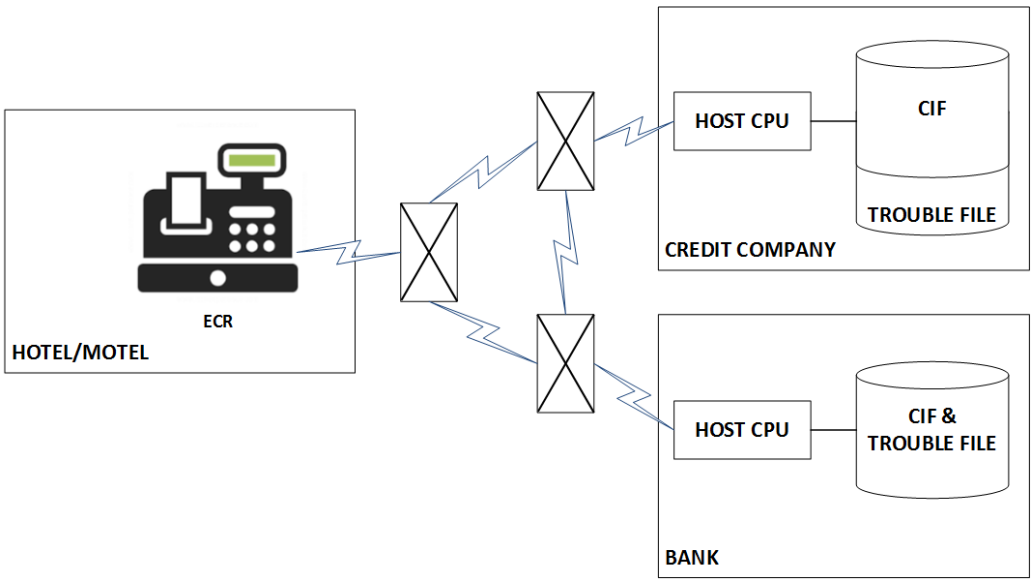
1888-1915 döneminde, süslü dökme metal durumlarda olan yazarkasa, hemen hemen her perakende kuruluşuna yayılmıştır. Bu dönemde en iyi pirinç ile kaplanmış dökme kalıplarla üretildi.

Pirinç malzeme, toplam pazarın %95'ini temsil etmek üzere büyüyen NCR şirket üretim hattına egemen oldu. NCR, o dönem dünyanın en büyük pirinç dökümhanesini işletti ve bu nedenle o zaman "Pirinç Dönemi" olarak tanımlandı.

Birinci Dünya Savaşı antik dönem yazarkasanın sonunu getirdi. Birinci Dünya Savaşı'ndan sonra, mekaniğin artık bir cazibe merkezi olmadığı kesin bir dönüm noktası oldu.

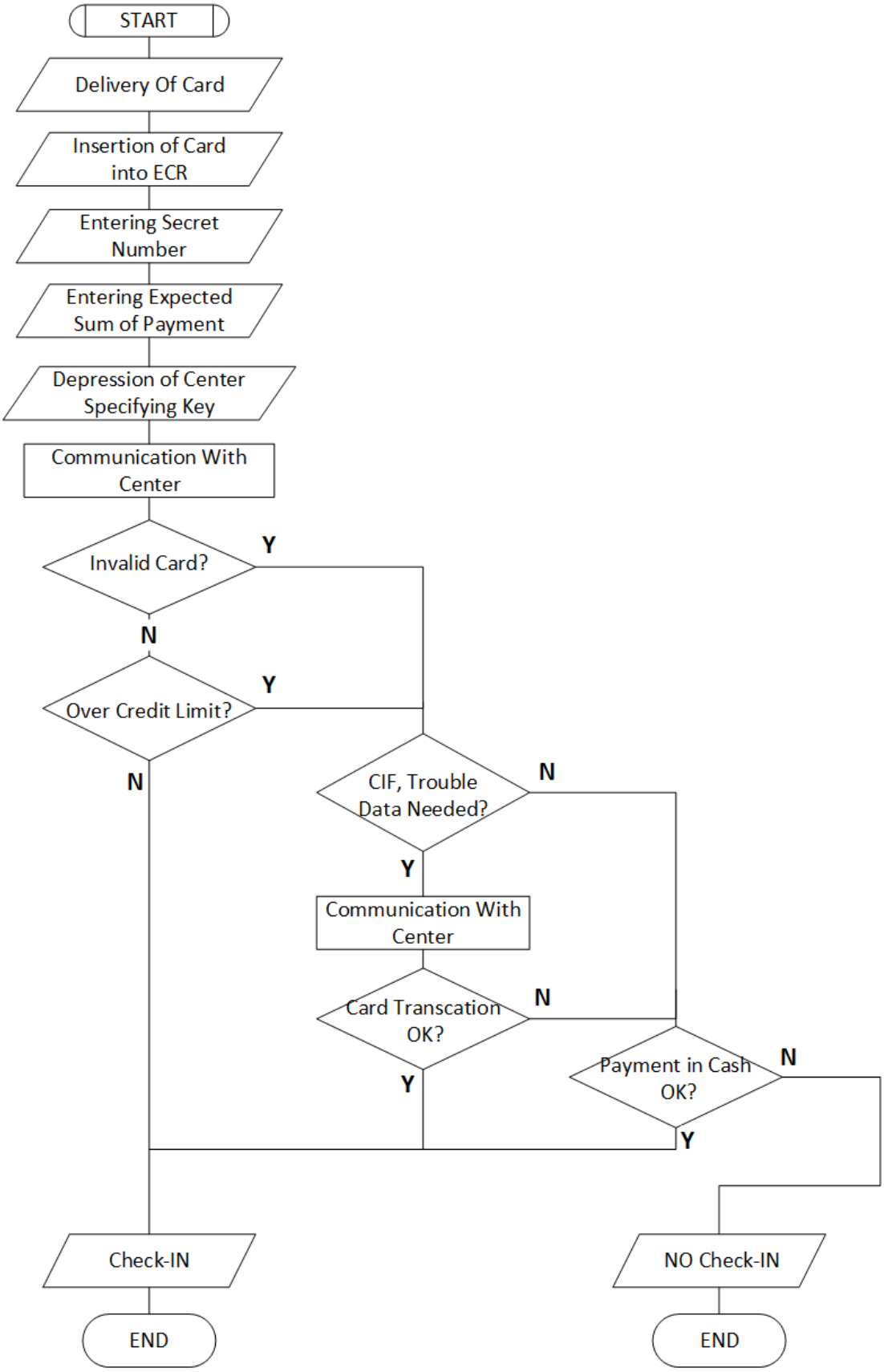
NCR'ın milyonuncu yazarkasası 1911'de satıldı ve 1915'e kadar şirket, Dayton'un en büyük işvereniydi ve maaş bordrosunda 5900'den fazla işçi vardı. İki milyonuncu makine sadece dokuz yıl sonra satıldı [18].

Sonraki yıllarda bilgisayarlı teknolojilere geçinceye kadar donanımsal olarak yazarkasa için alınan patentlerde çok farklılıklar olmadığı görülmektedir [20],[21],[22]. Bu patentlerden Ohmae vd. (1984) tarafından önerilen, oteller gibi konaklama tesislerinde kullanılabilecek ve üzerinde kartı okuyucusu bulunan elektronik yazarkasa modeline ait patent YN ÖKC basitçe andıran nitelikte bir patenttir [22]. Kredi kartlarının bankalarda kullanıma sunulmasından sonra, müşteri kartlarının her defasında resepsiyonist tarafından telefonla uygunluğu ve kredisi için sorgulanması müşterilerde memnuniyetsizlik oluşturmuştur. Özellikle telefonla kredi şirketi sorgulamasının uzun sürmesi müşteriler açısından bazen katlanılmaz uzun bekleme seviyelerine geldiği ifade edilmektedir. Bu maksatla konaklama tesislerinde bulunan elektronik yazarkasaların bu işlemi otomatik yapmasına imkân verecek bir işleyiş önerilmiştir. Resim 2.2'de sistemin işleyişine ait genel blok diyagramı görülmektedir.



Resim 2.2 : Elektronik yazarkasa kullanarak kredi kartı soruşturma sistemi [22].

Bu önerilmiş patentte [22] elektronik yazarkasa, içerisinde müşteri bilgi dosyası (Customer Information File - CIF) ve sıkıntılı dosyayı barındıran (trouble file) bir merkez olan kredi şirketine ve/veya bankaya telefon sistemiyle bağlanabilmektedir. Sistemin akış şeması Şekil 2.1'de kısaca gösterilmiştir. Sistemde güvenlik ise girilen bir numarayla sağlanır. Gizli numara gerektiğinde bu numara klavye kullanılarak konuk tarafından girilir ve karttan okunan referans gizli numarayla girilen bu numara kontrol edilir.



Şekil 2.1 : Otelde izlenecek prosedürü gösteren akış şeması [22].

Girilen numara diğeriyle eşleştiğinde, sonraki adım izlenir; Eşleşmiyorsa, ekran sonucu gösterir ve başka adım atılmaz. Merkez yani kredi kuruluşu ve/veya banka gizli numarayı müşteri bilgi dosyasında (CIF) saklayabilir ve girilen veya karttan okunan gizli numara, merkeze gönderilebilir ve burada eşleme için iki sayı karşılaştırılır. Böylelikle onay verilip verilemeyeceği anlaşılmış olur.

2.2 Türkiye'de Yazarkasa

Türkiye yazarkasa ile çok sonraları tanışmıştır. Türkiye'de 3100 sayılı (1984) kanunla yasal adı "ödeme kaydedici cihaz" olarak tanımlanan yazarkasa kullanımı, 1 Temmuz 1985'ten sonra 1 Ocak 1989'a kadar kademeli olarak tüm birinci ve ikinci sınıf tüccarları kapsayacak biçimde yaygınlaştırılmıştır. İlgili kanunda ödeme kaydedici cihazlar, "Maliye ve Gümrük Bakanlığınca belirlenen şartları taşıyan elektronik yazarkasalar, yazıcı tertibatı bulunan elektronik teraziler veya elektronik terminaller" gibi cihazlar olarak tanımlanmıştır [23].

3100 sayılı kanunla ilk kullanılması söylenen "ödeme kaydedici cihazların; her alış veriş için satışla ilgili bilgileri taşıyan bir satış fişi ve günlük kapanış fişi vermesi, satış fişinde yazılı olan bilgilerin aynen kaydedildiği ayrı bir şerit tertibatı olması, fiş ve günlük toplamlar için en az iki ayrı sayıcısının bulunması, mekanik, elektronik veya manyetik müdahalelere karşı korunmuş harici bir enerjiye ihtiyaç göstermeyen sadece pozitif işlem kabul eden toplam tahsilat ve vergi tutarlarını kaydeden bir mali hafızasının olması, mali hafıza ile bağlantısının açılması halinde çalışmaması, yetkili kimseler dışında cihaza müdahaleye imkan vermeyecek tarzda hayati bölümlerin muhafazasının tek bir vida ile kapatılmasına ve üzerinin özel bir mühürle mühürlenmesine uygun yapıda olması ve makine içerisine tespit edilmiş mali hafızaya da kaydedilen bir sicil numarasının bulunması gerektiği" ifade edilmiştir [23].

Yayınlanan 3100 sayılı kanundan sonra 2012 yılına kadar yazarkasalarda çok fazla değişiklik yapılmamıştır. Maliye Bakanı vergi kaybını önlemek için "Öyle bir yazarkasa istiyorum ki fiş kesilmeden kredi kartı kesilmesin" diyerek belki de ilk kez resmi ağızdan yeni nesil ödeme kaydedici cihazı tariflemiş olmuştur [24].

Kayıt dışı Ekonomi ile Mücadele Stratejisi Eylem Planı (2008-2010) madde 64 ile "Pos Cihazlarının Yazarkasa Niteliğine Kavuşturulması için fizibilite, teknik

gereksinimler ve yeterlilik, uygulanabilirlik incelemeleri gerçekleştirilecek; inceleme çalışmaları sonuçlarına göre uygulanabilirlik çerçevesinde yasal düzenlemeler yapılacaktır." eylem kararı alınmıştır [6]. Kayıt dışı Ekonomi ile Mücadele Stratejisi Eylem Planı (2011-2013) madde 13 ile de "POS cihazlarının yazarkasalarla uyumlaştırılması sağlanacaktır" eylem kararı alınarak teknik ve hukukî alt yapının tamamlanması için gerekli çalışmalar Gelir İdaresi Başkanlığı koordinatörlüğünde başlatılmıştır [7].

2.3 Dünyada Kartlı Ödeme Sistemlerin Tarihçesi

Edward Bellamy'nin "Looking Backward 2000-1887" isimli romanında, insanların yanlarında nakit taşımalarına gerek olmaksızın alışverişlerde ödeme yapabilmeleri fikri ve kredi kartı ifadesi tarihte ilk kez ortaya çıkmıştır [25]. Bellamy (1888), "kredi kartı (credit card)" söz dizisini kitabında tam 10 farklı yerinde geçirmektedir [25].

Bugün ödeme kartı olarak kabul edilen ilk araç ABD'nin önde gelen telgraf şirketi Western Union tarafından 1914 yılında çıkartılmıştır [26]. Asker künyesine benzeyen ve üzerinde adının yazılı olduğu bu metal plakayı kullanan müşteri, çok sayıda telgrafı gönderebiliyor ve ay sonunda gelen ayrıntılı faturayı tek seferde ödeyebiliyordu [26]. Kaliforniya Umumi Petrol Şirketi (General Petroleum Corporation) ilk önce çalışanlarına ve seçkin müşterilerine, zaman içinde tüm halkı kapsayacak şekilde benzin alımında kullanabilecekleri ilk kredi kartını 1924 yılında çıkarmış, Mobil ve Shell petrol şirketleri de kısa süre içinde benzer uygulamaları hayata geçirmiştir [26].

MasterCard'a göre banka kartı konseptini ilk uygulayan kişi bankacı John Biggins olmuştur. Biggins, bankasındaki mevduat sahipleri için, Brooklyn civarında yapacakları harcamalarda geçerli olmak üzere 1946 yılında "Charge-It" adıyla bir banka kartı çıkarttı [26]. New York'taki Franklin National Bank, benzer bir konsepti yalnızca bankada hesabı olanlar tarafından kullanılabilecek şekilde ilk kredi kartları için 1951'de uyguladı. Sonraki yıllarda benzer olarak birçok banka seçtikleri satıcılarla kredi kartını kullanmayı kabul etti [27].

1950'lerde ülke çapında çok sayıda restoranda geçerli olmaya başlayan Diners Club kartı bir süre sonra bazı oteller ve araç kiralama şirketlerin de de geçen bir kart olarak kullanılmaya başlandı [26].

American Express'in 1958 yılında piyasaya sürdüğü hem ABD'de hem yurtdışında geçerli olan kartı bir anda lider konuma gelmiştir. Ardından Hilton Otelleri zinciri, müşterilerine nakit kullanmadan konaklama yapma, yeme-içme ve eğlenme olanağı veren kendi kartını çıkarttı [26].

Resim 2.3 : Metal plakalarda ilk özgün kredi kartları [26].

16 Ağustos'ta bir grup kredi veren bankalar tarafından kurulmuş InterBank Kartı Birliği (ICA) ulusal bir kredi kartı sistemi oluşturmuştur. Diğer benzerlerinin aksine ICA (şimdi MasterCard Worldwide) tek bir bankanın hakimiyeti altında değildi. ICA, kart provizyon, takas ve mahsuplaşma prensiplerini belirledi ayrıca, para değişimini işlemeye yönelik bir ödeme ağı ve sistemi geliştirdi [27].

1970'ler ilk kredi kartı otorizasyon sisteminin hayata geçirildiği tarih olmuştur. O zamanın komite üyesi Dee Hock, 1973 Kasım ayında IBM'e büyük bir donanım siparişi vermiş ve IBM'den uzmanlar sistemi kurmak ve devreye almak için Visa'nın teknik ekibiyle yakın bir çalışma gerçekleştirmiştir [24].

Kredi kartının dünyanın farklı yerlerinde sürekli başka adlarla anılıyor olmasının sistemin büyümesine engel teşkil edeceği açıktı. Dünyanın çoğu yerinde genelde kartı çıkaran bankanın adını taşıyan kartlara piyasadaki diğer bankalar katılmakta gönülsüz davranıyordu [26]. Ayrıca kartın farklı adlarla piyasaya çıkması kafaları karıştırıyordu. Dolayısıyla evrensel bir anlama ve cazibeye sahip yeni bir isim bulundu ve 1977 yılında bankalar tüm ürünlerinin adını Visa olarak değiştirmeyi kabul etti [27].

2.4 Banka Kartı Terminallerinin Tarihçesi

Milyonlarca işletme tezgahının üzerinde yer alan kredi kartı terminalleri çok kısa bir geçmişe sahiptir. Bu durum, günümüzde en çok kullanılan terminallerin neden 20

yaşında bir teknoloji kullandığını açıklamaktadır. Askeriye gibi, kredi kartı terminalleri de teknolojilerini güvenilirlik ve güvenlik temeline oturtmaktadır. Yeni teknolojiler büyük güvenlik sağlayabilirken, bu teknolojilerin kullanımı zamanla test edildiğinden ödeme işlemlerinde gerçekleştirilmesi yavaş olmaktadır.

Bu bölümde günümüzde kullanılan POS terminallere gelinceye kadar banka kartlarının kullanılmasında kullanılan terminaller kısaca açıklanacaktır.

2.4.1 Manuel görüntüden yazıcı (Imprinter)

Manuel görüntüden yazıcılar, kredi kartlarının geniş kabulünün başlangıcından bu yana etrafımızda olmuştur. İşletmelerin birincil yöntemi kullanamadığında kullanabildiği ve bir yedekleme işleme yöntemi olarak kabul edildiği dönemlerde olmuştur. Başlangıçta, tüccarlar müşterilerinin kartlarını bastırıp fişlerini kendi bankalarına postalamaktaydı. Bu işlem zaman alıcıydı ve bugün standart olan hız ve anlık aktarma yeteneklerini sunmamaktaydı. Tüccarlar manuel görüntüden yazıcı kullanarak anında kredi kartının görüntü kopyasını oluşturabiliyordu. Sonrasında bu kopyaları bankaya yollayarak paralarını inceleme bittikten sonra alabiliyordu [28].

2.4.2 Elektronik yetkilendiriciler

İlk elektronik kredi kartı yetkilendirmeleri telefonla yapıldı ve çoğu zaman beş dakikadan fazla sürdü. Tüccarların işlemlerini manuel görüntüden yazıcılarla görüntü kopyasını alması veya bir yetkilendirme çağrısı yapma seçeneği vardı. Zamanında bir işlemin telefon üzerinden yetkilendirilmesi için uzun süre bekletildiği için, birçok işletme yalnızca büyük miktarlı işlemlerde sesli yetkilendirmeyi seçmiştir.

2.4.3 POS terminaller

Point of Sale (POS) terminalleri 1979'da Visa'nın hantal bir elektronik veri yakalama terminali başlatmasıyla ortaya çıktı. Bu cihaz bugün bildiklerimiz gibi kredi kartı terminallerinin ilkiydi ve bir kredi kartının işlemesi için gereken süreyi önemli ölçüde azalttı. Aynı yıl MasterCharge MasterCard oldu ve manyetik bilgi şeridi içeren kredi kartları geliştirildi. 1979 yılı kredi kartı işleme sektöründe bir dönüm noktası oldu [26].

Günümüzde kredi kartları ile nakit gerekmeksizin üye iş yerlerinden mal veya hizmet alınabilmesi için POS makinelerine gereksinim duyulmaktadır. "POS makineleri, enerji ile çalışan telefon veya data hatlarını kullanarak elektronik ortamda kurulumu gerçekleştirilerek kurulum bankası ile iletişim sağlayarak, dünyadaki kartlı sisteme dâhil bankaların bilişim sistemlerine ulaşarak 10-15 saniye gibi kısa sürede yetkilendirme (otorizasyon) alan ve kendi belleği ile de bazı kontrolleri yaparak satış belgesi basabilen bir tür bilgisayar" olarak tanımlanmaktadır [29].

Kredi kartı işlem teknolojisinin ilerlemesi için çok özellik vardır. Artan işlem hızı, güvenilirlik ve güvenlik, teknolojiyi ilerletmenin arkasındaki itici güçtür. IP ve WiFi tabanlı işlemler yeni ortaya çıkarken, kontaksız ödemeler, biyoteknoloji ve akıllı kartlar hemen köşede beklemektedir. İşleme endüstrisinde sabırsızlıkla beklenecek çok şey vardır ve yakın gelecekte kesinlikle yeni teknolojilerin uyarlanması kaçınılmazdır [28].

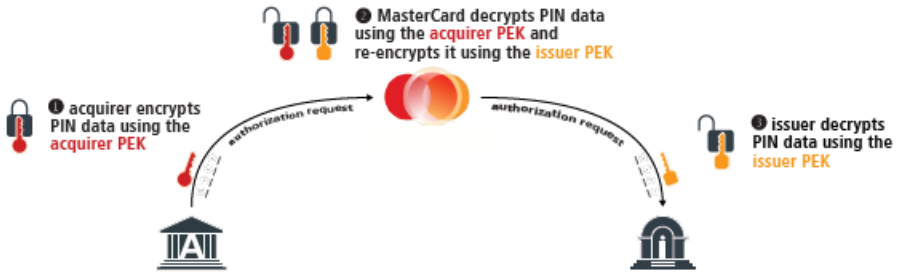
2.5 PCI PIN Güvenliği Standardı Açısından POS Cihazlarında PIN ve Anahtar Güvenliği

Ülkemizde kredi kartı ve banka kartı kullanımı giderek artmaktadır. Özellikle nakit kullanımı yerine alışveriş işlemlerinin ödemesini kart ile yapmak insanlara kolay gelmektedir. Ayrıca insanlara kazandırdığı puan vb. avantajlar nedeniyle kredi kartlarının kullanımının fazlasıyla artacağa benzemektedir.

Kart hizmetleri sunan firmaların operasyonlarını gerçekleştirirken uyması gereken uluslararası kurallar, PCI-SSC (Payment Card Industry Security Standards Council) adı verilen ve aralarında American Express, MasterCard Worldwide, Visa Inc., Discover Financial Services ve JCB International gibi üyeleri bulunan bir konsey tarafından geliştirilmekte ve yayımlanmaktadır [36]. Bu kapsamda kart sahibi ve POS sahibi kuruluşların uyması gereken PCI DSS (PCI Data Security Standards), PA DSS (Payment Application Data Security Standards) ve PIN Security gibi standartlar bulunmaktadır.

Mastercard, PIN bilgisini iletim esnasında korumak için kullandığı anahtarı PEK (PIN Encryption Key) olarak tanımlamaktadır [30]. PIN Şifreleme Anahtarı (PEK), PIN verilerini MasterCard ağı üzerinden gönderirken şifrelemek için kullanılır. Tüm

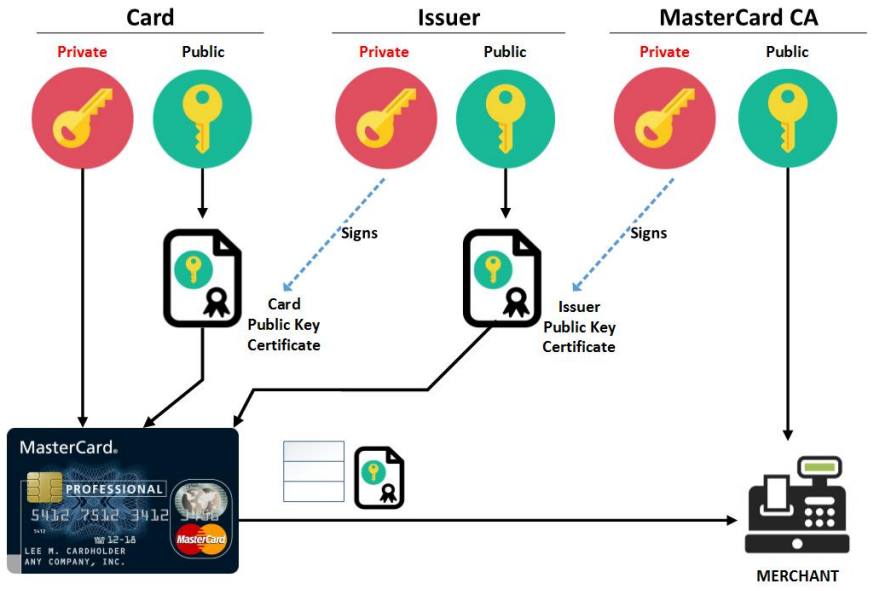
kart sahibi kuruluş (issuer) ve POS sahibi kuruluş (acquirer) (veya işlemcileri), PIN tabanlı işlemleri gerçekleştirmek için bir PIN Şifreleme Anahtarına (PEK) ihtiyaç duyar. Resim 2.4'te bu paylaşım gösterilmiştir.



Resim 2.4 : MasterCard ağı üzerinde PIN paylaşımı [30].

Üye İşyeri, MasterCard'a yetkilendirme talebi için sorgulamadan önce göndereceği mesaj içerisindeki PIN verisini kendisine ait PEK ile şifreler. MasterCard, kendisine gelen mesajdaki şifreli PIN verisini üye işyerine ait PEK ile çözer. Mastercard, kart sahibi kuruluşa mesajı göndermeden önce mesaj içindeki PIN verisini kart sahibi kuruluşa ait PEK ile tekrar şifreler. Bu işlemin yürütülebilmesi için her iki tarafa ait PEK, öncesinde güvenli bir şekilde MasterCard'a ulaştırılmış ve kaydedilmiş olmalıdır. Kart sahibi kuruluş kendisine gönderilen mesaj içerisinde şifreli PIN verisini kendisine ait PEK ile çözer ve üye işyerine yetkilendirme bilgisine ait uygun yetkilendirme cevabını geri döner.

EMV Çip (Chip), kart ödemeleri endüstrisinin tamamında eski ve daha az güvenli manyetik şerit teknolojisini yavaş yavaş değiştiren bir teknoloji altyapısını ifade eder. EMV (Europal MasterCard Visa baş harfleri); Europal, MasterCard ve Visa tarafından 1990'ların ortalarında geliştirilen ve bu altyapı üzerinde birlikte çalışabilirliği sağlayan standardı ifade eder. EMV çip kartı, dünyanın herhangi bir yerindeki herhangi bir EMV terminalinde çalışacaktır. EMV çip altyapısında simetrik ve asimetrik kriptografi kullanılabilmektedir [31]. Aslında EMV çipli kartlarda Açık Anahtar Altyapısı (Public Key Infrastructure – PKI) kullanılıyor demek daha doğru olacaktır. MasterCard özellikli kredi kartların sertifika temelli yapısı Resim 2.5'te sunulmuştur.



Resim 2.5 : Anahtar sertifikalandırma prosesi [31].

Her ne kadar çipli kartlarda güçlü anahtar altyapısı olmasına rağmen POS cihazları henüz Açık Anahtar Altyapısı (Public Key Infrastructure - PKI) gibi güçlü anahtar yönetimi için geçiş aşamasındadır. Özellikle banka ile haberleşmede sertifika temelli güvenlik altyapısını kullanan POS cihazlarını görmek mümkün değildir.

Bu çalışmada kişisel bilgilerin taşınmasında güvenli anahtar yönetimi ve işlem trafiğinde hassas veri iletimi olmasından dolayı, bu işlemleri yapabilmek için sahip olunması ve uyulması gereken PCI-DSS ve PIN Güvenliği standartlarına birlikte değinilecektir [32,33]. PCI PIN Güvenlik Gereksinimleri, PIN doğrulama işlemlerini kabul eden veya işleyen işletmeler için PCI Veri Güvenliği Standartlarıyla (DSS) tamamlanır [32].

PCI-DSS, 12 ana başlıkla tanımlanan güvenlik gereksinimini ve bunlara karşılık gelen test prosedürlerini bir güvenlik değerlendirme aracında birleştirir [32]. PIN güvenliğiyle bir bütün çepeçevre güven sağlanmış olur.

PCI-DSS, üye iş yerleri, işlemci kuruluşlar, mali kuruluşlar ve hizmet sağlayıcıların yanı sıra, kart sahibi verilerini ve/veya hassas kimlik doğrulama verilerini saklayan, işleyen ya da ileten tüm diğer kuruluşları da içermek üzere, ödeme kartı işlemede kapsanan tüm kuruluşlara uygulanır. Kart sahibi verileri ve hassas kimlik doğrulama verileri çizelge 2.1'de gösterildiği şekilde tanımlanır:

Çizelge 2.1 : Kart sahibi verileri ve hassas kimlik doğrulama verileri [32].

Hesap Verileri	
Kart Sahibi Verileri	**Hassas Kimlik Doğrulama Verileri**
• Birincil Hesap Numarası (PAN) • Kart Sahibi Adı • Son Kullanma Tarihi • Hizmet Kodu	• Tam izleme verileri (manyetik şerit verileri ya da bir çipteki eşdeğeri) • CAV2/CVC2/CVV2/CID • PIN'ler ve PIN blokları

Birincil hesap numarası (Primary Account Number - PAN), kart sahibi verileri için tanımlayıcı etkendir. Kart sahibi adı, hizmet kodu ve/veya son kullanım tarihi, PAN ile saklanır, işlenir ve iletilirse veya kart sahibi verileri ortamda başka bir şekilde mevcut olursa, bunlar yürürlükteki PCI DSS gereksinimlerine göre korunmalıdır. PCI DSS gereksinimleri, hesap verilerinin (kart sahibi verileri ve/veya hassas kimlik doğrulama verileri) saklandığı, işlendiği ya da iletildiği kuruluşlara ve ortamlara uygulanır [32].

Türkiye'de model olarak belirtilen Trusted Service Manager (TSM) merkezleri terminal anahtar yönetimini ve bankacılık işlem trafiğini üzerinden geçirerek ilettiği için PCI-DSS ve PIN Security standartlarına sahip olmalıdır.

Anahtar; verinin gizliliğini sağlamak için gereksinim duyulan şifreleme ve şifre çözme algoritmalarına sağlanan değerdir [36]. Kart operasyonları ve birçok güvenli işlem için çok sayıda anahtar içeren bir anahtar hiyerarşisinden faydalanılmaktadır. LMK anahtarı, Hardware Security Module (HSM) denilen donanımsal güvenlik modülü cihazları dışında depolanacak olan diğer şifreleme anahtarlarını şifrelemek için kullanılan simetrik bir anahtardır. Genellikle tüm diğer anahtarlar LMK ile şifrelenmiş şekilde veritabanında tutulmaktadır. Yalnızca LMK anahtarı Donanımsal Güvenlik Modülü (HSM) cihazları içinde bulunmaktadır ve saklanmaktadır. PIN en basit haliyle debit kartı veya kredi kartını kullanmak için ATM veya POS PIN giriş cihazlarından girmiş olduğumuz 4, 5 veya 6 haneden oluşan şifrelerimizdir. Kart sahibi banka daha uzun PIN değerlerini, ISO 9564 tanımına göre maksimum 12 hane olacak şekilde destekleyebilir [34]. Ancak girilen bir PIN altı basamağı aşarsa, POS sahibi bankanın girileni en fazla altı haneli olarak kesmesine izin verilir.

Çoğu ülkede manyetik şeritli kartlardan çip göçü, baskın Kart Doğrulama Metodu (Card Verification Method – CVM) olarak daha güvenli PIN doğrulamasına geçmek için bir fırsat olarak algılanmıştır. EMV çipi hem PIN hem de imzayı Kart Doğrulama Metodu olarak desteklemektedir, ama yeni olarak çevrimdışı PIN opsiyonunu da içermektedir [35]. Manyetik şeritli kartlar için ise önemli bir Kart Doğrulama Metodu olarak PIN, iyi koruma sağlar, ancak Manyetik şeritli kartlar için PIN yalnızca PIN'i şifrelemek ve şebeke üzerinden güvenli bir şekilde nakletmek için uygun güvenlik altyapısı bulunduğu zaman uygulanabilir [31].

Genel olarak PIN doğrulama, ıslak imza doğrulamasından üstündür ve kayıp, çalıntı ve kart varlığı alınmayan kart dolandırıcılığının azaltılmasında önemli bir faktördür. PIN kullanımı, işlem hızı ve verimliliği arttırmış ve kart hamili ve tüccar deneyimini önemli derecede geliştirmiştir. Tüccarların çalışanları artık bir imzayı beklemek veya kağıt makbuzunu işlemek ve saklamak zorunda değillerdir [31]. Bu yüzden PIN'in kendisi kadar PIN'in güvenli iletimi önemlidir.

Manyetik şeritler, Track adı verilen (Track 1, Track 2 ve Track 3) alanlarda metin ve sayısal bilgi içermektedir. Genellikle Track 1 ve Track 2 alanları kullanılır. Bu alanlarda kart numarası (PAN), kart sahibinin adı, son kullanım tarihi, PIN doğrulama verisi vb. hassas veriler bulunabilir [34]. Bu alanların POS banka işlemlerinde güvenli olarak taşınması için şifre anahtarları kullanılır.

Anahtar ve PIN güvenliği için dikkat edilmesi gereken noktaları ve anahtar kullanım sürecini üç başlık altında incelenebilir. Bu başlıklar kısaca aşağıda sunulmuştur [36].

- Donanımsal Güvenlik Modülü (HSM) cihazların temini
- Anahtarların üretilmesi ve güvenli saklanması
- Anahtarların kullanılması, paylaşılması ve kullanım dışına alınması

Bu bölümün geri kalan kısmında bu maddelere kısa kısa değinilecektir.

2.5.1 Donanımsal güvenlik modülü (HSM) cihazların temini

HSM gibi korunaklı olması gereken cihazların temini ve kullanılacağı lokasyona kadar güvenli transferi, PIN ve anahtar güvenliğinin sağlanması adına yapılması gereken ilk aşamalardan biridir. Bu cihazları anahtar yönetim işlemleri için

kullanacak olan kurumların, cihazı satın aldığı noktadan teslim edildiği noktaya kadar herhangi bir müdahaleye maruz kalmadığından emin olmalıdırlar [36]. Bunun için satın alma sürecini, ürünün güvenli taşınmasını, ürün kontrol ve kurulum gibi süreçlerini bu prensibe göre dizayn etmelidir. Buradaki amaç üretim yerinden teslimine kadar geçen süreçlerde güven zincirinin kontrol altında olmasının sağlanmasıdır [33]. Örneğin yeni bir HSM satın alımında, HSM üreticisinden çıkarak firmaya kadar cihazın güvenli bir kanal ile ulaştırılması sağlanmalı, firmaya ulaşan HSM ile fatura üstünde belirtilen seri numaraları karşılaştırılmalı, ambalajının taşıma aşamasında açılıp açılmadığı kontrol edilmeli ve HSM en az iki kişi (dual control) ile izlenen/girilebilen güvenli alana kaldırılmalıdır [36]. Cihazın çıkarılıp başka bir alana taşınıp kurulması adımlarında da aynı hassasiyet gösterilme, bu tür cihazlara müdahale olmadığını kanıtlayabilmek adına delil zinciri oluşturulmalı, korunmalı ve kırılmadan sürdürülebilmelidir [33],[36].

2.5.2 Anahtarların üretilmesi ve güvenli saklanması

Anahtar üretimi için HSM denilen ve PCI standartlarının istediği güvenli cihazlar kullanılmaktadır. Kurcalamaya karşı koruma özelliğine sahip bu cihazlar herhangi bir fiziksel zorlama karşısında üzerlerindeki objeleri sıfırlar (zeroization) ve içerisinde sakladığı anahtarları kullanılamaz hale getirir [36].

HSM cihazları sistem odaları gibi fiziksel güvenliği sağlanmış ortamlar içerisinde çift anahtarlı (dual control) kabinler içinde muhafaza edilmelidir. Bu cihazlara erişimin kontrol edilmesi sağlanması ve erişim izinin tutulması sağlanmalıdır [32].

HSM cihazlarına bilgi saklayabilecek ya da ağın diğer bilgisayarlarına bilgi transferi yapabilecek akıllı terminaller kesinlikle bağlanmamalıdır. HSM cihazlarında yapılan işlemleri kaydeden fakat konsolu ve ekranı direkt olarak görmeyen kamera sistemi mutlaka ilgili bölümde bulundurulmalıdır ve kamera kayıtları muhafaza edilmelidir [32],[33],[36].

HSM cihazlarının mevcut PCI standartlarına göre FIPS 140-2 seviye 3 veya üstü garanti seviyesine sahip olması gerekmektedir [32].

HSM içinde saklanacak olan anahtarlar belli bir anahtar seremonisi ile üretilmelidir. Seremoni birden fazla kişinin iştirakiyle ve gözetimiyle yapılan bir işlemdir. Üretim

aşamasında anahtar HSM cihazının rastsal sayı üreticiyle rastgele ürettirilmelidir. Oluşturulacak anahtar ideali üç parça (komponent) olmasına rağmen minimum iki parçadan oluşturulmalı ve her parçanın sorumluluğu farklı kişilere verilmelidir [33],[36]. Anahtar üretiminde gerek konsol vasıtasıyla HSM'e değer girilmesi gerekse komponentlerin kâğıda aktarılması gerektiği durumlarda gönderilen ZMK (Zone Master Key) gibi anahtarların açık halleri HSM cihazına konsol yardımıyla veya keypad vasıtasıyla girilmesi gerekmektedir [33],[36]. HSM'in başında her bir anahtar komponent girişinde tek kişi olması sağlanmalı, bir kişinin birden fazla anahtar parçasını görmesi engellenmelidir. ZMK, iki uç arasında güvenli iletişim için zone oluşturmak için gereklidir. Her iki uçta bulunan bu simetrik anahtar ile iletilen mesajların şifrelenmesi ve güvenli hale getirilmesi sağlanmaktadır.

Anahtar üretiminden sonra anahtarların bütünlük kontrolünün yapılmasına imkân sağlayan KCV (Key Check Value) denilen anahtar kontrol değerleri de kayıt edilmelidir. Anahtar kontrol değeri, sıfır ikili değerinin anahtarın 64 bitlik bir dizesi ile 3DES kullanılarak şifrelenmesiyle hesaplanır. Sonuçtaki en soldaki 24 bit, altı basamaklı kontrol değerini oluşturan altı onaltılık basamağa dönüştürülür ve ekranda gösterilerek kayıt edilmesi sağlanır [35].

Üretim (production) ve test ortamları için kesinlikle farklı anahtarlar kullanılmalı ve üretim ortamı için oluşturulmuş bir anahtar hiçbir şekilde test ortamlarında veya başka ortamlarda kullanılmamalıdır. Eğer her iki ortam için üretilen anahtarlar aynı HSM cihazında saklanıyorsa test ortamına da üretim ortamı kadar hassas davranılmalıdır [33].

HSM kullanılarak oluşturulan veya girişi anahtar parça sahipleri tarafından yapılan her bir anahtar için işlem tutanağının hazırlanması, imzalanması ve muhafaza edilmesi yapılacak denetimler için önem arz etmektedir [37]. Her bir işlem için farklı formların bulunması ve gerekli bilgilerin sağlanarak tutanaklı bir şekilde süreçlerin ilerletilmesi sağlanmalıdır. Bunun için personel, form ve prosedür üçlüsü tutanağı gerekli her işlemde net belli olmalıdır.

HSM üstünde ürettirilen anahtarların fiziksel güvenliği büyük önem taşımaktadır. Akıllı karta veya kâğıt üzerine yazılmış anahtarların ve/veya anahtar parçalarının güvenliğinin sorumluluğu anahtar parça sahiplerine (Key Officer) aittir [36]. Bu

sebeple bu görevi üstlenecek kişilere eğitim verilerek bu konuda yeterli farkındalığa ulaşmaları sağlanmalıdır [30].

Akıllı kartlar ve/veya kâğıt üzerine yazılmış bulunan anahtar ve/veya anahtar parçalarını muhafaza etmek için çift anahtarlı (dual control) veya şifresi en az iki parçadan (split knowledge) oluşan kasalar kullanılmalıdır. Burada dikkat edilmesi gereken husus ise akıllı kartlar ve akıllı kartlara ait şifrelerin ayrı ayrı muhafaza edilmesi ve bu muhafaza edilen kasalara erişen kişilerin farklı kişilerden olmasıdır [33],[36].

2.5.3 Anahtarların kullanılması, paylaşılması ve kullanım dışına alınması

Üretilen anahtarların açık yani şifresiz halleri hiçbir şekilde donanımsal güvenlik cihazlarının dışında bulundurulmamalıdır. Sadece gerekli durumlarda en az 2 komponent olacak şekilde ve farklı kişilere emanet edilmiş olarak anahtarlar bir yerden başka bir yere farklı iletişim kanallarından taşınmalıdır.

POS'lar için Terminal Master Key (TMK)'ler manuel olarak üretiliyorsa bu anahtarlar en az iki parça halinde üretilmeli, farklı kanallardan (farklı kargo şirketi gibi) yükleme işlemini yapacak anahtar sorumlularına tutanakla teslim edilmelidir. Terminallerde bulunan TMK, iletişim esnasında kullanılan diğer şifreleme anahtarlarını şifrelemek için kullanılan simetrik bir anahtardır. TMK anahtarının yüklenmesi en az iki farklı kişi tarafından yapılmalı ve bu anahtarlar belli periyot ve/veya işlem adedi sonrasında uzaktan veya güvenli odaya alınarak değiştirilmelidir. Bu anahtar parçalarının ilgili cihaza yüklendikten sonra imha edilmesi (kağıtlar için kâğıt öğütücü cihazlarının kullanılması veya yakılarak imha edilmesi) gerekmektedir. Anahtar parçalarının belli bir süre saklanması gerekiyorsa (anahtar parçasının hepsinin ilgili hedef adrese iletiminin tamamlanmasına kadar saklanabilir) bu anahtarlar, anahtar saklama prosedürüne uygun şekilde güvenli kasalarda ayrı parçalar halinde (dual control) olacak şekilde saklanması gerekmektedir.

Issuer (kart sahibi) bankalar kart kişiselleştirme ve kart basımı gibi hizmetleri ödeme servis sağlayıcı denen firmalardan hizmet alarak tedarik edebilmektedir. Bu işlemler için gereken anahtarların ve kart bilgilerinin bu ödeme servis sağlayıcı kuruluşlar ile

güvenli olarak paylaşmaları gerekmektedir. Burada önemli olan anahtarların güvenli şekilde (kendi personelleri tarafından en az iki parça olarak ya da parçalar halinde farklı kuryeler/kanallar tarafından) iletilmesi ve hedef lokasyondaki konumlanmış HSM cihazlarına anahtarların farklı anahtar sahipleri (key officer) tarafından güvenli terminal makine üzerinden veya HSM cihazına bağlanan keypad vasıtasıyla girilmesi ve bir kişinin anahtarın bütün haline yani anahtarın bütün parçalarına sahip olmamasının sağlanmasıdır [32],[36].

Açık şekilde şifresiz paylaşılan anahtarların muhafaza edilmemesi ve sisteme girildikten sonra imha edilmesi önemlidir. İmha işlemi için bir imha prosedürü olmalı ve ilgili imha prosedürü işletilmelidir.

Atıl duruma düşmüş veya tamir amaçlı olarak güvenli oda dışına alınacak olan HSM üzerinde bulunan anahtarlar ilgili anahtar sahibi gözetiminde, anahtar imha formları doldurularak ve imzalanarak prosedürlere uygun olarak yok edilmelidir.

2.6 Güvenli İşlem Sistemleri ve Metotları

Günümüzde anahtar temelli güvenli işlem ve metotları sıkça kullanılan yöntemlerden biridir. Çeşitli bilgiler ile kurgulanan ödeme sistemleri ve farklı unsurların güvenli işlem için kullanılması günümüzde karşımıza çıkabilecek unsurlar olarak söylenebilir. 2009 yılında alınmış bir patentte ödeme sistemi olarak hesap sunucusu önerilmiştir [38]. Bu ödeme sistemi önerisinde tüketicinin mobil telefon numarası hesap sunucusuna erişim için kullanılmaktadır. Kasiyer işlemi başlattıktan sonra müşteri telefon ve PIN bilgisini girmekte Track 2 (PAN, şifreli PIN, son kullanma tarihi vb) olarak ifade edilen hassas verilerin şifrelenmesi bu girilen telefon ve PIN ile şifrelenmektedir. Şifrelenen data hesap sunucusuna POS ile iletilerek ön yetkilendirme alınması sağlanmaktadır. Öte yandan 2008 yılında alınmış bir patent ile işlem kartlarının dijital imza ile doğrulanması tariflenmektedir. Bir tüketicinin kimliğinin doğrulanması için tariflenen bu buluşta dijital imzalar kullanılarak kimlik doğrulama bir işlem kartı kullanımıyla anlatılmıştır [39]. Bu sistemler ve yöntemler, tüketicilerin işlem bilgilerini özel bir anahtarla dijital olarak imzalamalarını sağlamaktadır. Özel anahtar ile işlemin dijital olarak imzalanması, özel anahtarın bütünlüğünü koruyan barındırılan veya yerel bir sistem aracılığıyla sağlanabilir. Bir

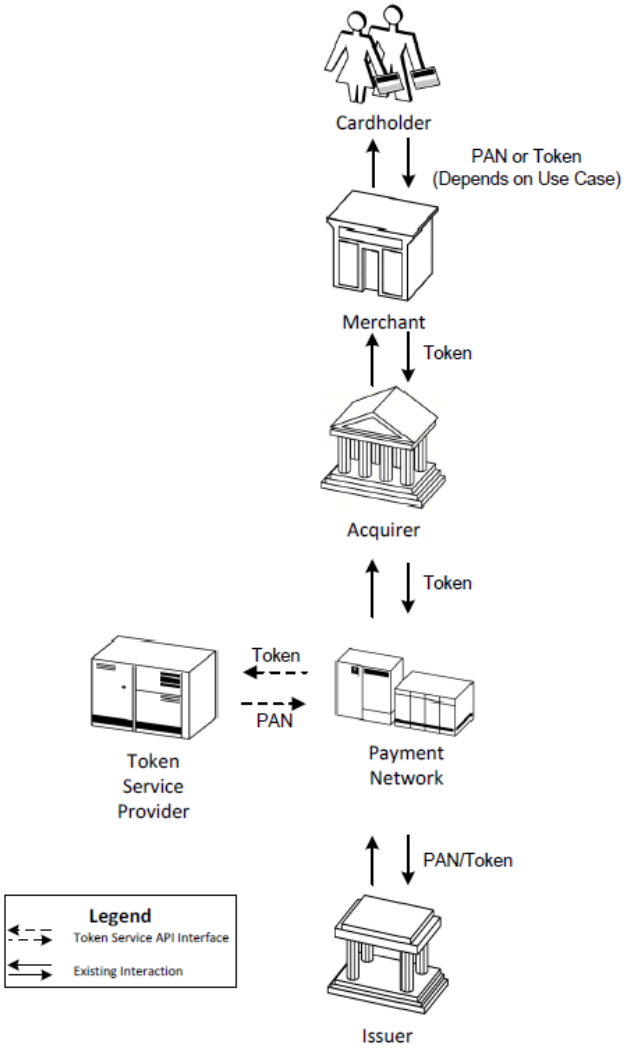
finans kurumu, dijital imzayı açık anahtar ile çözerek tüketici kimliğini doğrulayabilir.

EMV, 2008 yılı itibariyle 730 milyondan fazla kartın dolaşımıyla dünya çapındaki ödemelerde akıllı kart için kullanılan baskın bir protokoldür [40]. EMV, kredi kartı ve banka kartı işlemlerini hem kartın hem de müşterinin varlığını kriptografik kimlik doğrulama kodları, dijital imzalar ve bir PIN girişi kombinasyonu ile doğrulayarak güvenli hale getirir. Çip ve PIN teknolojisi bir önceki manyetik şeritlerin kullanımına nazaran ve önceki lokal akıllı kart ödeme standartlarının aksine ulusal sınırların ötesinde sahtekarlığa karşı büyük bir direnç göstermektedir [41]. Ancak uygulamanın karmaşıklığı ve uygulamanın hatasız olamaması bazı açıklık ihtimallerini beraberinde getirebilmektedir. Yapılan bir çalışmada suçluların bir ödeme yapmak için kartın PIN kodunu bilmeden orijinal bir kart kullanmalarına ve tüccarın bankacılık ağına çevrimiçi bir bağlantıya sahip olsalar bile algılanamamasına sebep olan bir protokol kusuru anlatılmıştır [40]. Sahtekâr kişi, terminali kandırmak için araya girme (man-in-the-middle) saldırısı gerçekleştirmektedir ve karta PIN girilmediğini söylerken terminale ise PIN doğrulandığını inandırmaya çalışmaktadır. Bu tarz saldırıların TSM tarafından kurulacak sertifika temelli işlemlerle engellenmesi ve tespit edilmesi mümkündür.

Bir diğer kaynakta PIN bilgisinin doğrudan karta sağlanamadığından ve arada fiziksel araçlar olduğundan dinlenme olasılığı olduğu ifade edilmektedir [42]. Güvenilir ekranların eksikliğinden yapılan işlemin kimle yapıldığı veya ne kadar yapıldığı bilenemediğinden veri akışının başka bir yöne yönlendirilmesinin mümkün olduğu belirtilmiştir. Eğer EMV işleminde kart bilgisi ve PIN bilgisi POS cihazında yönlendirilebilirse, elde edilen bilginin manyetik şeritli karta yazılarak yurtdışında EMV desteklemeyen terminallerde kullanımının mümkün olacağını belirtmiştir. Bu tarz saldırılar genellikle terminal tarafında yapılan fiziksel saldırılardır. Yapılan bu saldırılarla ilgili birçok POS ekipmanının özellikleri avantajlarıyla ve dezavantajlarıyla sıralanmıştır [42]. Bunlardan bazıları kamera ve ikili okutma, ele geçirilmiş terminal, terminal skimmer ve taklit terminallerdir [42].

Görüldüğü gibi her türlü saldırı bu tarz ödeme sistemlerine yapılabilmektedir. Son iki yıldır bu tarz saldırılardan hassas verilerin korunması için “token” (jeton) mantığı üzerinde durulmaktadır. İlk kez 2014 yılında EMV tarafından yayınlanan Ödeme

Tokenizasyon (Jetonlama) Teknik Altyapısı ile ödeme işlemlerinde hassas veri yerine jeton kullanımına yönelik teknik spesifikasyon tanımlanmıştır [43]. Bu teknik dokümanda bu jeton işlemlerini yürütecek Jeton Servis Sağlayıcılar ifade edilmiştir. Bunun hemen akabinde PCI, Jeton Servis Sağlayıcıların uyumluluk ve değerlendirme raporlarını ve kurallarını belirlemiştir [44],[45]. Bu gelişmelerle ödeme işlemlerinde Jeton Servis Sağlayıcılarla entegrasyon ve kullanımın yakın zamanda olacağı söylenebilir. Resim 2.6'da jeton işlem mimarisi betimlenmiştir.



Resim 2.6 : Ödeme sistemlerinde jeton işlem mimarisi [43].

Tokenizasyon (Jetonlama) ve şifreleme aynı şey midir veya hangisi iyidir sorularını verilecek en iyi cevap ikisinin tamamen birbirinden farklı teknolojiler olduğudur. Çoğu şifreleme araçlarının ve tekniklerinin amacı, orijinal veriyi maskelemek, sonra

da şifrelerin çözülmesini sağlamaktır. Şifreleme, verileri uygun bir anahtara sahip olmayan herkes tarafından okunamayan kılan bir algoritma kullanır.

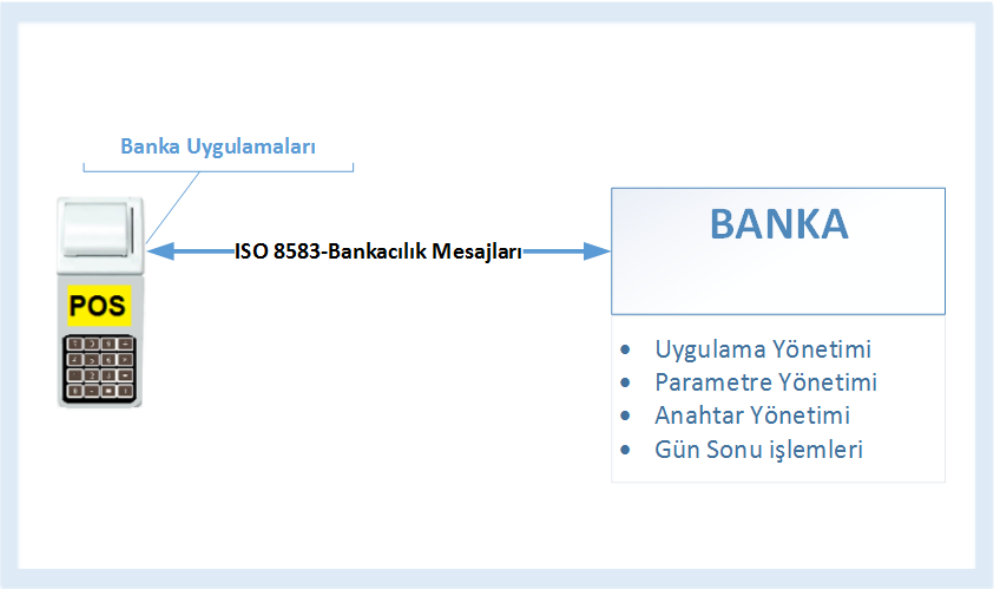
Bazı savunucular, şifrelenmiş kart verilerini bir veritabanında "dinlenme" esnasında okunamadığını ya da bir alım işlemi sırasında "hareket halinde" iken şifreli olduğundan okunamadığını ve bir anahtarın şifresini çözene kadar erişilemiyor olduğundan verileri yakalayan ve çalan bir bilgisayar korsanı (hacker) tarafından elde edilme şansının az olduğunu söyler [46]. Ancak kart verileri, edinen bir bankaya veya ödeme ağ geçidine giden çoklu dahili sistemleri geçerse; şifreleme, şifre çözme ve yeniden şifreleme sürecindeki hatalar dolandırıcılara karşı geniş bir güvenlik açıklığı açabilir.

Birçok şirket jetonlamayı uçtan uca şifrelemeye göre daha ucuz, daha kolay ve daha güvenli olduğunu söylemektedir [46]. Jetonlama, bir şirketin dahili ağlarından kredi kartı verilerini tamamen kaldırır ve benzersiz, üretilen bir yer tutucu veya "jeton" ile değiştirir; bu durum bir hırsızın çalması için hiçbir şeyi olmayan bir depoyu boşaltmak gibidir. Tüccarlar, yalnızca müşterilerin kredi kartı bilgilerini almak, bunlara erişmek veya korumak için jeton kullanır. Bu arada, müşterilerinin gerçek kart verileri çok güvenli ve uzak bir yerde saklanır.

Bir şirketin sistemi herhangi bir şekilde ihlal ediliyorsa, jetonların kendiliğinden anlamı yoktur ve jetonlar suçlulara değersizdir. Jeton rastgele oluşturulur ve orijinal kart numarasını geri alacak herhangi bir algoritması yoktur. Dolandırıcılar, sunuculardan jetonları el koysalar dahi gerçek kredi kartı numarasını tersine mühendislik ile elde edemez [46]. Jetonları kullanmak bir tüccarın ödeme işleme deneyimini de değiştirmez. Tıpkı kredi kartları gibi, jetonlar müşteri satışları, geri ödemeler ve krediler için kullanılabilir - yalnızca satıcı için gerçek kredi kartlarından daha güvenlidirler.

3. YENİ NESİL ÖDEME KAYDEDİCİ CİHAZ ve TRUSTED SERVICE MANAGER

Yeni Nesil Ödeme Kaydedici Cihazlar sadece Trusted Service Manager denilen merkezler üzerinden ilgili birimlere bağlantı kurmalıdır. GİB, bu sayede TSM merkezleri üzerinden ilgili kayıtların izini tutmasını istemiş, yayınladığı GMP (GİB Mesaj Protokolü) spesifikasyonları ile de YN ÖKC ile TSM, TSM ile GİB BS (GİB Bilgi Sistemleri) arasındaki iletişimi tanımlamıştır. GİB bunun dışında YN ÖKC'nin içinde bulunacak POS özelliğinin uluslararası sağlaması gereken standartları belirtmiş, bunun harici bankacılık uygulamalarının yapısı, mesajlaşmaları ve sistemlerine ait kuralları detaylı olarak belirlememiştir. Sadece en son yayınladığı GMP-3 dokümanında yapılan mali işlem ile finansal işlemlerin izini birlikte tutmak için bir başlık yapısı tariflenmiş ve bu başlığın TSM tarafına gönderilmesi ve kaydedilmesi gerekliliği ifade edilmiştir [47]. Bununla birlikte TSM çalışma modeli olarak iki modelin özelliği tariflenmiştir. İleriki bölümlerde bu modeller (kısaca TK1 ve TK2 modelleri olarak adlandırılacaktır) detaylı açıklanacaktır. Normal iletişimde POS cihazları bankaya Resim 3.1'de gösterildiği gibi bağlanmaktadır.



Resim 3.1 : EFT-POS genel çalışma mimarisi.

Bankalar bankacılık işlemlerinde iletişim esnasında uluslararası kabul görmüş ISO 8583 [8] mesaj formatını kullanmaktadır. Terminal yönünden bankalara akan bir akış söz konusudur. Yani banka sunucuları host olarak istemci olan POS terminallerine hizmet vermektedir. İşlem terminal tarafından başlatılır ve terminale dönecek bir mesaj ile sonlanır veya bir sonraki işleme geçilir. Bu yüzden bankalar genel anlamda POS cihazları ile aşağıdaki ana başlıklardaki işlemleri yerine getirmektedir. Kısaca bu işlemler:

- Uygulama Yönetimi
- Parametre Yönetimi
- Anahtar Yönetimi
- Gün Sonu İşlemleri

Bu bölümde YN ÖKC ile TSM için sağlanması gereken anahtar yönetimi hakkında bilgiler aktarılacaktır. Yayınlanan teknik kılavuzlarla [2],[47],[5],[9] GİB'in talep etmiş olduğu bilgiler ve YN ÖKC, TSM ile Gelir İdaresi Başkanlığı Bilgi Sistemleri (GİB BS) mesajlaşma standartları bütünüyle tariflenmiştir. İlgili teknik kılavuzlarda YN ÖKC ile banka haberleşmesinde mesajlaşma standartları belirtilmemiş ama TSM'in sağlaması gereken güvenlik gereksinimleri, ilgili bankacılık mevzuatlarına paralel olarak düzenlenmiştir [48],[49]. Bu çalışma, TSM ile GİB BS iletişiminden yola çıkarak TSM ile banka güvenli iletişimini de içerek şekilde oluşturulmuş bir TSM modelini açıklamaya çalışacaktır.

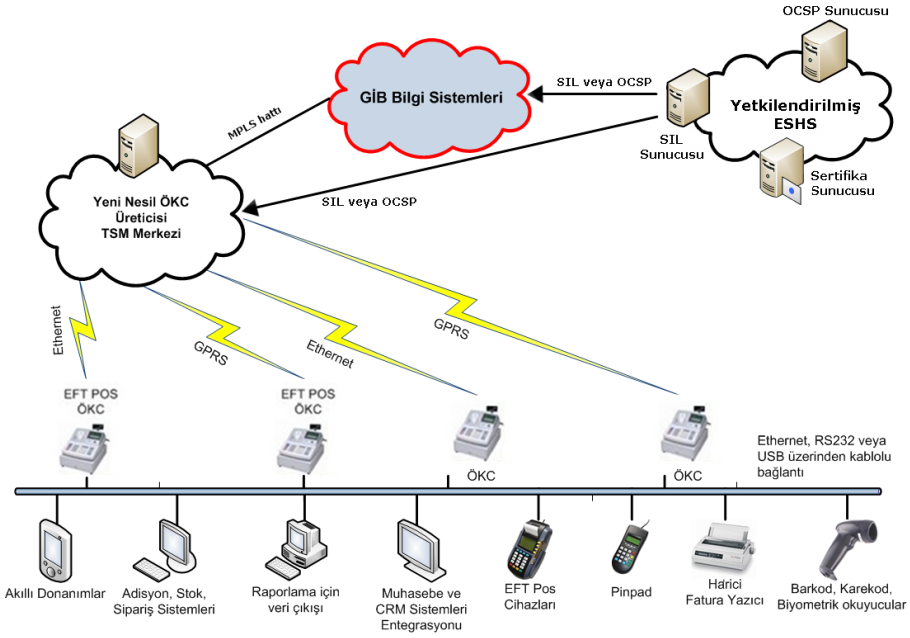
3.1 Sistem Mimarisi

YN ÖKC ve bu cihazlara bağlanabilecek harici donanım ve yazılımlar için, YN ÖKC üreticisi tarafından belirlenen TSM ve Gelir İdaresi Başkanlığı arasında dinamik ve uçtan uca güvenli bir haberleşme alt yapısı oluşturulması hedeflenmiştir. Bu yapı ile hedeflenenler aşağıda maddelendirilmiştir [4],[5]:

- Dış yazılım ve donanımlar ile YN ÖKC arasında işlemlere ilişkin bilgi aktarımı,
- YN ÖKC ile TSM arasında parametre yükleme ve GMP mesajlarının güvenli bir alt yapı ile aktarımı,

- TSM ile GİB arasında parametre bilgileri, Z raporları, satış fişleri, satışlara ait raporlar gibi mali bilgilerin YN ÖKC üzerinde şifrelenmiş hallerinin güvenli bir şekilde aktarımı.

YN ÖKC'lerin GİB, TSM ve diğer yazılım ve donanımlar ile ilgili taraflarla genel haberleşme topolojisi Resim 3.2'de gösterildiği gibi olacaktır [4],[5].



Resim 3.2 : Genel haberleşme topolojisi [4],[5].

3.2 Mesaj Yapısı

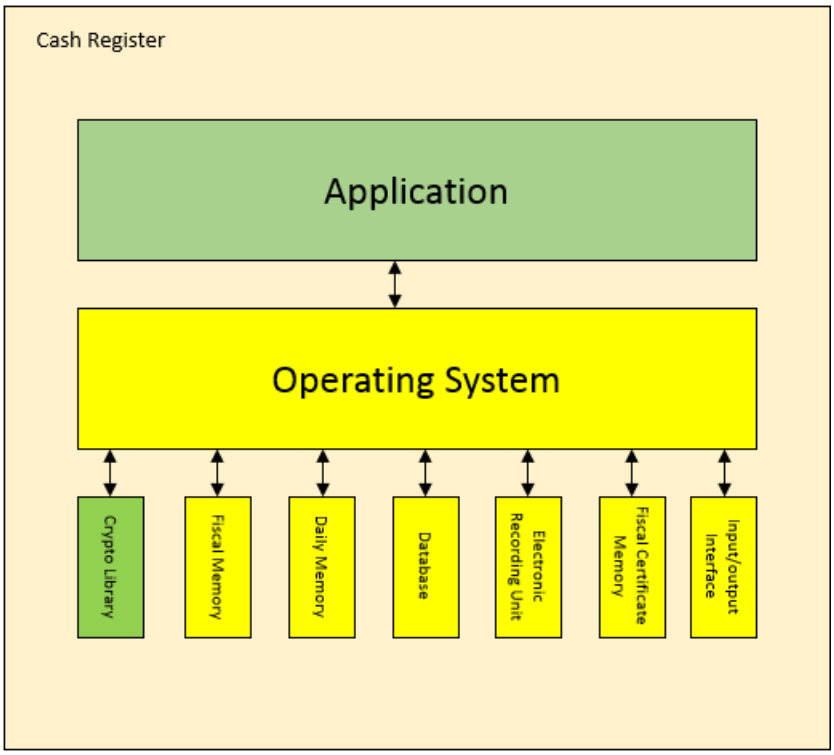
YN ÖKC ile tüm dış haberleşmede TLV (Tag-Length-Value) mesaj formatında GİB Mesajlaşma Protokolü (GMP) kullanılmaktadır. Tüm işlemler bu protokol baz alınarak oluşturulmuş bir yapı kullanılarak yapılmaktadır. Bir mesaj içeriği; her alanın başında içeriğin ne olduğuna ilişkin bir tanımlama alanı (tag), arkasından bir uzunluk bilgisi (length) ve son olarak verinin kendisi (value) yazılarak oluşturulmuştur. Protokolde yer alan mesaj tipleri, mesaj alan grupları ve mesaj alan tipleri her haberleşme bölümü için ayrı ayrı tanımlanmıştır [4],[5].

GİB tarafından belirlenen, gizlilik ve bütünlüğü korunarak iletilmesi gereken veriler, kılavuzlarda ilgili bölümlerde belirtildiği şekilde korunarak güvenli bir şekilde iletilmelidir. Diğer veriler ise açık yani şifresiz olarak iletilebilir. Maksimum paket boyutu 2048 bayt olarak belirlenmiştir. Her paketin başında on altılı formatta iki bayt uzunluğunda paket uzunluğu bilgisi yer alır. Her paketin sonunda bir bayt

uzunluğunda LRC (Longitudinal Redundancy Check) alanı yer alır. Tüm istek ve cevap mesajlarında LRC değeri, mesaj uzunluğu (ilk iki bayt) dışında kalan bütün verinin doğrulama değeridir ve mesajın sonuna eklenir. LRC değeri içeren tüm mesajların yapısı [MESAJ UZUNLUK] + [VERİ] + [LRC] şeklindedir ve LRC değeri sadece [VERİ] ile ifade edilen kısım kullanılarak hesaplanmalıdır [4],[5].

3.3 Yeni Nesil Ödeme Kaydedici Cihaz

Yeni Nesil ÖKC'ler üzerinden yapılan satışlarda, işlemin ilk YN ÖKC'de başlaması ve YN ÖKC'de sonlandırılması esastır [2],[3]. 69 seri no'lu katma değer vergisi mükelleflerinin ödeme kaydedici cihazları kullanmaları mecburiyeti hakkında kanunla ilgili genel tebliğine göre yeni nesil ödeme kaydedici cihazlar, teknik ve fonksiyonel bakımlardan Gelir İdaresi Başkanlığı'nın yayımladığı teknik kılavuzunda [2],[3] belirtilen özelliklere haiz olmalıdır [1]. Temel olarak yazarkasa içeriği Resim 3.3'teki gibi olmalıdır [50].



Resim 3.3 : YN ÖKC teknik mimarisi [9].

Yeni Nesil ÖKC'lerin sahip olması gereken "Temel Teknik Özellikler" bir tablo halinde Çizelge 3.1'de gösterilmiştir [4],[5]. Bu tabloda eski nesil yazarkasalarla farkları da görmek mümkündür.

Çizelge 3.1 : YN ÖKC temel teknik özellikleri tablosu [4],[5].

Temel Teknik Özellikler	Bilgisayar Bağlantılı	EFT-POS Özellikli	Eski Nesil Yazarkasa
1. İşletim Sistemi	X	X	YOK
2. Veritabanı	X	X	YOK
3. Mali Hafıza	X	X	VAR
4. Günlük Hafıza	X	X	YOK
5. Elektronik Mühür ve Yetkli	X	X	YOK
6. Mali Sertifika	X	X	YOK
7. Mali Raporlar	X	X	VAR
8. Elektronik Kayıt Ünitesi	X	X	VAR
9. Olay Kayıt Özelliği	X	X	YOK
10. Fiziksel İletişim Arayüzleri	X	X	YOK
11. Güvenli Veri İletimi	X	X	YOK
12. Erişim Kontrolü	X	X	YOK
13. Kimlik Doğrulama	X	X	YOK
14. Yazılım Güvenliği	X	X	YOK
15. Güvenlik Garantisi (gerekli sertifikasyonlara uyumluluk)	X	-	YOK
16. Harici EFT-POS/PinPad Uyumu (EFT-POS özelliği olan ÖKC'lerde harici EFT-POS veya PinPad bağlantısı olmayacaktır)	X	-	YOK
17. Barkod/Karekod Okuyucu, Sipariş Cihazları Uyumu	X	X	YOK
18. PCI (3.0) veya Üstü Güvenlik	-	X	YOK
19. EMV Sertifikaları	-	X	YOK
20. Kasiyer ve Müşteri Göstergesi	X	X	VAR
21. Klavye Ünitesi	X	X	VAR
22. Dâhili Pil (Zaman bilgisini aktif tutmak için)	X	X	YOK
23. Dâhili Batarya (Uzun süreli	İ	İ/X*	YOK
24. Stok & Muhasebe Entegrasyonu, Perakende Otomasyonu ve Bilgisayar Bağlantısı	İ	İ	YOK
25. Ödeme Sistemleri ve Entegrasyonu	İ	İ	YOK
26. Grup Kampanya, Kupon, Promosyon vb. Uygulamalar	İ	İ	YOK
27. ÖKC Yazıcısı	X	X	VAR

Tabloya göre değerler: (X=Zorunlu, İ=İhtiyari, - = Yoktur).

Çizelge 3.1'de kırmızı ile işaretlenmiş olarak görüldüğü gibi, eski nesil yazarkasalarda olmayan ama YN ÖKC için gerekli güvenli iletişim, sertifikasyon ve güvenlik parametreleri önemli bir hale gelmiştir. 3.3.1 ve 3.3.2 bölümlerinde bu maddelerden önemlileri kısaca değinilecektir.

3.3.1 Mali sertifika

Yeni Nesil ÖKC'lere ilk kurulum esnasında yetkilendirilmiş ESHS (Elektronik Sertifika Hizmet Sağlayıcısı) tarafından sağlanmış sayısal sertifika güvenli odada yüklenmelidir. Bu yüklenmiş sertifika ile cihaz kimlik doğrulama işlemi, Yeni Nesil ÖKC'lerin sahada kullanım süresinin kontrolü ve GMP teknik dokümanlarında belirtilen diğer kontroller yapılmaktadır [2],[3]. Bu mali sertifika, açık anahtar altyapısı sisteminden üretilmiştir. Mali sertifika ve ilgili özel anahtarı, cihaz içerisindeki elektronik ve fiziksel olarak korunmuş güvenli bir alanda (TPM) veya akıllı kart içerisinde saklanır [2],[3].

Yeni Nesil ÖKC'lere yüklenecek sertifikalar yetkilendirilmiş ESHS tanımında [2],[3] belirtildiği üzere; TÜBİTAK Kamu SM'den temin edebileceği gibi, GİB tarafından yetkilendirilmiş sertifika otoritesinden de temin edilebilir. Bu sertifika, GİB tarafından yetkilendirilmiş ESHS olarak belirlenmiş kurum tarafından cihaza özel üretilir.

TÜBİTAK Kamu SM harici bir sertifika otoritesinin GİB tarafından "Yetkilendirilmiş ESHS" olarak kabulü için; bu sertifikaların üretim, dağıtım ve sonrasında yönetimini gerçekleştirmek üzere kurulan ya da kurulacak olan ve sertifika üretmek için gerekli donanım ve yazılım altyapısına Payment Card Indıustry (PCI) Security Standards Council (SSC) tarafından yayınlanmış ve yürürlükte olan PIN Güvenlik gereksinim dökümanında tariflenen anahtar yükleme tesisine, güvenlik cihazlarına ve onaylanmış algoritmalara uyduğunu Visa PIN Security programı kapsamında VISA tarafından akredite olan "Visa Approved PIN Security Assessors (PIN SA)" kuruluşları aracılığı ile denetlettirmeli ve olumlu sonuç raporunu sunmalıdır. Bununla birlikte bu kurulan sertifika otorite merkezlerinin tüm fiziksel ve operasyonel birimlerinin "Türkiye Ülke Sınırları" içerisinde bulunması ve gerektiğinde GİB tarafından da denetlenebilir olması zorunludur [2],[3]. İleriki bölümlerde sertifika konusu detaylı şekilde açıklanacaktır.

3.3.2 Güvenli veri iletimi

Yeni Nesil ÖKC'ler önce TSM Merkezi sonra GİB BS ile olacak şekilde haberleşir. Güvenli veri alışverişi aşağıdaki kurallar çerçevesinde yapılır [2],[3]:

a) TSM merkezleri, YN ÖKC'leri yönetimini, her işlemde terminalden gelen GMP mesaj bilgilerinin format ve doğruluğunu değerlendirme, değişmezliğinin ve bütünlüğünün kontrolünden sorumludur.

b) Yeni Nesil ÖKC'ler ile GİB BS iletişiminde taşınan hassas veriler şifreleme mekanizması kullanılarak korunur.

c) Yeni Nesil ÖKC'ler, yetkilendirilmiş ESHS tarafından sağlanan ve cihaza güvenli odalarda yüklenmiş sayısal sertifikaları kullanarak kimlik doğrulama, şifreli haberleşme ve veri bütünlüğü kontrolü yapar. Sertifika kontrolünün başarısız olduğu durumlarda cihazın işlem yapması TSM merkezi tarafından engellenmeli ve bu durum GİB BS'ye bildirilmelidir.

3.4 Trusted Service Manager (TSM)

GİB Bilgi Sistemlerine veri aktarma, dokümanlarda [4],[5] detaylı şekilde tanımlandığı gibi TSM Merkezleri üzerinden olacaktır. Tanımlanmış bu mimari yaklaşıma göre daha önceki POS dünyasında arada bulunmayan TSM, bütün trafiği üzerinde taşıyan ve iletişimi sağlayan bir mimaride çalışmaktadır. Bu rolle TSM, GİB tarafından kendisine biçilmiş görev ve sorumlulukları sağlarken YN ÖKC'lerin yönetimini de üstlenen bir role getirilmiştir. YN ÖKC'ler TSM ile güvenli iletişimde aynı zamanda Ortak Kriter Koruma Kılavuzuna uygun şartları [9] da sağlamalıdır. Bu gereksinim idare tarafından hazırlanan Ortak Kriterler Dokümanına göre YN ÖKC firmaları tarafından yerine getirilir [49].

GİB BS, YN ÖKC ve Üretici TSM merkezleri arasındaki haberleşmede uyulacak temel kurallar aşağıda ifade edilmiştir [2],[3]:

- GİB Bilgi Sistemleri, YN ÖKC ve Üretici TSM merkezleri arasındaki haberleşme GMP'ye (Gelir İdaresi Başkanlığı Mesajlaşma Protokolü) uygun olarak yapılacaktır.

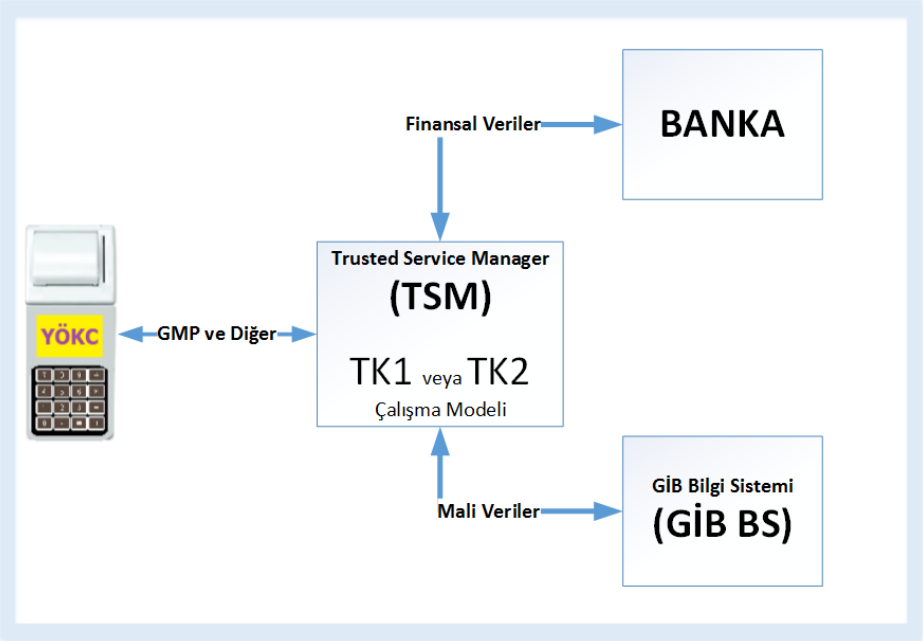
- YN ÖKC ile TSM arasında güvenli haberleşme alt yapısı sağlanmalıdır. TSM ile GİB BS arasında ise iletişim güvenli kiralık data hat üzerinden yapılmalıdır.

- YN ÖKC'den GİB Bilgi Sistemlerine iletilen verilerde güvenlik sağlanacak, GİB Bilgi Sistemleri dışında herhangi bir yerde veri depolama, farklı yere yönlendirme işlemi yapılmayacaktır.

TSM olarak adlandırılan merkezler; "YN ÖKC'lere yazılım-parametre yükleme, güncelleme, bu cihazları 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, YN ÖKC mesajlarının GİB BS ve üye işyeri anlaşması yapan kuruluşlara GMP'lerde belirlenen iletişim protokolleri çerçevesinde aktarılmasını sağlama amacıyla YN ÖKC üreticileri tarafından veya bir Dış Hizmet Sağlayıcısı (DHS) tarafından kurulmuş terminal yönetim merkezi"ni ifade eder [2],[3]. TSM Merkezleri YN ÖKC üreticileri için münhasıran kurulmuş donanım, yazılım ve işletimi içermelidir [2],[3]. TSM Merkezi iletişim esnasında sistemi üzerinden bankacılık verisi de geçirdiği için çeşitli uluslararası standart ve sertifikasyonları da sahip olmalıdır. TSM, bağımsız firmalar tarafından gerçekleştirilecek düzenli sızma testleri ile bilgi güvenliği standardına uygun işletildiği raporlanmış olmalıdır [49]. Bununla birlikte PCI DSS (Payment Card Industry Data Security Standard) onaylı [32] ve dolayısıyla POS terminalleri için tanımlanmış PIN anahtar güvenliği gereksinimlerini [33] de sağlıyor olmalıdır. TSM alt yapısı içinde sistemde kurulan uygulama sunucuları her YN ÖKC üreticisi için ayrı bir fiziki ve/veya sanal ortamlarda kurulmalıdır [49]. Kurulan bu fiziki ve/veya sanal ortamlar sadece YN ÖKC alt yapısına hizmet vermeli ve PCI-DSS kriterlerine uygun şekilde yapılandırılmalıdır.

TSM altyapısında kullanılan veritabanı sunucularına ait veriler her YN ÖKC üreticisi için kendisine ait disk gruplarında barındırılmalıdır [49]. Böylelikle herhangi bir olumsuz durumda bu disklerin kolayca alınabilmesi ve sistemden çıkarılabilmesi mümkün olması istenmiştir. Bir TSM Merkezi birden fazla YN ÖKC üreticisi için TSM merkezi olarak çalışabilir. Ancak sistem münhasırlığı sağlandığı müddetçe bu çalışmaya izin verilmektedir. Yani yukardaki bölümlerde bahsettiğimiz gibi fiziksel

ve/veya sanal olarak birbirinden izole olabilecek şekilde işletilmelidir. Genel anlamda TSM haberleşme mimarisi Resim 3.4'teki şekilde sunulmuştur.



Resim 3.4 : TSM haberleşme mimarisi.

TSM merkezleri YN ÖKC haricinde en temel olarak iki uca daha bağlıdır: Bankalar ve GİB Bilgi Sistemleri. Bankalarla iletişimde finansal veriler taşınırken, GİB iletişiminde mali veriler taşınmaktadır. Dolayısıyla her iki dünyanın anahtar yönetimi tabi oldukları mevzuat ve standartlara göre farklılık göstermektedir. Anahtar yönetimi bölümünde bu farklılıklar bahsedilecektir.

GİB'in yayınladığı teknik kılavuzlara göre [2],[3] TSM iki modelde çalışabilmektedir: TK1 (Teknik Kılavuz 1'e tabi model) ve TK2 (Teknik Kılavuz 2'ye tabi model). TSM, iki model olan Teknik Kılavuz 1 (TK1) ve Teknik Kılavuz 2 (TK2) çalışma modellerinden birinde uyumlu olarak çalışmalıdır. Her ne kadar TSM, tanım olarak her iki modelde [2],[3] aynı şekilde tanımlanmış olsa da yapısal olarak bazı farklı işleyişlerde ve özelliklerde olmaya yatkındır. Teknik kılavuzlarda tanımlanmış bu iki modele göre farklılıklar ön plana çıkartılacak ve bu çalışmada önerilecek olan TSM modeli için güvenlik altyapısı açıklanacaktır.

3.4.1 TK1 TSM

Teknik Kılavuz 1'e tabi olan TSM'lerde haberleşme, YN ÖKC ile TSM arasında SSL CA tünel oluşturulması ve bu sayede hattın güvene alınması ile başlar. Verilerin, TSM üzerinden GİB bilgi sistemlerine özel güvenli ağ üzerinden güvenli bir şekilde iletilmesiyle haberleşme sonlanır. Güvenli haberleşme altyapısı olarak YN ÖKC ile TSM arasında TLS v1.2 protokolü kullanılmaktadır [2],[4]. Bu modelde çalışan TSM, geleneksel bankacılık mesajlaşma altyapısını çok değiştirmeden GİB'in TSM'den istediği zorunlu bilgileri ve izleri tutmaya odaklı olduğu söylenebilir. TSM merkezleri YN ÖKC üzerinde bankacılığa ait güvenli anahtar yönetimini, banka uygulaması yazılım ve parametrelerini kendisi kontrolü sağlamak kaydıyla bankanın müdahil olmasıyla veya tamamen kendisi yapabilir. Bu yaklaşımla TK1, bankanın daha kolay müdahil olduğu ve geleneksel yaklaşıma daha yatkın bir model olduğu söylenebilir. TK1 modeli, şeffaf olarak araya girerek bankacılık mesajlarında yönlendirme akışı sürdürürken diğer talep edilen zorunlu altyapıları da GİB BS için sağlar niteliktedir.

3.4.2 TK2 TSM

Teknik Kılavuz 2'ye tabi olan TSM'lerde YN ÖKC ile TSM arasında TLS v1.2 protokol kullanım zorunluluğu yoktur. Ancak YN ÖKC ile TSM arasında güvenli ve kapalı bir haberleşme alt yapısı kurulması istenmektedir. YN ÖKC üreticisi ve dolayısıyla TSM, bu güvenliği sağlamaktadır [3],[5]. Bu modelde çalışan TSM'ler genelde YN ÖKC trafiğini kendi üzerinde sonlandırıp Banka ve GİB BS sunucularına ayrı bir işlem hattı üzerinden terminal gibi davranarak çeşitli bağlantı ve iletişim altyapıları kurarak işlemleri sağlamaktadır. Dolayısıyla TSM yazılım kontrolü ve diğer kontroller konusunda daha rol alıcı hüviyette çalışabilmektedir.

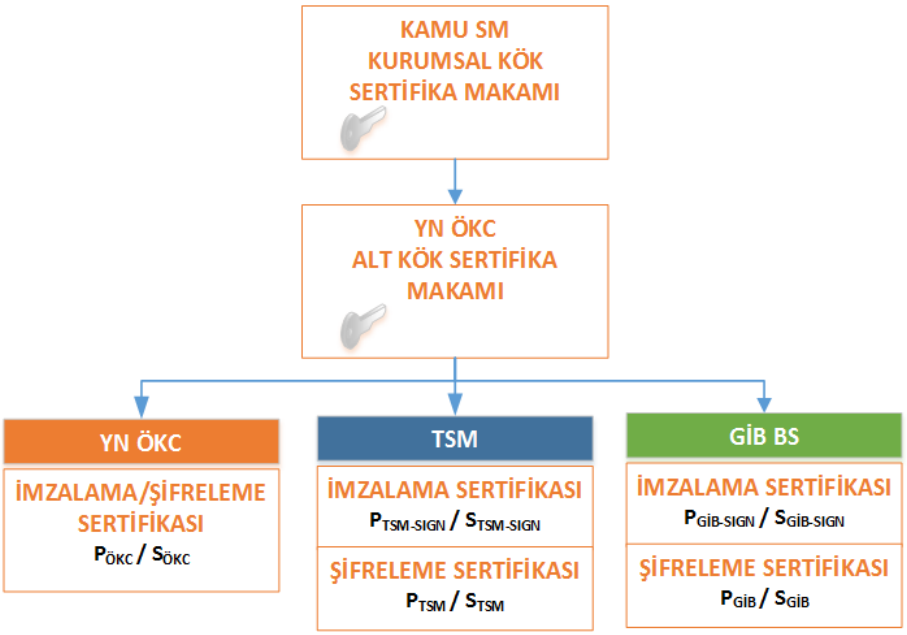
3.4.3 TK1 ile TK2 karşılaştırması

TK1 için TK2'den farklı olarak sistemde kullanılan kriptografik algoritmaların tanımlarının ve kullanım şekillerinin yanısıra anahtar ve parametrelerinin üretim yöntemlerine ve mesajlarına yönelik farklılıklar bulunmaktadır. TK2 modelinde TLS v1.2 kullanım zorunluluğu olmadığından bu anahtar değişimine ait GMP mesajları eksiktir. Diğer durumlarda GİB açısından GMP mesaj formatları dahil TSM'lerin

çalışma mantığı Teknik Kılavuz 1 ve 2'de birbirine benzerdir. Bankacılık uygulamaları ise yukarıdaki bölümlerde ifade edildiği gibi nasıl isteniyorsa o şekilde yapılması mümkündür. GİB, finansal uygulamaların nasıl olacağıyla ilgilenmemektedir. TK1 çalışan TSM merkezlerinde imzalama ve şifreleme sertifikaları gibi ayrım olmadan tek bir sertifika bulunmaktadır. Her iki çalışma modelinde TSM ile GİB BS arasındaki iletişim aynıdır.

3.5 Sertifikalar ve Sertifika Mimarisi

Sayısal Sertifika Koruma Kılavuzu ve Teknik Kılavuzlarda [4],[5],[51] ifade edildiği gibi YN ÖKC'lere ilk kurulum esnasında ITU X.509 formatı ile uyumlu sayısal sertifikalar güvenli odalarda yüklenmektedir. Bu sertifikalar cihaz kimlik doğrulama, YN ÖKC'lerin saha kullanım süresini belirleme, GİB BS ve TSM Merkezi ile güvenli haberleşme için gerekli kontrollerde kullanılır. YN ÖKC için elektronik sertifikalar, GİB tarafından yetkilendirilmiş ESHS (bu makale hazırlandığı sırada sadece TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi yetkilidir) tarafından YN ÖKC üreticisine sertifika yaşam döngüsü kılavuzuna [4],[5] uygun olarak teslim edilerek cihaza özel üretilmektedir. Asimetrik anahtar çiftleri için üretilen sertifikaların doğrulama zincirindeki kök sertifika otoritesi Kamu SM olduğu durumda sertifika hiyerarşisi Resim 3.5'teki gibidir.



Resim 3.5 : Yetkilendirilmiş ESHS sertifika otoritesi yapısı.

Mali işlemler için kullanılan sertifikalar her bir uç için yukarıdaki şekilde gösterilmiş Sertifika Otoritesi mimarisinden sağlanmaktadır. GİB Hassas YN ÖKC Verisi; YN ÖKC'lerden TSM Merkezi'ne, TSM Merkezi'nden GİB BS'ye, yetkilendirilmiş ESHS'ye ait kriptografik anahtarlarla şifrelenerek iletilen ve ancak GİB BS'de açılabilen, Z raporu, fiş bilgileri, fiş iptal mesajları, kurulum ve anahtar değiştirme mesajları vb. bilgileri ifade eder [48]. Bu tanıma göre GİB BS'ye taşınan hassas veriler TSM tarafından sadece iletilmeli, kayıt izi tutulmalı ve TSM tarafından içeriği görülememelidir.

YN ÖKC'lere anahtarlar ve anahtarlara ait sertifikalar, GİB ile TÜBİTAK tarafından denetlenmiş ve güvenlik seviyesi belirlenmiş özel yerler olan güvenli odalarda [41] yüklenmelidir. Sistemdeki bütün mali sertifikalar kısaca aşağıda tanımlanmıştır [52].

- Kamu SM Kurumsal Kök Sertifikası (Üst Kök): Sertifika zinciri doğrulama işlemlerinde gereklidir. Bu sertifika self-signed (kendi kendini imzalamış) sertifika olarak güven unsurunun en tepesinde bulunmaktadır. Hiyerarşi olarak bu sertifikanın altından üretilmiş tüm sertifikalar bu sertifika ile zincir olarak doğrulanır.

- YN ÖKC Kök Sertifikası (Alt Kök): Üst kök tarafından imzalanmış olan bu sertifikada sertifika zinciri doğrulama işlemlerinde kullanılmaktadır.

- YN ÖKC Sertifikası: GİB BS ve TSM ile kurulacak olan bağlantılarda kimlik doğrulama ve cihazın saha kullanım süresinin kontrolünün yapılabilmesi için kullanılır. YN ÖKC'lerin onaylanmış saha kullanım süresi GİB tarafından 10 yıl olarak belirlenmiştir. Onaylanmış saha kullanım süresinin kontrolü sertifikanın geçerlilik süresi aracılığı ile yapılmaktadır. Depo süreside düşünülerek bu sertifikaların geçerlilik süreleri Kamu SM tarafından 11 yıllık olarak sağlanmaktadır.

- TSM İmza Sertifikası ($P_{TSM\text{-}SIGN}$): TK1 TSM çalışma modeli için TLS haberleşmesinde ve GİB tarafından imzalanmış parametrelerin doğrulanması için kullanılır. İlk kurulum sırasında cihaza yüklenmezse iletişim anında TSM tarafından online olarak gönderilebilir. TK2 TSM çalışma modeli için ise bu sertifika TSM ile şifreleme anahtarının paylaşımı esnasında imza doğrulaması

amacıyla ve diğer imza doğrulamaları için kullanılır. Bu sertifikaların ömrü en fazla üç yıl olacak şekilde sunulmaktadır.

- TSM Şifreleme Sertifikası (P_{TSM}): Bu sertifika anahtar paylaşımı esnasında anahtarları şifrelemek için kullanılır. Bu sertifikaların ömrü en fazla üç yıl olacak şekilde sunulmaktadır.
- GİB İmza Sertifikası ($P_{GİB\text{-}SIGN}$): Bu sertifika şifreleme anahtarının paylaşımı esnasında imza doğrulaması için gereklidir. Bu sertifikaların ömrü en fazla üç yıl olacak şekilde sunulmaktadır.
- GİB Şifreleme Sertifikası ($P_{GİB}$): Bu sertifika GİB BS ile şifreleme anahtarının paylaşımı esnasında anahtarı şifrelemek için kullanılır. YN ÖKC'ler bu sertifika anahtarını kullanarak ürettikleri "Terminal Random Master Key-TRMK" anahtarını şifreleyerek GIB-BS'ye iletmektedir. Bu sertifikaların ömrü en fazla üç yıl olacak şekilde sunulmaktadır.

Mali işlemler için kullanılması gerekli olan bu sertifika yapısı ve anahtarlar, finansal işlemler için kullanılamamaktadır. Çünkü finansal işlemler için kullanılan anahtarları üreten/yöneten kurumun (sertifika otoritesi olmasına gerek yoktur) PIN Security standartları gereğince Visa tarafından denetlenmesi gerekmektedir. Bu yüzden henüz Kamu SM tarafından sağlanan anahtarlar ve sertifikalar, Kamu SM PIN security kapsamında denetlenmediği için finansal işlemler için kullanılamamaktadır. Bu yüzden TSM merkezleri finansal işlemler için ayrı bir anahtar/sertifika yapısını kullanmaktadırlar. Bölüm 3.3.1 Mali Sertifika bölümünde kısaca "Yetkilendirilmiş ESHS" tanımı yapılmıştır. Teknik kılavuzlara göre ESHS (Elektronik Sertifika Hizmet Sağlayıcısı); "Yeni Nesil ÖKC'lere, YN ÖKC TSM Merkezlerine ve GİB BS'ye yüklenecek sertifikaların üretimini, dağıtımını, yönetimini ve denetimini gerçekleştirecek kurum (TÜBİTAK Kamu SM) ya da GİB tarafından yetkilendirilmiş sertifika otoritesi olan kurum" olarak ifade edilmektedir [2,3]. Dolayısıyla ileriki yıllarda finansal işlemler için kurulan/kurulacak olan sertifika otoritesinin GİB tarafından yetkilendirilmiş sertifika otoritesi olması durumunda bu anahtar yapısı hem mali hem de finansal işlemler için ortak kullanılabilir olacaktır. Bu çalışmada finansal işlemler için önerilen sertifika otoritesi anahtar yapısı bu iki ihtiyacı tek bir otorite birleştirecek nitelikte olacaktır.

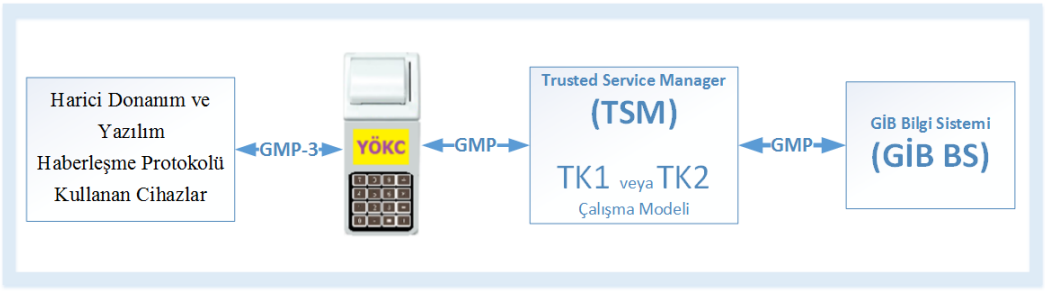
3.5.1 Sertifikaların doğrulanması

Yeni Nesil ÖKC içerisinde bulunan ve kurulum esnasında güvenli odada yüklenen mali sertifikaların güvenli bir şekilde korunması önemlidir. Bu kapsamda cihaz içerisinde bulunan sertifikaların kullanılmadan önce sertifika doğrulama işleminden geçirilmesi gerekmektedir.
Sertifika doğrulama işlemi esnasında ana başlıklar olarak aşağıdaki maddelerin kontrol edilmesi gerekmektedir [52].

1. Elektronik sertifikanın format (X509), yayıncı, anahtar kullanım alanı, geçerlilik süresi, subject alanı vb. kontrollerinin yapılması.
2. Kök sertifikadan YN ÖKC sertifikasına kadar tüm sertifika zincirinin imza kontrolünün yapılması.
3. Sertifika üzerindeki imzanın doğrulanması

3.6 Gelir İdaresi Başkanlığı Mesajlaşma Protokolü

Gelir İdaresi Başkanlığı Mesajlaşma Protokolü (GMP), hem TK1 hem de TK2 TSM çalışma modeli için ayrı ayrı tanımlanmıştır. Teknik kılavuzlarla GMP-TK1 ve GMP-TK2 olarak adlandırılan bu mesajlar mali işlemler ve diğer yönetsel işlemler için kullanılmaktadır. Daha önceki bölümlerde GMP'nin TLV mesaj yapısına sahip olduğu belirtilmişti. GMP hem YN ÖKC ile TSM hem de TSM ile GİB BS arasında kullanılabildiği gibi YN ÖKC ile harici cihazla ve yazılımlarla haberleşme protokolü [47] olarak da kullanılmaktadır. Resim 3.6'da bu haberleşme mimarisi sunulmuştur.



Resim 3.6 : GMP haberleşme mimarisi.

Protokolde haberleşmenin yapılacağı uçlardan bağımsız olarak ortak mesaj yapıları belirlenmiştir. Bu sayede verinin taşınma esnasında herhangi bir çevrime tabi tutulmasına gerek kalmamış ve verinin uçtan uca hiç değiştirilmeden taşınması

hedeflenmiştir. Yapı esnek bir taban üzerine oturtulduğu için genişletilmesi her zaman için mümkündür.

YN ÖKC-TSM paket iletişim genel yapısı çizelge 3.2'deki şekilde tanımlanır [4],[5].

Çizelge 3.2 : YN ÖKC-TSM paket iletişim genel yapısı.

Uzunluk	TPDU					Terminal Seri No	Mesaj	LRC
0x0000-0xFFFF	0x60	0xXX	0xXX	0xXX	0xXX	12 Bayt	Mesaj içeriği	1 Bayt

TSM-GIB paket iletişim genel yapısı çizelge 3.3'teki şekilde tanımlanır [4],[5].

Çizelge 3.3 : TSM-GIB paket iletişim genel yapısı.

Uzunluk	TPDU					Mesaj	LRC
0x0000-0xFFFF	0x60	0xXX	0xXX	0xXX	0xXX	Mesaj içeriği	1 Bayt

YN ÖKC tarafından gönderilen mesajlarda TPDU alanını takiben Terminal Seri No bilgisi yer almaktadır. Bu çalışmada aynı YN ÖKC üreticisinin farklı TSM modellerinde çalışabilir cihazlarını bu alan kullanarak ayrıştırmamız mümkündür. 4. Bölümde TK1 ve TK2 TSM çalışma modelinde ayrıştırmada bu konu detaylandırılacaktır.

3.7 TSM Güvenlik ve Anahtar Yönetimi

TK1 ve TK2 TSM modelinde anahtarlar farklılık göstermektedir. TK1 TSM modelinde SSL sertifikaları varken TK2 TSM modelinde her bir iş (imzalama ve şifrelenmiş) için iki ayrı amaçlı uç sertifikası bulunmaktadır. Bu farklılıklarla anahtar yönetimi anlatılmaya çalışılacaktır.

YN ÖKC'lerin GİB bilgi sistemlerine bağlanmasında aktarılacak verilerin güvenliğinin sağlanması ve veriyi üreten/gönderen YN ÖKC'nin GİB tarafından tanınabilmesi amaçları ile şifreleme için GİB'e ait şifreleme açık anahtarını ($P_{GİB}$) içeren GİB şifreleme sertifikası ve TSM'e ait şifreleme açık anahtarını (P_{TSM}) içeren TSM şifreleme sertifikası, imzalama işlemi için ise GİB'e ait imzalama açık anahtarını ($P_{GİB\_SIGN}$) içeren GİB imzalama sertifikası ve YN ÖKC'ye ait şifreleme özel anahtarını ($S_{ÖKC}$) içeren YN ÖKC şifreleme sertifikası olmak üzere dört adet sertifikanın YN ÖKC üreticisi tarafından güvenli odada YN ÖKC'ye yüklenmesi gerekmektedir [5]. Her ne kadar GİB BS sertifikaları sonradan üretilmiş olmasına

rağmen sahada daha önceden bulunan YN ÖKC içerisinde bulunan kök sertifikaların mevcudiyetinden dolayı uzaktan bu sertifikalar yüklenebilir. Zaten 10 yıllık YN ÖKC ekonomik ömründe, sertifika süreleri maksimum üç yıl olan GİB ve TSM sertifikalarının en az dört kez uzaktan yenilenerek yüklenmesi gerektiği anlaşılmaktadır.

3.7.1 Anahtar açıklamaları ve güvenlik gereksinimleri

YN ÖKC tarafından GİB ve TSM ile güvenli haberleşebilmek için anahtar üretimi yapılmaktadır. GİB iletişimi için TRMK anahtarı ve TSM iletişimi için ise TRMKD anahtarı YN ÖKC güvenli belleğinde üretilir.

GİB ve TSM üzerinde üretilen anahtarlar ise HSM kullanılarak üretilmektedir. GİB HSM'de; TREK, TRAK ve LMK simetrik anahtarları üretilir. TSM HSM'de ise; TDK ve LMK (TDK) simetrik anahtarları üretilir. TDK şifreleme dışındaki tüm simetrik şifreleme işlemleri için AES-256 algoritması kullanılmaktadır [4],[5].

Kamu SM ya da GİB tarafından yetkilendirilmiş başka bir sertifika otoritesi üzerinden GİB BS için, her bir TSM için ve her bir YN ÖKC için asimetrik kriptografik anahtar çiftleri (açık anahtar ve özel anahtar) üretilir, yenilenir ve SİL kontrolleri yapılır. GIB-BS için imzalama/doğrulama ($S_{GİB\text{-}SIGN}/P_{GİB\text{-}SIGN}$) ve şifreleme/çözme ($S_{GİB}/P_{GİB}$) amaçlı kullanılmak üzere iki çift anahtar gerekmektedir. Aynı şekilde TSM'ler için de imzalama/doğrulama ve şifreleme/çözme amaçlı iki anahtar çifti bulunur. YN ÖKC'ler için ise imzalama/doğrulama amaçlı bir anahtar çifti bulunur. Anahtarları üreten GİB tarafından yetkilendirilmiş sertifika otoritesi her public anahtar için sertifika vererek anahtar yönetimini yapmaktadır. Aynı zamanda, düzenli periyotlarda Sertifika İptal Listesi (SİL) yayınlanır [4],[5].

Terminal açık anahtarlarının geçerlilik kontrolü, yukarıda belirtilen periyodik SİL kontrolünün yanı sıra GİB sistemi üzerinde de her mesaj için kontrol edilecektir. Sistemde kayıtlı olan tüm açık anahtarlar, GİB HSM'in LMK anahtarı altında şifreli olarak GİB BS veritabanında saklanmaktadır. Sistemde tanımlanan anahtarların saklanacağı taraflar çizelge 3.4'teki tabloda belirtilmektedir [5].

Çizelge 3.4 : Mali haberleşme sistemi anahtar tablosu [5].

ANAHTAR	**YN ÖKC**	**TSM**	**GİB BS**
GİB-Şifreleme Açık ($P_{GİB}$)	X	X	X
GİB-Şifreleme Özel ($S_{GİB}$)			X (GİB in sahip olduğu HSM'de)
GİB-İmzalama Açık ($P_{GİB\_SIGN}$)	X	X	X
GİB-İmzalama Özel ($S_{GİB\_SIGN}$)			X (GİB in sahip olduğu HSM'de)
TSM-Şifreleme Açık (P_{TSM})	X	X	X
TSM-Şifreleme Özel (S_{TSM})		X (TSM in sahip olduğu HSM'de)	
TSM-İmzalama Açık (P_{TSM_SIGN})	X	X	X
TSM-İmzalama Özel (S_{TSM_SIGN})		X (TSM in sahip olduğu HSM'de)	
YN ÖKC-İmzalama Açık ($P_{ÖKC\_SIGN}$)	X	X	X (GİB DB'de)
YN ÖKC-İmzalama Özel ($S_{ÖKC\_SIGN}$)	X		
ESHS-Kök Açık (ESHS Kök Sertifikası)	X	X	X
TREK	X		X (LMK_{GIB} altında DB'de)
TRAK	X		X (LMK_{GIB} altında DB'de)
TDK	X	X (LMK_{TSM} altında DB'de)	
LMK_{GIB}			X (GİB in sahip olduğu HSM'de)
LMK_{TSM}		X (TSM in sahip olduğu HSM'de)	
TRMKD	X(Geçici)	X (Geçici)	
TRMK	X(Geçici)		X(Geçici)

Yukarıdaki bölümlerde bahsedildiği gibi TK1 TSM modelinde bazı anahtarlar eksiktir. O modelde güvenli haberleşme için TLS kullanıldığından, TDK ve TRMKD anahtarları TK1 TSM modelinde bulunmamaktadır. Bu anahtarlar, TK2 TSM modelinde verileri şifrelemek için kullanılan anahtarlardır. YN ÖKC ile TSM

arasında veri güvenliği TLS v1.2 ile sağlanmaktadır. Bu yüzden veri şifrelemesi için bu anahtarlar kullanılmaz.

Sistemde kullanılan ama detaylı açıklanmamış anahtarlar bu bölümün alt bölümlerinde aktarılacaktır [5].

3.7.1.1 Terminal random master key (TRMK)

TRMK 256 bitlik bir AES anahtar olup, YN ÖKC ile GİB arasındaki anahtar yükleme mesajı akışında rastgele olarak YN ÖKC tarafından üretilir. Bu anahtar $P_{GİB}$ ile şifreli bir şekilde TSM üzerinden GİB BS'ye taşınır. GİB BS bu anahtarı kullanarak kimlik doğrulama ve şifreleme amacıyla kullandığı diğer anahtarları (TRAK ve TREK) şifreler ve YN ÖKC' ye gönderir. TRMK anahtarı, anahtar değişim işlemi esnasında kullanılan geçici bir anahtar olup kullanım süresi boyunca YN ÖKC içerisinde yer alan güvenli bölgede tutulur. Bu anahtar, hiçbir zaman ve şekilde GİB bilgi sistemleri tarafından saklanmaz. Anahtar değişim işlemi sonrası bu anahtar GİB BS'den ve YN ÖKC'den silinir [4],[5].

3.7.1.2 Terminal random master key for data (TRMKD)

TRMKD 256 bitlik bir AES anahtar olup, YN ÖKC ile TSM arasındaki anahtar yükleme mesajı akışında rastgele olarak YN ÖKC tarafından üretilir. Bu anahtar P_{TSM} ile şifreli bir şekilde TSM'e gönderilir. TSM bu anahtarı kullanarak TDK anahtarını şifreler ve YN ÖKC' ye gönderir. TRMKD anahtarı, YN ÖKC ile TSM arasındaki anahtar değişim işlemi esnasında kullanılan geçici bir anahtar olup kullanım süresi boyunca YN ÖKC içerisinde yer alan güvenli bölgede tutulur. Bu anahtar hiçbir zaman ve şekilde TSM tarafından saklanmaz. Anahtar değişim işlemi sonrası bu anahtar TSM'den ve YN ÖKC'den silinir [5].

3.7.1.3 Terminal data key (TDK)

TDK 256 bitlik bir AES anahtar olup, TSM'de bulunan HSM tarafından ilklendirme mesajı gönderen her cihaz için üretilir. YN ÖKC'den TSM'ye (ya da TSM'den YN ÖKC'ye) taşınacak olan mesajların şifrelenmesi/çözülmesi bu simetrik anahtar kullanılarak yapılır. YN ÖKC'den TSM'e gönderilen istek mesajları TDK ile şifreli olarak TSM'ye aktarılır. TSM'den YN ÖKC'ye gelen cevap mesajını da TSM yine

TDK ile şifreleyerek ilgili YN ÖKC'ye iletir. TDK anahtarı, YN ÖKC içerisinde yer alan güvenli bölgede tutulur. Cihazın tamper duruma düşmesi durumunda bu anahtarlar anında silinir. TSM veritabanında da ilgili TSM'in LMK'sı altında şifrelenerek saklanır [5].

3.7.1.4 Terminal random encryption key (TREK)

TREK 256 bitlik bir AES anahtar olup, GİB bilgi sistemlerinde bulunan HSM tarafından üretilir. YN ÖKC ile GİB BS arasında güvenli taşınması gereken veri grupları veya alanların şifrelenmesi amacı ile kullanılacak olan anahtardır. YN ÖKC üzerinden gönderilen anahtar yükleme istek mesajına cevaben GİB BS üzerinde oluşturulmaktadır. TREK anahtarı, YN ÖKC içerisinde yer alan güvenli bölgede tutulur. Cihazın tamper duruma düşmesi durumunda bu anahtarlar anında silinir. Bu anahtar, GİB veritabanında GİB'in LMK'sı altında şifrelenerek saklanır [4],[5].

3.7.1.5 Terminal random authentication key (TRAK)

TRAK 256 bitlik bir AES anahtar olup, GİB bilgi sistemlerinde bulunan HSM tarafından üretilir. Terminal veya GİB tarafından gönderilen verilerin SHA-256 özetlerinin şifrelenmesi ve mesaja eklenmesi ile mesaj bütünlüğünün sağlanması amacı ile kullanılmaktadır. YN ÖKC üzerinden gönderilen anahtar yükleme istek mesajına cevaben GİB BS üzerinde oluşturulmaktadır. TRAK anahtarı, YN ÖKC içerisinde yer alan güvenli bölgede tutulur. Cihazın tamper duruma düşmesi durumunda bu anahtarlar anında silinir. Bu anahtar, GİB veritabanında GİB'in LMK'sı altında şifrelenerek saklanır [4],[5].

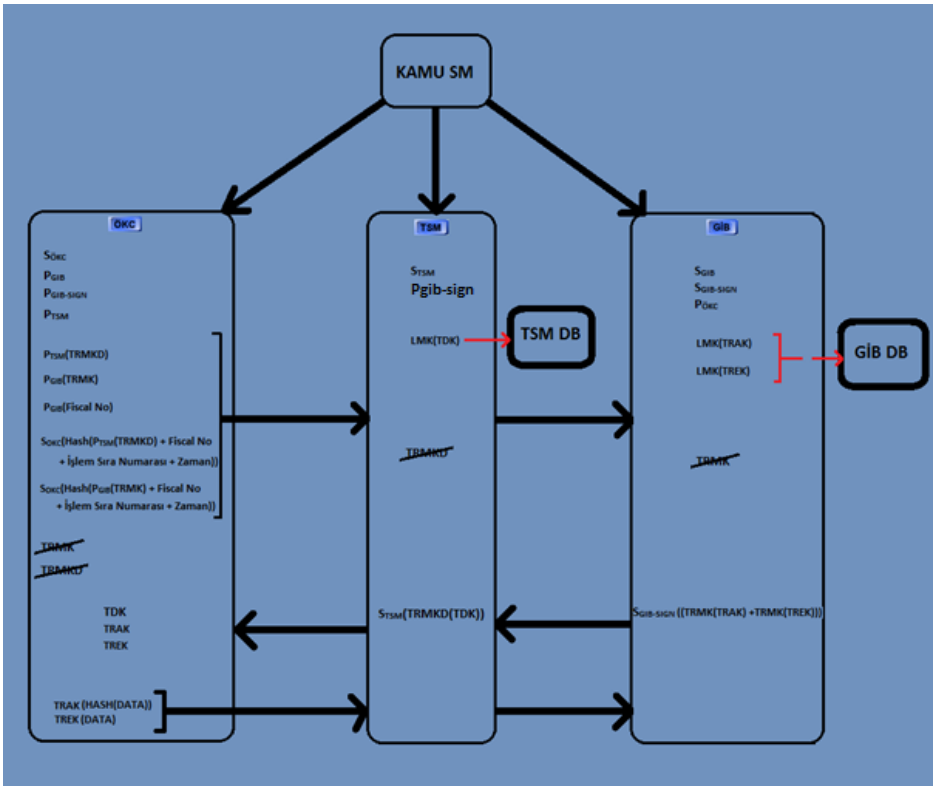
3.7.1.6 Local master key (LMK)

LMK 256 bitlik bir AES anahtar olup, GİB BS'de ve TSM'de bulunan HSM'ler tarafından üretilir ve HSM'lerde saklanır. GİB HSM'de üretilen LMK, her bir YN ÖKC için farklı olacak şekilde üretilen TRAK ve TREK anahtarlarının veya ihtiyaç halinde başka anahtarların GİB veritabanına şifreli yazılabilmesi amacı kullanılır. TSM HSM'de üretilen LMK ise yine her bir YN ÖKC için farklı olacak şekilde üretilen TDK anahtarlarının veya ihtiyaç halinde başka anahtarların TSM veritabanına şifreli yazılabilmesi amacı ile kullanılır. LMK anahtarı sadece HSM'de

saklandığından LMK altında şifrelenmiş olan TDK, TRAK ve TREK anahtarlarının veritabanına yazılması güvenlik zafiyetine neden olmayacaktır.

3.8 YN ÖKC, TSM ve GİB BS Online Anahtar Yükleme

Anahtarların saklanma ve değişim durumu Resim 3.7'de sunulmuştur [4],[5].



Resim 3.7 : Anahtar mimarisi [4],[5].

YN ÖKC anahtar yaşam döngüsü [4],[5] ve işlemler çizelge 3.5'te sunulmuştur. Bu çizelgedeki anahtar değişimlerine göre YN ÖKC – TSM ile TSM – GİB BS arasında güvenli mesajlaşma mümkün hale gelmektedir. Öncesinde uçlar kendi anahtar değişimlerini yapmış ve doğrulama için kendisinde barındırmış olmalıdır. Tabloda her bir blok içindeki işlem ikili mesaj arasındaki süreçte gerçekleştirilmektedir.

GİB mesajlaşmasında (GMP ile) TDK; TREK ve TRAK anahtar işlemlerin şifrelenmesinde kullanılır. Bu anahtarlar ilgili uçların veritabanında Local Master Key (LMK) anahtarı altında saklanırlar. LMK anahtarı ilgili uçların (TSM veya GİB BS) HSM cihazlarında saklanır. Böylelikle GMP mesajları uçlar arasında güvenli bir şekilde taşınır ve yönetilir.

Çizelge 3.5 : Online anahtar yükleme.

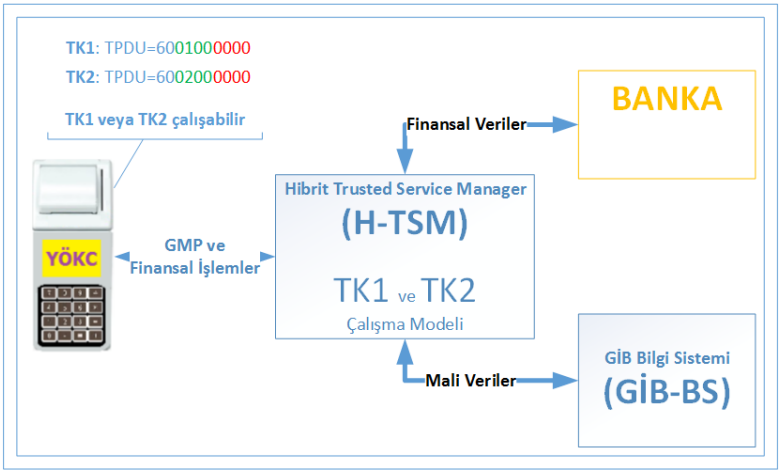
İşlem	***Açıklama***	***Kaynak***	***Hedef***
YN ÖKC - TSM Anahtar Yükleme			
Üretim	Terminal Random Master Key for Data TRMKD	YN ÖKC	-
Istek	P_{TSM}(TRMKD), $S_{ÖKC}$ [işlem verisi]	YN ÖKC	TSM
Üretim	Terminal Data Key - TDK	TSM	-
Saklama	Local Master Key - LMK (TDK)	TSM	TSM DB
Cevap	TRMKD (TDK), $S_{TSM-SIGN}$[TRMKD(TDK)]	TSM	YN ÖKC
YN ÖKC - GİB BS Anahtar Yükleme			
Üretim	Terminal Random Master Key (TRMK)	YN ÖKC	-
İstek	P_{GIB}(TRMK), $S_{ÖKC}$ [işlem verisi]	YN ÖKC	GİB BS
Üretim	Terminal Random Authentication Key - TRAK ve Terminal Random Encryption Key - TREK	GİB BS	-
Saklama	LMK(TRAK) ve LMK(TREK)	GİB BS	GİB BS DB
Cevap	TRMK(TRAK), TRMK(TREK), $S_{GİB-SIGN}$[işlem verisi]	GİB BS	YN ÖKC

Not: Parantez (..) içerisinde kullanım, ilgili isimle adlandırılmış anahtarın parantez dışındaki isimli anahtarla şifrelenmiş olduğunu belirtmektedir. Örneğin LMK(TDK) ile TDK'ın LMK ile şifrelendiği belirtilir. Köşeli parantezli [..] gösterim ise ilgili isimle adlandırılmış anahtarın köşeli parantez dışındaki isimli anahtar ile imzalanmış olduğunu belirtmektedir. Örneğin $S_{ÖKC}$ [işlem verisi] ile işlem verisinin $S_{ÖKC}$ anahtarı ile imzalandığı anlaşılmalıdır.

4. TÜMLEŞİK VE HİBRİT TSM

Önceki bölümlerde aktarıldığı gibi GİB tarafından yayınlanmış teknik kılavuzlara göre iki model olarak TSM merkezleri çalışabilmektedir. Detaya girilmeksizin incelendiğinde bu iki modelin birbirinden çok farklı olmadığı ve mali işlemler için hibrit bir TSM modelinin tasarlanmasının mümkün olduğu görülmektedir. Ancak TSM sadece GİB BS ile iletişim halinde değildir, bankalarla da iletişim halinde olma durumu söz konusudur. Bunun için de kendi içerisinde bir ekosistemi barındırıyor olması finansal işlemler için uygun olacaktır.

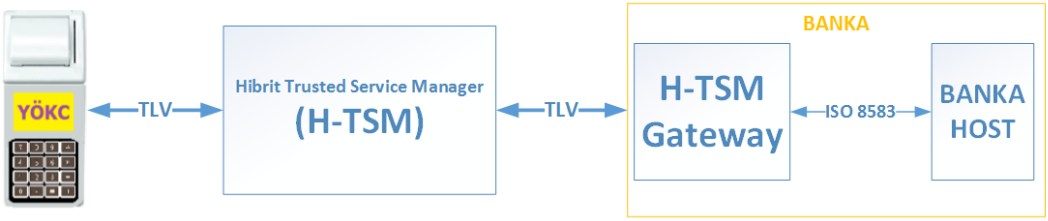
TSM merkezlerinin her bir YN ÖKC üreticisi için sistem münhasırlığını sağlaması gerekmektedir. Bir TSM merkezi fiziksel ve/veya sanal sistem ayrımını sağladığı müddetçe istediği kadar YN ÖKC üreticisinin TSM merkezi olabilmektedir [36]. Ancak bir YN ÖKC firması hem TK1 hem de TK2 TSM altyapısına uygun çalışabilir modelleri ve/veya bankacılık uygulamaları mevcutsa, önerilen bu H-TSM ile daha etkin ve az maliyetli olarak GİB tarafından zorunlu hale getirilmiş yazarkasa POS pazarında bir ayrıcalık kazanabilir. Çünkü aynı YN ÖKC üreticisinin mali işlemlerin iletimi için sistem münhasırlığını sağlamasına gerek olmayacaktır. Tek bir TSM modeli ile bu ihtiyacını çözebiliyorsa bir tane daha TSM altyapısı kurmasına gerek olmayacaktır. İşte bu ihtiyaçlar çerçevesinde Resim 4.1'deki gibi H-TSM modeli tasarlanmıştır.



Resim 4.1 : H-TSM mimari yapısı.

4.1 H-TSM Çalışma Modeli

Oluşturulacak H-TSM modelinin PCI-DSS [32] ve PIN güvenlik gereksinimlerini [33] karşılayacak güçlü bir anahtar yönetim mekanizmasını sağlaması esnek ve tümleşik bir TSM merkezinin kurgulanmasına salık verecektir. Öte yandan bankacılık uygulamalarında mesajlaşma için kullanılan ISO 8583 mesaj formatında bankaya özel alanların (reserved) her bankada farklı kullanılması bu mesaj formatında farklı ek işlemleri yapan tek bir formatı mümkün kılamamaktadır. Dolayısıyla anahtar yönetimi dahil birçok işlemde mesaj standardının yakalanması pek kolay olamamaktadır. Bankalar temel olarak 4 grupta POS işlemlerini yürüttüğü söylenebilir. Bunlar bankacılık işlemleri, yazılım ve parametre yükleme/güncelleme işlemleri, gün sonu işlemleri ve anahtar yönetim işlemleridir. Ancak yazarkasa POS ile araya giren TSM merkezinden dolayı bu işlemleri TSM'e devretmesi veya TSM bilgisi dahilinde dolaylı yönetmesi gerekecektir. Dolayısıyla yeni geliştirmelerin yapılması ve bu YN ÖKC dünyasına uyarlanması gerekecektir. Tüm bu ihtiyaçlar çerçevesinde GMP'de de kullanılmış olan TLV mesaj iletişim yapısıyla işleyen Resim 4.2'deki gibi bir H-TSM çalışma modeli önerilmektedir. TLV, GMP mesaj yapısında kullanılan bir yapı olduğundan kurgulanan bu modeldeki TSM ekosistemi için tek tip bir mesaj sistemi olacaktır.



Resim 4.2 : H-TSM haberleşme yapısı.

Bu yapıya göre banka lokasyonunda konumlandırılan, YN ÖKC bankacılık parametre yönetimini ve ISO 8583 mesajlaşma formatını [8] iki yönlü olarak TLV mesaj formatına dönüştüren bir TSM gateway düşünülmüştür. Böylelikle YN ÖKC-Banka arasında şeffaflığı sağlayacak ve aynı zamanda yönetimi kolaylaştıracak kendi yaşam ekosistemi oluşturulmuş olacaktır. Geleneksel POS mimarisine yatkın olan bankacılık uygulamalarının ise ISO 8583 formatındaki mesajlarının uçtan uca TLV olarak taşınması ve hem TSM gateway tarafında hem de YN ÖKC üzerinde koşan

bankacılık uygulamalarıyla haberleşecek küçük dönüştürme uygulamalarıyla sağlanacaktır. Yani TK1 TSM modeline ihtiyaç duyan ama YN ÖKC mevzuatlarına uymak zorunda olan eski bankacılık uygulamalarında TLV mesaj tipinde anahtar yönetimi tesis edilirken, TK2 TSM modeline yatkın ve yeni bankacılık yazılımları yazılacak YN ÖKC'ler içinde TSM gateway üzerinde TLV-ISO mesaj dönüşümleri yapılacaktır. Böylelikle eski ve yeni altyapının tek bir mimaride birleşmesi ve güçlü bir anahtar yönetim sistemi kullanması mümkün olabilecektir.

TK1 ile TK2 TSM modelinin en bariz farkı olan TLS v1.2'nin YN ÖKC ile TSM arasında tesis edilmesiyle hibrit TSM merkezinin desteklenmesi ve TLV tipinde bankacılık mesajlaşma altyapısının birleştirilmesi mümkün olacaktır. Bu hibrit TSM modeli mevzuatlar ve teknik kılavuzlarla kendisi için tanımlanmış sorumlulukları, bankanın banka uygulaması tarafında müdahilinin az veya fazla olmasına bakılmaksızın esnek ve tümleşik olarak sağlar niteliktedir.

Bankacılık sisteminde kullanılan cihazların anahtar yönetimini yön veren kuruluşlar ve uluslararası standartlar POS cihazlarında güçlü bir anahtar yönetiminin olmasını istemektedirler. Bunun için bankaların POS dünyasında uzaktan anahtar yükleme (RKL - Remote Key Loading) mekanizmalarını kurması ve anahtar değişim yönetimini sağlaması zorlanmaktadır. Mevcut POS'larda sertifika temelli güçlü bir anahtar yönetim alt yapısının olmadığı Bölüm 2.5'te bahsedilmiştir. Bu yüzden her bir bankanın geçmek zorunda olduğu güçlü anahtar yönetiminin bankaların altyapısından dolayı zor ve uzun vadeli olduğu görülmektedir.

Resim 4.3'te gösterilen bu mimari yapıda, banka POS dünyasında kendisinin yaptığı işlemleri yine yapabilir olacaktır. Ancak anahtar yönetimini H-TSM, bankanın altyapısına bakmaksızın TSM ekosistemi içerisinde güçlü bir şekilde yapabilecektir. Banka kendi anahtar yönetimini banka tarafında konumlandırılan H-TSM Gateway ile, basit veya güçlü anahtar yönetimi ne olursa olsun herhangi mesaj formatlı olarak devam edebilir olacaktır. H-TSM Gateway banka içerisinde olduğu için bankanın basit anahtar yönetimi yapması sorun teşkil etmeyecektir. H-TSM bu haberleşmenin üstüne bir katman daha güçlü bir anahtar mekanizması sağlayarak TLV formatında güvenli iletişim altyapısını YN ÖKC ile sağlayacaktır. Böylelikle her bankada farklılık gösteren anahtar yönetimi daha güvenli bir yapıyla desteklenecek ve PCI DSS ile PIN güvenliği standartlarını karşılar nitelikte olmuş olacaktır.

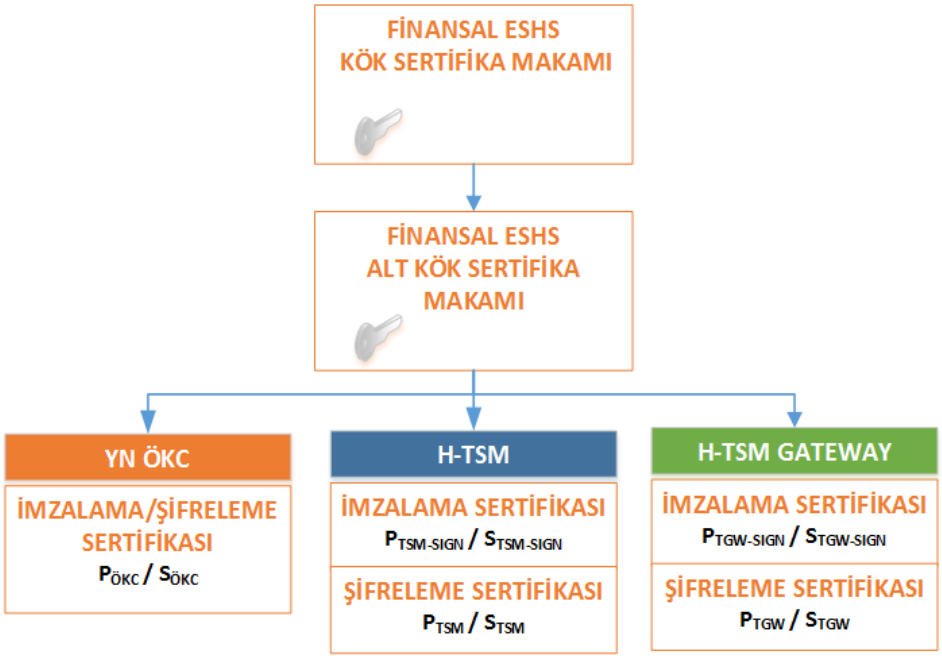
Resim 4.3 : H-TSM çalışma yapısı.

GMP protokolünün mesaj yapısı Bölüm 3.6'da kısaca anlatılmıştır. YN ÖKC ile TSM arasında kullanılması öngörülen TPDU değeri, TK1 ve TK2 çalışma modeli seçiminde mesaj bazında ayrım için kullanılacaktır. Toplam beş bayt olarak tanımlanan ve her GMP mesajında olan bu başlık sayesinde gelen mesajdan hangi modelde çalışan TSM'in seçimini yapmak mümkün olacaktır. Örneğin TK1 çalışan TPDU olarak 6001000000 gönderirken, TK2 ise 6002000000 gönderecektir. Bu yöntemle birlikte GMP ile modellerin tümleştirilmesi ve birleştirilmesi mümkün hale gelmiş olacaktır.

4.2 Finansal Elektronik Sertifika Hizmet Sağlayıcısı

Anahtar yönetimi ve kullanım yöntemleri mali işlemler için GMP teknik klavuzlarında [2],[3],[4],[5] detaylı şekilde açıklanmıştır. Kullanılan anahtarlar ve sertifikalar yetkilendirilmiş ESHS tarafından verilmektedir. Ancak yetkilendirilmiş ESHS'lerin finansal işlemler için kullanılması anahtarı sağlayan ve yönetimini yapan kuruluşun PIN Güvenliği kapsamında VISA tarafından akredite olan "Visa Approved PIN Security Assessors (PIN SA)" kuruluşları aracılığı ile denetlettirmesi ve olumlu sonuç raporunu alması durumunda finansal işlemler için kullanılabilir. Aksi takdirde başka bir anahtar yönetiminin kurulması ve bu denetimden olumlu sonuç raporunun alınması gerekir. Şu anki anahtarlar ve sertifikalar TÜBİTAK Kamu SM tarafından sağlanmaktadır ve bu kurumun bahse konu olan olumlu sonuç raporuna sahip olmamasından dolayı yeni bir finansal elektronik sertifika hizmet sağlayıcısının kurulması gerekliliği vardır. Bir başka husus ise Visa'nın sertifikalar için en fazla beş (bazı durumlarda üç) yıllık bir süre belirlemesidir. Ancak YN ÖKC için verilen sertifikalar daha önceki bölümlerde de belirtildiği gibi YN ÖKC ekonomik ömrü kadar yani 10 yıllıktır. Hatta Kamu SM, depo süresini de düşünerek 11 yıl süreli YN ÖKC sertifikası vermektedir. Sertifika sürelerinden dolayı finansal işlemler için

kullanılacak asimetrik anahtarlar mecburen terminaller için farklı olmak durumundadır. Kurulacak olan yeni sertifika otoritesi, mali sertifika otoritesine benzer şekilde Resim 4.4'teki gibi bir yapıda olması önerilmektedir.

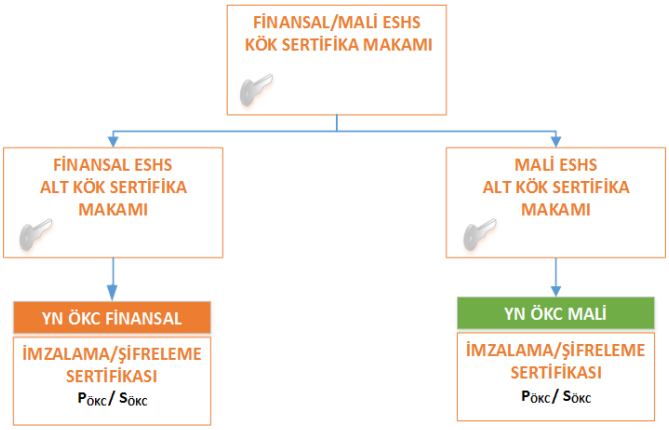


Resim 4.4 : Finansal ESHS sertifika otoritesi yapısı.

PCI-DSS isterlerine uygun olarak hassas verilerin terminalden bankaya kadar uçtan uca şifreli ve TSM merkezlerinin de göremeyeceği bir şekilde taşınıyor olması gerekir. Bunun için H-TSM Gateway ucu da ayrı bir host gibi sertifikalandırılacaktır. H-TSM Gateway tamamen bankanın kontrolünde olan ve anahtarların yönetimini bankaya sunan bir alt yapıda olacaktır. Sertifikalandırma, PCI-DSS kriterlerine uygun olan sertifika otoritesi olmak koşuluyla finansal ESHS tarafından yapılabilir. Yeni bir uç olarak her bir banka içinde konumlanan TSM Gateway için bu yeni sertifika otoritesinden üretilen sertifikalar, YN ÖKC ile H-TSM sertifikalarının oluşturulduğu kök zincirinden üretilebilir.

Finansal işlemler için sertifikalar üreten finansal ESHS eğer GİB tarafından yetkilendirilmiş ESHS olarak tanınması durumunda hem mali hem de finansal işlemler için kullanabilir. Bu durumda her ne kadar aynı anahtarlar bütün uçlar için her türlü mesaj tipi için kullanabilir olsa da YN ÖKC ekonomik ömrü mali sertifikaya bağlı olduğundan (en az 10 yıl geçerli sertifika) ve finansal sertifikalar bunu sağlayamayacağından belki iki farklı alt kökü Resim 4.5'te gösterilmiş yapıdaki gibi ayırmak mümkün olabilir. Resim 4.5'te sertifika otoritesi yapısında bu hibrit

yapı gösterilmiştir. Onun harici diğer uçların sertifikaları finansal ESHS Alt Kök Sertifika Makamı tarafından en fazla geçerlilik tarihi üç yıl olacak şekilde verilebilir.



Resim 4.5 : Hibrit ESHS sertifika otoritesi yapısı.

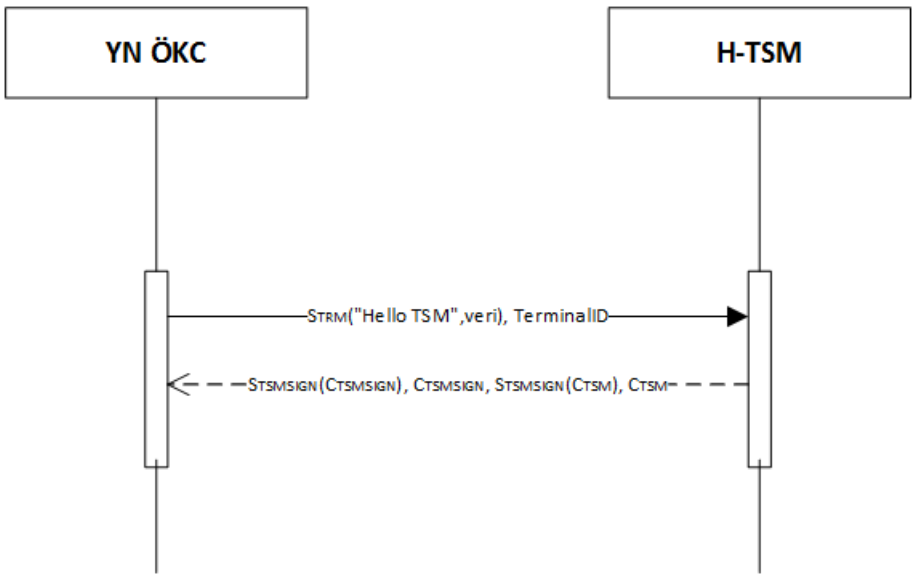
4.3 Anahtar Yönetimi

Önerilen modelde her bir uç finansal ESHS tarafında sertifikalandırılacaktır. Anahtar yönetimi açık anahtar altyapısına uygun yönetilecektir. Sertifika otoritesinden verilen sertifikalar için mali sertifika otoritesindeki amaçlarla aynı tipte anahtarlar sertifikalandırıldığı için birlik olması açısında aynı tarzda kısa isimlendirme kullanılmıştır. Anahtar gösterimlerinde kullanılan ana harfler şunlardır: "P" İngilizcede "Public" (Açık) kelimesinin kısaltması olarak, "S" İngilizcede "Secret" (Gizli) kelimesinin kısaltması olarak ve "C" İngilizcede "Certificate" (Sertifika) kısaltması olarak gösterilmiştir.

4.3.1 İlk kurulumlar

YN ÖKC için anahtarlar ve ilk sertifikalar güvenli odada yüklenmelidir. Güvenli odada YN ÖKC'ye ait açık anahtarlar ($P_{ÖKC}$, $S_{ÖKC}$) ve sertifikası ($C_{ÖKC}$) yüklenir. Bununla birlikte güvenli odada bütün zincir kök sertifikaları da yüklenir. Güvenli odada anahtarları yüklenen tüm terminallerin (YN ÖKC) seri numarasıyla sertifikaları H-TSM veritabanında kullanımından önce kaydedilmelidir. GİB yayınladığı YN ÖKC aktivasyon kılavuzuna göre [53] cihazda aktivasyon işlemi yapabilmek için YN ÖKC'ye ait sertifika bilgilerinin GİB BS'de var olmasını beklemektedir. İşte bu bilgilerin TSM'e bildirilmesi esnasında bütün sertifika bilgileri üretimden sonra belirlenen yöntemlerle TSM'e iletilir ve TSM veritabanına

kaydedilir. Aynı şekilde finansal sertifikalar da YN ÖKC aktif edilmeden evvel H-TSM'e iletilmelidir. YN ÖKC ile H-TSM ilk haberleşmesinde Şekil 4.1'de gösterildiği gibi anahtar değişimi yapar ve YN ÖKC, H-TSM'e ait sertifikaları alır ve güvenli alanına kaydeder.

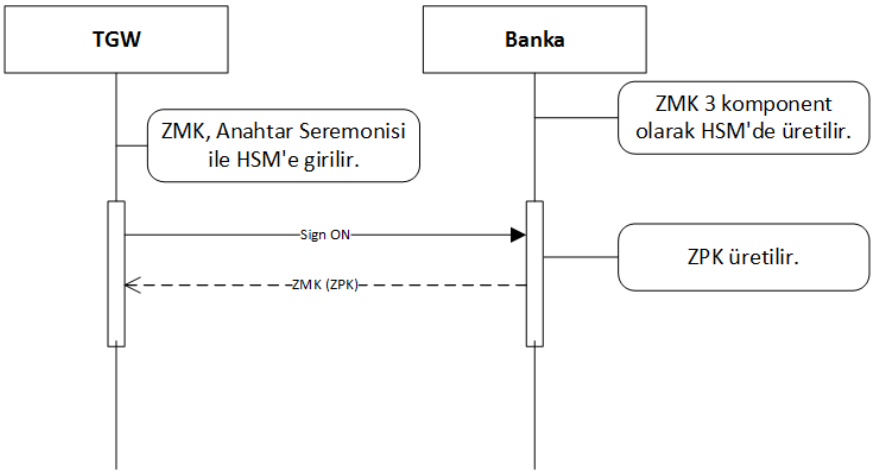


Şekil 4.1 : YN ÖKC – TSM arasında TSM sertifika yükleme.

H-TSM Gateway ilk kez bankaya kurulurken banka hostu ile güvenli iletişim için ZMK yüklemesi yapılması gerekmektedir. Bölüm 2.5'te anlatıldığı gibi bankalar güvenli anahtar paylaşımında bu güvenli alanı oluşturmak için ZMK anahtarını kullanır. ZMK, üç komponent olarak banka anahtar yöneticileri gözetiminde H-TSM Gateway sunucusuna ait HSM cihazına girilir. İlk kurulumda H-TSM Gatewaye (TGW) ait açık anahtarlar ($P_{TGW-SIGN}$, $S_{TGW-SIGN}$, P_{TGW}, S_{TGW}) ve sertifikaları ($C_{TGW-SIGN}$, C_{TGW}) yüklenir. Ayrıca YN ÖKC ile hassas veri paylaşımında kullanılmak üzere HSM'de GMK (Gateway Master Key) simetrik anahtarı üretilir. TGW'de herhangi bir anahtarları saklamak için bir veritabanı bulunmaz. Çünkü TGW'nin bakımının çok kolay olması ve basit kurguda olması amaçlanmıştır. Bununla birlikte ilk kurulumda finansal ESHS zincir kök sertifikaları da TGW'ye yüklenir. H-TSM ile TGW ilk haberleşmesini yapmadan önce TGW'ye ait sertifikalar H-TSM merkezine ait veritabanında kayıtlı olmalıdır. Böylelikle TGW ilk haberleşmesinde H-TSM merkezi ile anahtar değişimi yaparak H-TSM'e ait sertifikaları kendine alır.

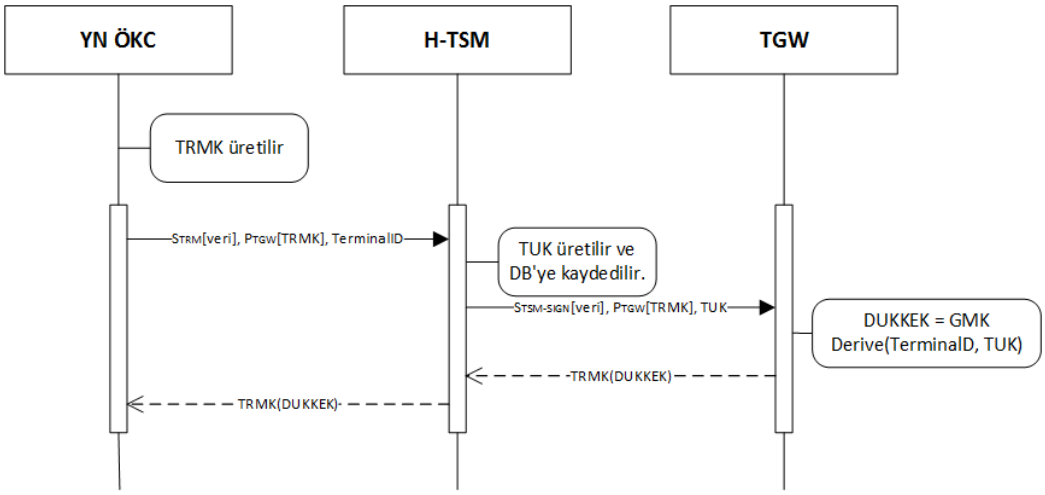
TGW, banka ile ilk haberleşmesinde anahtar değişimi ile ZPK (Zone PIN Key) paylaşır. ZPK, YN ÖKC tarafından bankaya gönderilmek üzere önce TGW'ye şifreli

gönderilen, sonrasında TGW tarafından ZPK ile şifrelenerek bankaya gönderilecek olan PIN değerini şifrelemek için kullanılır. Şekil 4.2'de bu akışı gösterilmiştir.



Şekil 4.2 : TGW – Banka arasında signon mesajları.

YN ÖKC, ilk kurulumu ve aktivasyonu tamamladıktan sonra banka uygulamasını yükler. Banka uygulamasıyla beraber ilgili bankanın TGW sertifikalarını da yüklemiş olur. Banka uygulamasını kullanmadan önce veri paylaşım anahtarlarını Şekil 4.3'teki akıştaki gibi paylaşmalıdır.



Şekil 4.3 : YN ÖKC – TGW arasında veri anahtarı paylaşımı.

TGW'de herhangi bir veritabanı bulunmaz. Böylelikle bakım maliyetleri en az hale indirgenmiş olur. YN ÖKC ile TGW arasında ortak anahtar H-TSM tarafından bildirilen bilgilere göre GMK anahtarından türetilir. Derived Unique Key - Key Encryption Key (DUKKEK), GMK anahtarından türetilen bir anahtardır. Terminal Unique Key (TUK) türetme için kullanılan başka bir anahtardır.

4.3.2 PIN anahtar paylaşımları

YN ÖKC ile banka arasında PIN bilgisi paket şifresinden bağımsız ayrı bir simetrik anahtarla şifrelenerek iletilmelidir. Bu anahtarın yönetimi H-TSM ile yapılmaktadır. PIN bilgisini şifrelemek için gerekli olan simetrik anahtar TPK (Terminal PIN Key), YN ÖKC isteği doğrultusunda her seferinde H-TSM tarafından üretilir ve ilgili terminalin seri numarasıyla indeksli olarak veritabanında LMK ile şifreli olarak saklanır. İlgili işlemler Çizelge 4.1'deki tabloda sunulmuştur.

Çizelge 4.1 : TPK üretimi.

İşlem	**Kaynak**	**Açıklama**	**Hedef**
Üretim	YN ÖKC	TRMK üretilir. (Tek sefer rassal)	-
İstek	YN ÖKC	P_{TSM}(TRMK), $S_{ÖKC}$ [İşlem Verisi]	H-TSM
Üretim	H-TSM	HSM ile TPK üretilir	-
Saklama	H-TSM	LMK(TPK) olarak veritabanında saklanır.	Veritabanı
Cevap	H-TSM	TRMK(TPK), $S_{TSM-SIGN}$ [İşlem Verisi]	YN ÖKC

Yine aynı şekilde benzer işlem H-TSM ile TGW arasında olur. H-TSM ile TGW arasında TPK anahtarını paylaşmak için TPKEK (TPK Key Encryption Key) anahtarı TGW tarafından üretilir ve H-TSM tarafından şifreli olarak veritabanında saklanır. İlgili işlemlere ait tablo Çizelge 4.2'de sunulmuştur.

Çizelge 4.2 : TPKKEK üretimi.

İşlem	**Kaynak**	**Açıklama**	**Hedef**
Üretim	H-TSM	GRMK üretilir. (Tek sefer rassal)	-
İstek	H-TSM	P_{TGW}(GRMK), $S_{TSM-SIGN}$ [İşlem Verisi]	TGW
Üretim	TGW	HSM ile TPKKEK üretilir	-
Saklama	TGW	LMK(TPKKEK) olarak dosyada saklanır.	Dosya
Cevap	TGW	GRMK(TPKKEK), $S_{TGW-SIGN}$ [İşlem Verisi]	H-TSM

4.3.3 Güvenli finansal işlem

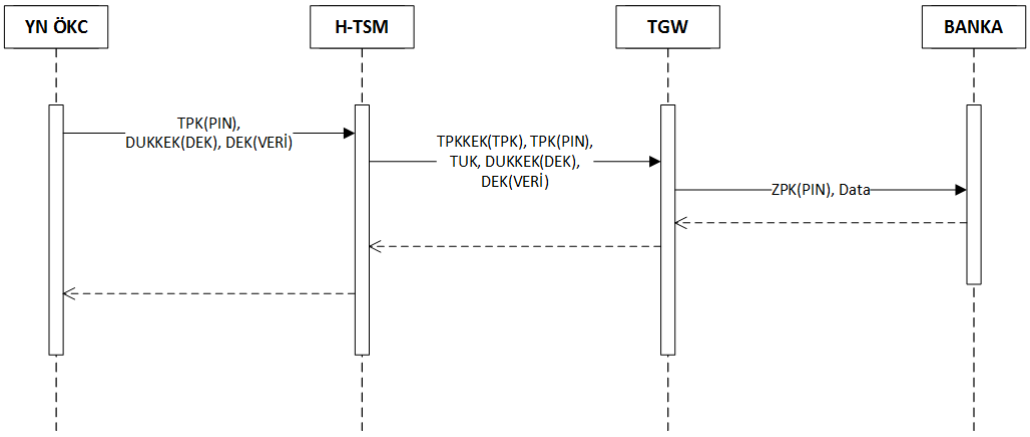
YN ÖKC ile kartla yapılan ödemelerde TSM üzerinden bankaya bir finansal işlem akışı söz konusudur. Bu çalışmada önerilen H-TSM ile PIN içeren bir finansal işlemin, PIN güvenlik standartlarına uygun olarak nasıl iletildiği açıklanacaktır. Öncesinde gerekli anahtarlar, uçlar arasında güvenli bir şekilde paylaşılmış ve güvenli saklama yöntemleriyle saklanmıştır. Gelinen durumda modelimizde bulunan uçların sahip olduğu anahtar tablosu Çizelge 4.3'te sunulmuştur.

Çizelge 4.3 : Güvenli finansal işlemde ilk anahtarlar.

YN ÖKC	H-TSM	TGW	BANKA
$S_{ÖKC}$	$S_{TSM-SIGN}$ S_{TSM}	$S_{TGM-SIGN}$ S_{TGM} ZMK	ZMK ZPK
DUKKEK TPK	TPKKEK TPK TUK	GMK ZPK TPKKEK DUKKEK*	

*: DUKKEK = GMK Derive (TerminalD, TUK)

İşlem anında finansal akış Şekil 4.4'teki gibidir.



Şekil 4.4 : PIN içeren güvenli finansal işlem.

PIN bilgisi YN ÖKC tarafından TPK altında şifrelenir. Hassas veri grubu ise rassal olarak üretilen DEK (Data Encryption Key) simetrik anahtarı ile şifrelenir. DEK ise daha önce TGW ile paylaşılmış DUKKEK ile şifrelenerek iletilir. H-TSM akan trafikte TPK anahtarına bilmesine rağmen DEK ile şifrelenmiş hassas veri grubunda bulunan TPK(PIN) bilgisini açamaz. Çünkü DEK anahtarı DUKKEK ile şifrelenmiştir ve DUKKEK anahtarı H-TSM'de mevcut değildir. TGW ise H-TSM ile gönderilen bu finansal mesajı açabilir. Çünkü GMK anahtarından türetilen DUKKEK'i üretebilmektedir. DUKKEK, GMK anahtarından türetilir. TGW, hassas veri grubunu, DUKKEK ile açarak elde ettiği DEK ile açar. Hassas veri grubundan TPK(PIN) bilgisini kendisine H-TSM ile gönderilen TPK ile açar. Öncesinde tabii ki TPK'yı kendisinde bulunan TPKKEK ile açmıştır. Bankaya finansal işlemi

göndermeden önce ZPK ile PIN bilgisini şifreler. Böylelikle hassas veri H-TSM üzerinden görülmeden YN ÖKC ile banka arasında iletilmiş olur.

4.3.4 Anahtarlar ve kullanım alanları

Önerilen modelde kullanılan anahtar kısaca bu maddenin alt bölümlerinde anlatılmıştır.

4.3.4.1 Gateway master key (GMK)

Bu anahtar TGW içerisinde LMK altında bir dosyada güvenli şekilde saklanan bir simetrik anahtardır. İlk kurulum esnasında oluşturulur. Herhangi bir uç ile paylaşılmaz. DUKKEK üretimi esnasında kullanılan bu anahtar işlem miktarına göre kısa ömürlü olarak kullanılması yerinde olacaktır. Tercihen 6 aylık dönemlerde değiştirilebilir.

4.3.4.2 Terminal PIN key (TPK)

TPK, PIN bloğunu şifrelemek için H-TSM tarafından üretilen bir simetrik anahtardır. TPK, H-TSM veritabanında LMK altında saklanır ve YN ÖKC'ye iletilir. Gün sonunda veya cihaz her açıldığında bu anahtar tekrar yenilenir.

4.3.4.3 TPK key encryption key (TPKKEK)

TGW tarafından üretilen bu simetrik anahtar H-TSM ile TGW arasında TPK anahtarının güvenli taşınmasında kullanılır. H-TSM veritabanında LMK altında şifreli olarak saklanır. TGW'de ise LMK altında bir dosyada şifreli olarak saklanır. Bu anahtar H-TGW ile TGW arasında her bağlantı koptuğunda veya gün sonunda tekrar üretilen bir anahtardır.

4.3.4.4 Diğer anahtarlar

Bunun dışında iletişimde kullanılan anahtarlar tek seferlik veya belli aralıklarla değişen anahtarlardır. Data Encryption Key (DEK), Terminal Random Master Key (TRMK) ve Gateway Random Master Key (GRMK) rassal üretilen tek seferlik simetrik anahtarlardır. DUKKEK üretimi için kullanılan Terminal Unique Key

(TUK) belli aralıklarla her değiştirildiğinde DUKKEK değişmektedir. ZPK'da TGW ile banka arasında her yeniden bağlantı kurulduğunda üretilen bir simetrik anahtardır.

4.3.5 Sistem için önerilen uzaktan sertifika yükleme/yenileme süreci

Normal şartlar altında YN ÖKC'nin ekonomik ömrü maksimum 10 yıldır. Bu yüzden belli dönemlerde süresi sona erecek olan H-TSM ve TSM Gateway (TGW) anahtarları yeniden üretilerek sertifikalandırılmalı ve bu sertifikalar uzaktan YN ÖKC'ye yüklenmelidir. Hatta finansal işlemler için üretilen YN ÖKC sertifikası da maksimum beş yıl (daha az süreli de olabilir) olabileceğinden YN ÖKC'ye ait anahtarların da yeniden üretilerek sertifikalandırılması ve bu sertifikaların uzaktan yüklenmesi gerekir. YN ÖKC, güvenli odada güvenli alanına yüklenen zincir kök sertifikalarını kullanarak bu yeni sertifikaları doğrulayacaktır.

H-TSM, mevcut sertifikaların henüz geçerliliği dolmadan belli bir süre öncesinde yeniden üretilmiş $\mathbf{P_{TSMSIGN-Y}}$ ve/veya $\mathbf{P_{TSM-Y}}$ ve/veya $\mathbf{P_{TGWSIGN-Y}}$ ve/veya $\mathbf{P_{TGW-Y}}$ ve/veya $\mathbf{P_{ÖKC-Y}}$ anahtarlarına ait sertifikaları barındırıyor olmalıdır. Bu işlem sahadaki tüm YN ÖKC'lerin sertifika güncelleme süreleri de düşünülerek en az üç ay öncesinden başlatılmalıdır. Yeni üretilmiş sertifikaların geçerlilik başlangıç tarihi bir önceki sertifikanın bitiş tarihi olmalıdır. Böylelikle aynı anda geçerli iki sertifika olmayacaktır.

Yeni sertifikalar mevcut gösterimin sonuna "Y" eklenerek gösterilmiştir. Buna göre

$C_{TSMSIGN-Y}$: TSM'e ait yeni imzalama sertifikası
C_{TSM-Y}: TSM'e ait yeni şifreleme sertifikası
$C_{TGWSIGN-Y}$: TGW'ye ait yeni imzalama sertifikası
C_{TGW-Y}: TGW'ye ait yeni şifreleme sertifikası
$C_{ÖKC-Y}$: YN ÖKC'ye ait imzalama sertifikası

şeklinde tanımlanmıştır.

4.3.5.1 YN ÖKC'ler için önerilen sertifika yükleme ve yenileme süreci

Bu bölümde H-TSM ve TGW sertifikalarının uzaktan yükleme adımları açıklanacaktır. Aşağıdaki adımlar hem yeni yükleme hem de yenileme için

işletilebilir. İmzalanarak gönderilen verinin her iki taraf tarafından bilinir ve zaman, saat ve tuzlama (salting) gibi tekniklerle değişken olması gerekmektedir. Böylelikle tekrarlama (replay) tarzı işlemlerin/atakların önüne geçilmiş olunacaktır.

1. YN ÖKC yeni sertifika yükleme isteği ile H-TSM merkezine gelir. Bunun için yeni sertifika yükleme mesajını YN ÖKC tarafında bulunan özel anahtarla imzalar ve TSM'e gönderir.

   $S_{ÖKC}$ [Yeni Sertifika Yükleme Mesajı], Veri → H-TSM

2. H-TSM kendisine gönderilen imzalı veriyi doğrulaması gerekir. Bunun için bir takım doğrulama adımlarını yerine getirir.
   a. Sertifika kontrolleri (Anahtar kullanım alanı, geçerlilik tarihi, kök sertifika zincir kontrolleri vb)
   b. Sertifika İptal Listesi (SİL) kontrolü ile sertifikanın geçerli olup olmadığı kontrol edilir.
   c. İmzalanan verinin sertifika içerisindeki açık anahtarla doğrulanması

   Doğrulamalar başarılıysa H-TSM, kendisine ait $S_{TSMSIGN}$ özel anahtarla yeni sertifikayı, yeni sertifikaya ait $S_{TSMSIGN-Y}$ ile mevcut kullanılan sertifikayı imzalayarak, imzalar ile birlikte $C_{TSMSIGN-Y}$ sertifikasını YN ÖKC'ye gönderir.

   $S_{TSMSIGN}$ [$C_{TSMSIGN-Y}$], $S_{TSMSIGN-Y}$ [$C_{TSMSIGN}$], $C_{TSMSIGN-Y}$ → YN ÖKC

   Eğer sadece yeni anahtar ve sertifika üretimi varsa veya ilgili terminal eski terminalde bulunan $C_{TSMSIGN}$ sertifikasının geçerlilik tarihinden sonra sertifika yükleme işlemi yapıyorsa aşağıdaki şekilde mesaj iletilir. Burada esas önemli olan gönderen ucun yani H-TSM sertifikasının güncel olarak karşıya iletilmesidir.

   $S_{TSMSIGN-Y}$ [$C_{TSMSIGN-Y}$], $C_{TSMSIGN-Y}$ → YN ÖKC

Eğer sertifika bir şifreleme sertifikası ve TGW sertifikaları ise yani **C_{TSM-Y}, C_{TGW-Y}, $C_{TGWSIGN-Y}$** sertifikaları yüklenecekse bu sertifikalarda H-TSM'e ait güncel imzalama anahtarı ile imzalanarak yollanır.

$S_{TSMSIGN}$ [C_{TSM-Y}], C_{TSM-Y} → YN ÖKC

veya

$S_{TSMSIGN}$ [C_{TGW-Y}], C_{TGW-Y} → YN ÖKC

veya

$S_{TSMSIGN}$ [$C_{TGWSIGN-Y}$], $C_{TGWSIGN-Y}$ → YN ÖKC

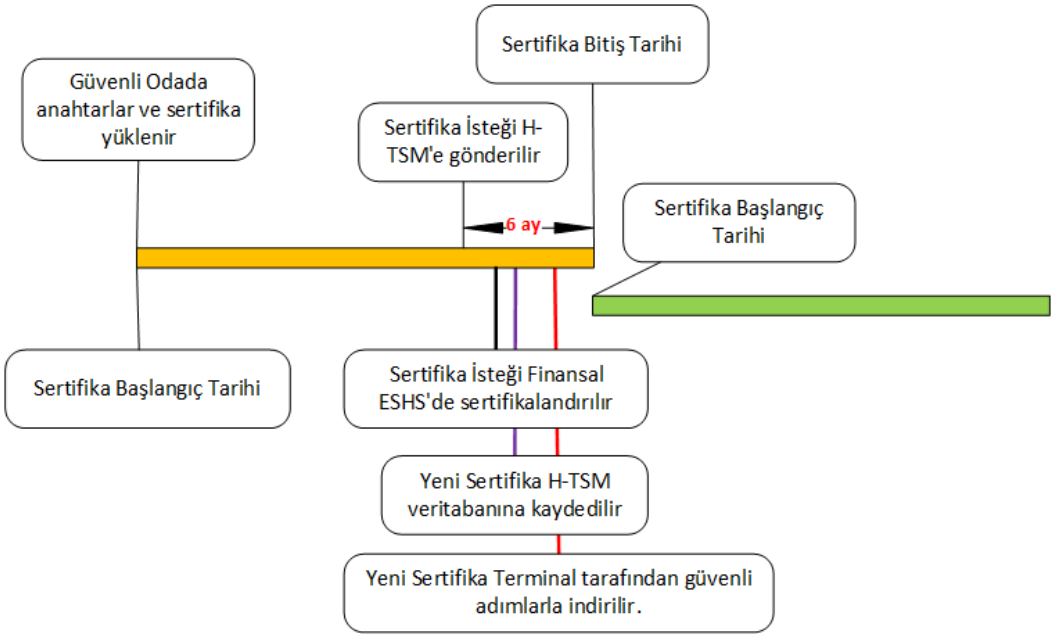
3. YN ÖKC kendisine gönderilen imzalı veriyi/verileri aşağıda ifade edilen doğrulamaları yaptıktan sonra doğrulamış olur. YN ÖKC'nin SİL kontrolü yapmasına gerek yoktur. Çünkü YN ÖKC, TSM dışında hiçbir yere bağlanamaz ve kaynak yönetimi açısından SİL indirmek maliyetli olacaktır.

    a. Sertifika kontrolleri (Anahtar kullanım alanı, geçerlilik tarihi, kök sertifika zincir kontrolleri vb.)
    b. İmzalanan verinin sertifika içerisindeki açık anahtarla doğrulanması

Doğrulamalar başarılıysa YN ÖKC, kendisine gönderilen sertifikayı güvenli alanına kaydeder. YN ÖKC, mevcut kullanılan sertifika süresi dolduğunda yeni sertifikayı kullanmaya başlar.

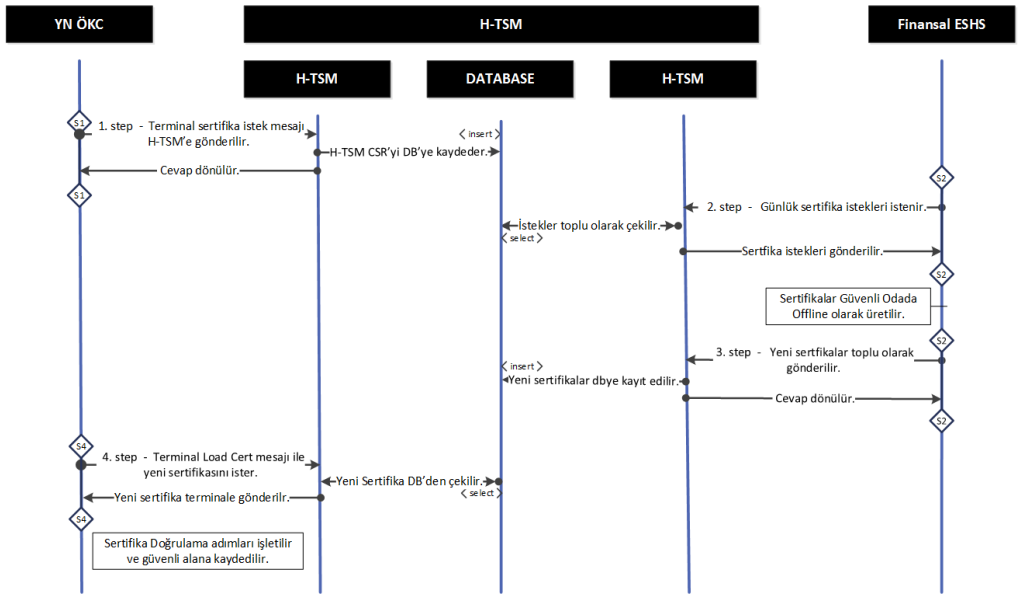
4.3.5.2 YN ÖKC'ler için önerilen anahtar üretimi ve sertifikalandırma süreci

YN ÖKC yaşam döngüsünde en az bir kez finansal işlem sertifikasını güncellemelidir. Çünkü verilecek finansal sertifikalar beş yıllıktır ama YN ÖKC'nin ekonomik ömrü 10 yıldır [9],[43]. İlk senaryomuz ilk seferde güvenli odada iki çift anahtar ve iki sertifika üretmektedir. Birinin başlangıç tarihi diğerinin bitiş tarihi olacak şekilde 10 yıllık anahtar kullanımı garantilenmiş olur. Bu durumda birşey yapmaya gerek olmayacaktır. Diğer senaryo ise uzaktan yüklemedir. İlki güvenli odada üretilip yüklenen anahtarlara ait sertifika süresi bitmeden önce yeni anahtarlar ve sertifika üretilmelidir. Terminal sertifikasının kullanım süresi dolmadan altı ay önce H-TSM'e terminal, sertifika istek mesajı (CSR – Certificate Signing Request) gönderir. Bu mesajı göndermeden önce güvenli bir şekilde asimetrik anahtar çiftini üretmiş olmalıdır. YN ÖKC'ye yeni anahtar üretim ve sertifikalandırma süreci kronolojik olarak Resim 4.6'da gösterilmiştir.



Resim 4.6 : Anahtar üretme ve sertifikalandırma kronolojisi.

H-TSM, kendisine mesajla iletilen sertifika isteğini güvenli yollarla finansal ESHS'ye ulaştırır. Sertifika isteği burada sertifikalandırılarak tekrar güvenli bir yol ve yöntemle H-TSM'e iletilir. Yeni sertifikanın başlangıç tarihi mevcut sertifikanın bitiş tarihinden sonradır. H-TSM, ilgili sertifikayı kendi veritabanında saklayarak terminalin bir sonraki kendisine ulaştığında yükleme emri vererek terminali bu sertifikayı almasına yönlendirir. Şekil 4.5'te tüm sertifikalandırma akışı gösterilmiştir.



Şekil 4.5 : YN ÖKC için sertifikalandırma akışı.

YN ÖKC yani terminal, sertifikayı aşağıda işlem adımlarıyla kendisine alır.

1. YN ÖKC yeni sertifika yükleme isteği ile H-TSM merkezine gelir. Bunun için yeni sertifika yükleme mesajını YN ÖKC tarafında bulunan özel anahtarla imzalar ve TSM'e gönderir.

   $S_{ÖKC}$ [Yeni Sertifika Yükleme Mesajı], Veri → H-TSM

2. H-TSM kendisine gönderilen imzalı veriyi aşağıda ifade edilen doğrulamaları yaptıktan sonra doğrulamış olur.
   a. Sertifika kontrolleri (Anahtar kullanım alanı, geçerlilik tarihi, kök sertifika zincir kontrolleri vb)
   b. Sertifika İptal Listesi (SİL) kontrolü ile sertifikanın geçerli olup olmadığı kontrol edilir.
   c. İmzalanan verinin sertifika içerisindeki açık anahtarla doğrulanması

   Doğrulamalar başarılıysa H-TSM, kendisine ait $S_{TSMSIGN}$ özel anahtarla yeni sertifikayı imzalayarak, imzalar ile birlikte $C_{ÖKC-Y}$ sertifikasını YN ÖKC'ye gönderir.

   $S_{TSMSIGN}$ [$C_{ÖKC-Y}$], $C_{ÖKC-Y}$ → YN ÖKC

4. YN ÖKC kendisine gönderilen imzalı veriyi/verileri aşağıda ifade edilen doğrulamaları yaptıktan sonra doğrulamış olur. YN ÖKC'nin SİL kontrolü yapmasına gerek yoktur. Çünkü YN ÖKC, TSM dışında hiçbir yere bağlanamaz ve kaynak yönetimi açısından SİL indirmek maliyetli olacaktır.

   a. Sertifika kontrolleri (Anahtar kullanım alanı, geçerlilik tarihi, kök sertifika zincir kontrolleri vb)
   b. İmzalanan verinin sertifika içerisindeki açık anahtarla doğrulanması
   c. YN ÖKC, kendisinin ürettiği açık anahtar ile sertifika içerisinde bulunan açık anahtarı karşılaştırır. Farklıysa hata mesajı gönderir.

Doğrulamalar başarılıysa YN ÖKC, kendisine gönderilen sertifikayı güvenli alanına kaydeder. YN ÖKC, mevcut kullandığı sertifika süresi dolduğunda yeni anahtarları ve sertifikayı kullanmaya başlar.

5. SONUÇ VE ÖNERİLER

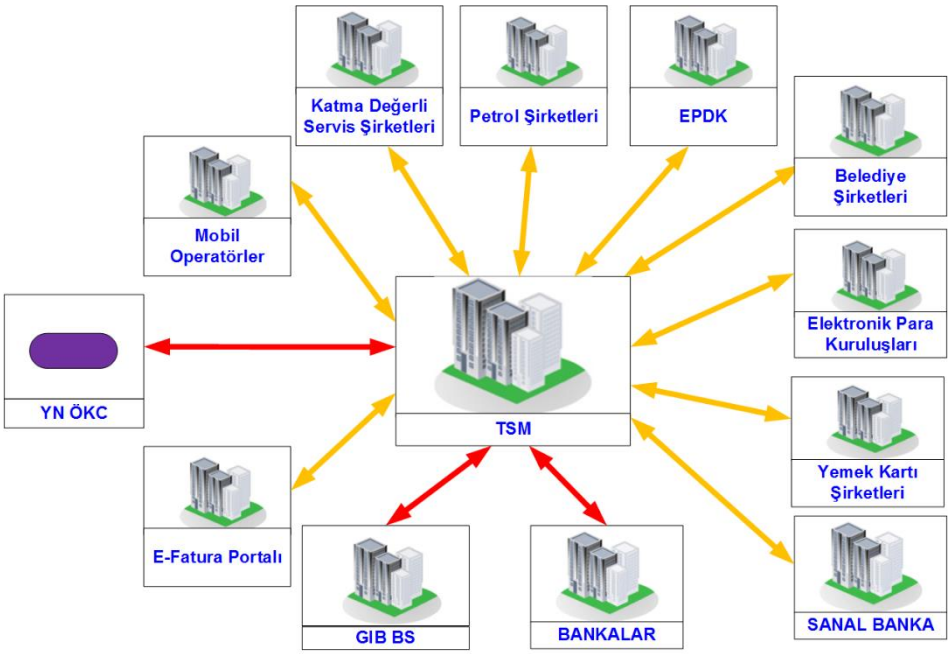
Yeni nesil ödeme kaydedici cihazlar ileriki yıllarda yaygınlaşarak bütün sektörlerde kullanılabilir olacaktır. Gelir İdaresi Başkanlığı yayınladığı mevzuatlarla [1] bu yayılım planını sunmuştur.

2013 yılında yayınlanan kanunla elektronik para kuruluşlarının kuralları belirlenmiştir [54]. GİB, YN ÖKC'lerde ödeme tiplerinden biri olarak elektronik para kuruluşlarınca sunulan kartlardan bahsetmektedir [2],[3]. Bu tarz kuruluşlarla TSM merkezlerinin iletişiminin de aynı banka kadar güvenli olması gerekmektedir. Bununla birlikte yemek kartları ve çekleri, belediye ulaşım kartları, yardım kartları ve ekleri, sanal ödeme, mobil ödeme, vb. ödeme tiplerinin de yakın zamanda TSM ile entegre olarak kullanılacağı öngörülmektedir. Hatta grup kampanya, kupon, promosyon uygulamaları gibi katma değerli servis uygulamalarının YN ÖKC ile kullanımının ve parkmetre/parkomat cihazlarında YN ÖKC kullanımının mümkün olacağı görülmektedir [2],[3]. Bu durumda birçok sektörün YN ÖKC vasıtasıyla iletilecek verileri almak için TSM merkezleri ile güvenli olarak entegre olması gerekmektedir.

Ülkemizde geçmiş yıllarda yayınlanmış 3100 sayılı kanun ve 58 seri no.lu genel tebliğ [55] ile akaryakıt sektöründe 2004 yılından itibaren ödeme kaydedici cihaz kullanma zorunluluğu getirilmiştir. Yakın zamanda YN ÖKC'lerin akaryakıt pompalarında kullanılmasına yönelik planlamaların GİB tarafından yürütüldüğü bilinmektedir [2,3]. Dolayısıyla akaryakıta özgü bilgilerin TSM üzerinden akması ile petrol şirketlerinin yürüttüğü sadakat kartı, hediye kartı, vb. kart bilgilerinin güvenli olarak taşınması ve petrol şirketlerine iletilmesi TSM kullanılarak sağlanabilir olacağı öngörülmektedir. Sadakat sisteminde müşteri bilgileri de aynı banka bilgileri hassasiyeti ile ilgili petrol şirketleriyle yapılacak güvenli haberleşme altyapısıyla iletilmesi gerekecektir. Öte yandan akaryakıt sektörü için Enerji Piyasası Denetleme Kurumu'na iletilme zorunluluğu olan akaryakıt hareketlilik bilgileri [56] de online olarak TSM üzerinden taşınabilmesinin mümkün olacağı tahmin edilmektedir.

Ülkemizde kullanılan diğer bir hizmet e-fatura hizmetidir. E-fatura, Vergi Usul Kanunu (VUK) hükümlerine göre düzenlenmesi zorunlu olan faturada yer alan bilgilerin belirli bir formatta standart hale getirilmiş, değiştirilemez bir şekilde mühürlenmiş, satıcı ve alıcı arasında güvenli, zaman ve maliyet tasarrufu sağlayan elektronik belgedir [57]. E-fatura, elektronik ortamda mali mühür ile imzalanarak üretilmiş ve kâğıt fatura ile aynı nitelikte hukuki geçerliliğe sahiptir [57]. Sonuçta e-fatura kullanabilen mükelleflerinin YN ÖKC ile alışverişlerinde e-faturalarının YN ÖKC kullanarak TSM vasıtasıyla kesilebilir olması da entegrasyonlarla mümkündür.

Yukarıda kısaca bahsedilen ve TSM merkezlerine değebilecek bu gelişmeler ile TSM merkezi, Resim 5.1'deki gibi bir mimari yapıya dönebilir.



Resim 5.1 : Gelecekteki tahmini TSM mimarisi.

Bu çalışmada önerilen bu TSM modelinde, anahtar yönetimiyle beraber finansal sertifika otoritesi mimarisi de açıklanmıştır. Bu yapının ileride entegre edilebilecek her türlü ödeme enstrümanına ve/veya kuruluşa güvenli bir şekilde entegre olabileceği söylenebilir. Özellikle her türlü ödemenin veya kritik bilgilerin TSM üzerinden iletileceği düşünülürse, kurulacak güçlü ve güvenli anahtar yönetim mimarisinin hassas veri iletimi gerektiren her türlü ödeme işleminde ve/veya diğer bilgilerin iletiminde kullanılması mümkün olacaktır. Sonuç olarak bu mimari yapıda yukarıdaki bölümlerde bahsedilen güvenli mesajlaşma ve anlık anahtar yükleme

mekanizmalarının bir benzerini her türlü ödeme sisteminde uygulamak mümkün hale gelecektir.

TSM merkezlerinin esas kuruluş amacı ödemeden çok, ödeme iziyle mali izi örtüştürmek ve takip etmek adına aracılık yapmaktır. Hal böyle olunca ödeme sistemleri ve diğer geliştirmelere göre kendisini yenilemesi gerekmektedir. Yazarkasa dünyasına bakıldığında çok fazla yenilikçi bir gelişimin bundan sonra olması pek olası gözükmemektedir ama ödeme sistemleri ise sürekli değişmekte, çeşitli araçlar ve enstrümanlarla farklılaşmaktadır. Bu anlamda gelecekte ne olabilir diye incelendiğinde, PCI ve diğer ödeme sistemlerine yön verici kuruluşların hassas veri taşımak yerine jeton iletimi mantığıyla hareket etmeye yönelmesi veya önermesidir. Bu durum aynı şekilde elektronik para kuruluşları için yapılacak entegrasyonlarda taşınan hassas veriler için de söz konusu olacağı düşünülmektedir. Bu bir ihtiyaç olduğundan TSM merkezlerinin de ister istemez bankacılık sistemlerinden dolayı bu yeni ödeme sistemlerine evirilmesi gerekecektir. Bir diğer konu da TSM'in ileride gelebileceği durumdur. TSM merkezleri ile o kadar fazla entegrasyon yapma olanağı vardır ki, bu verilerle (eğer TSM tüm bankacılık ödemelerini üzerinden geçirirken bir şekilde tutmasında sakıncalı olmayan banka kartlarının ilk 6 hane ve son 4 hanesini saklarsa) TSM merkezleri veri analizi yapar hale gelebilir. Buradaki sistemde ödemeyi yapan kişi bilinmez ama eline geçirebileceği kart numarasının belli haneleriyle bu kartın dolayısıyla kart sahibinin alışveriş eğilimini çıkarabilir. O yüzden bilgi güvenliği noktasında bunu önleyebilecek bir mekanizmanın çalışılması mümkün hale getirilebilir.

Sonuç olarak TSM merkezleri ödeme sistemlerinde POS ve bankacılık iletişimine daha güvenli bir altyapı sağlamıştır. Ancak hala sistemin üzerinden hassas verilerin taşınması yapılmaktadır. Ama son yıllardaki gelişmeler ödeme sistemlerinde hassas verilerin taşınması yerine hassas verileri indeksleyen jeton yapısına evrimin olacağını göstermektedir. Bundan sonraki çalışmalarda TSM merkezlerinin daha önce açıklanan bu Jeton Servis Sağlayıcılarını kullanması, akışın bu tarz kurgulanması ve buna yönelik çalışmaların yapılması gerekebilir. Bu süreçte ülkemizde mali verilerin ve finansal verilerin bu merkezlerden iletilmesi nedeniyle her şeyin TSM merkezine doğru aktığı düşünülürse, ödeme sistemlerine yönelik yeni trendlerin de TSM merkezleri tarafından desteklenmesi gerekmektedir. Bundan sonraki çalışmalarda bu

tarz yeni süreçleri barındıracak teknolojilerin TSM altyapısında tasarlanması önerilmektedir.

KAYNAKLAR

[1] 69,70 seri No'lu ÖKC Genel Tebliğleri ve 426-427-435-437-450-451-465-466 Sıra No'lu Vergi Usul Kanunu Genel Tebliğleri.

[2] **GİB**, Yeni Nesil Ödeme Kaydedici Cihazlar Teknik Kılavuzu TK-1, Sürüm 4.0, 20 Ekim 2016.

[3] **GİB**, Yeni Nesil Ödeme Kaydedici Cihazlar Teknik Kılavuzu TK-2, Sürüm 4.0, 20 Ekim 2016.

[4] **GİB**, Gelir İdaresi Başkanlığı Mesaj Protokolü (GMP) Spesifikasyonları 1, Sürüm 4.0, 18 Mayıs 2015.

[5] **GİB**, Gelir İdaresi Başkanlığı Mesaj Protokolü (GMP) Spesifikasyonları 2, Sürüm 4.0, 18 Mayıs 2015.

[6] **GİB Strateji Geliştirme Daire Başkanlığı** , , "Kayıtdışı Ekonomiyle Mücadele Stratejisi Eylem Planı (2008-2010)", Yayın No: 87, 27132 sayılı Resmî Gazete, 5 Şubat 2009.

[7] **GİB Strateji Geliştirme Daire Başkanlığı**, "Kayıtdışı Ekonomiyle Mücadele Stratejisi Eylem Planı (2011-2013)", Yayın No: 87, 28149 sayılı Resmî Gazete, 21 Aralık 2011.

[8] **International Standart Organisation**, ISO 8583:2003 Financial transaction card originated messages — Interchange message specifications, ISO 8583 Financial Transaction Message Format, 2003.

[9] **Revenue Administration**, Common Criteria Protection Profile For New Generation Cash Register Fiscal Applicaton Software (NGCRFAS PP), TSE-CCCS/PP-007, s.14-20, 6 Mayıs 2015.

[10] **European Commission**, 'Proposal for a Directive of the European Parliament and of the Council [of the EU] on Payment Services in the Internal Market and Amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC', 2013

[11] *https://usa.visa.com/dam/VCOM/download/merchants/tpa-registration-program-faqs.pdf*, alındığı tarih:01.12.2016

[12] *https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html*, alındığı tarih:01.12.2016

[13] *http://bkm.com.tr/bkm-hakkinda/bkmyi-taniyin/servis-saglayicilar*, alındığı tarih:03.12.2016

[14] **Santamaría, Javier**, (2014). The emergence of new payment service providers and their impact on the regulatory and market environment, *Journal Of Payments Strategy & Systems*, Volume 8, No. 4, 407-414.

[15] **Larkham, B.**, (2010). Direct access to payment service providers by businesses and organisations in Europe, *Journal of Payments Strategy & Systems*, Vol.4, 3.

[16] **Cortada, James W.**, (2000). Before the Computer: IBM, NCR, Burroughs, and Remington Rand and the Industry They Created 1865-1956, Princeton University Press, 64-79.

[17] **Marcosson, Isaac F.**, Wherever Men Trade: The Romance of the Cash Register, Arno Pr, 1972.

[18] **Crandall, Richard L.**, The Incorruptible Cashier,1988, Vestal Press Ltd.

[19] *http://www.patentmuzesi.com/patent/yazar-kasa*, alındığı tarih:14.11.2016.

[20] **Rubben, Murray A.** (1971). Electronic Cash Register, *United States Patent*, No: 199685 Tarih: 24.07.1973.

[21] **Tadakuma, Y., Saito, S., Eguchi, T.** (1977). Electronic Cash Register, *United States Patent*, No: 799987 Tarih: 27.02.1979.

[22] **Ohmae, K., Tateisi, K., Shinohara, Y., Ichihashi M.** (1984). Electronic Cash Register, *United States Patent*, No: 4562341 Tarih: 31.12.1985.

[23] 3100 sayılı, Katma Değer Vergisi Mükelleflerinin Ödeme Kaydedici Cihazlari Kullanmalari Mecburiyeti Hakkında Kanun, R. Gazete, 15/12/1984, Sayı : 18606.

[24] *http://www.milliyet.com.tr/parayi-yeni-urune-cevirdiler/ekonomi/haberdetayarsiv/18.03.2004/29617/default.htm*, alındığı tarih:14.11.2016.

[25] **Bellamy, Edward**, Looking Backward 2000-1887, Signet, 1960.

[26] **Özkan, Akdoğan,** Anı ve Fotoğraflarla Türkiye'nin Kartlı Ödeme Sistemleri Tarihi, BKM, ARYAN Basım Tanıtım ve Matbaa Hizmetleri, 2015.

[27] *http://www.mastercard.com/us/company/en/docs/history%20of%20payments.pdf,* alındığı tarih:09.11.2016.

[28] *http://www.merchantequip.com/merchant-account-blog/102/the-history-of-credit-card-terminals***,** alındığı tarih:09.11.2016.

[29] **Kaya, Ferudun,** Türkiye'de kredi kartı uygulaması, Türkiye Bankalar Birliği, Yayın No:263, Ocak 2009.

[30] **MasterCard Customer Implementation Services**, Key Management Implementation Quick Reference Guide, 2016.

[31] **MasterCard,** M/Chip Program Guide, 29.01.2015.

[32] **PCI SSC (Security Standards Council)**, Payment Card Industry (PCI) Data Security Standard (DSS), Requirements and Security Assessment Procedures, Version 3.2, Nisan 2016.

[33] **PCI SSC (Security Standards Council)**, Payment Card Industry (PCI) PIN Security Requirements, Version 2.0, Aralık 2014.

[34] **Visa,** Payment Technology Standards Manual, Visa Supplemental Requirements, 31.10.2014.

[35] **MasterCard,** On-behalf Key Management (OBKM) Interface Specifications, 16.02.2016.

[36] *https://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/pci-kapsaminda-pin-ve-key-guvenligi.html*, alındığı tarih:10.11.2016.

[37] **MasterCard,** On-behalf Key Management (OBKM) Procedures, 30.11.2011.

[38] **Fernandes, J. M., Wyatt, T., Markwell, S., Wu, K.E., O'connor, J.B.,** (2007). Payment Systems And Methods, *United States Patent*, No: US 2009/0024533 Tarih: 22.01.2009.

[39] **Loomis, N., Saville, J.** (2007). Digital Signature Authentication, *United States Patent*, No: US 2008/0222049 Tarih: 11.10.2008.

[40] **Murdoch, S. J., Drimer, S., Anderson, R., Bond, M.**, (2010). Chip And PIN is Broken, University of Cambridge, Computer Laboratory, IEEE Symposium on Security and Privacy.

[41] **Murdoch, S. J.**, (2009). Reliability of chip & PIN evidence in banking disputes, Digital *Evidence and Electronic Signature Law Review*, vol. 6. Pario Communications, 98–115, ISBN 0-9543245-9-5.

[42] **Adida, Ben, Bond, M., Clulow, J., Lin, A., Murdoch, S., Anderson, R., Rivest, R.**, Phish and Chips, Traditional and New Recipes for Attacking EMV, Security Protocols, Volume 5087, Lecture Notes in Computer Science, 40-48, (2009).

[43] **EMV**, EMV Payment Tokenisation Specification - Technical Framework, v1.0, Mart 2014.

[44] **Payment Card Industry**, PCI Token Service Providers, Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens), version 1.0, Aralık 2015.

[45] **Payment Card Industry**, Payment Card Industry (PCI) Token Service Providers, Report on Compliance –Token Service Providers, Version 1.0, Şubat 2016

[46] *http://www.3dsi.com/blog/credit-card-tokenization-101*, alındığı tarih: 07.12.2016.

[47] **Gelir İdaresi Başkanlığı**, ÖKC-Harici Donanım ve Yazılım Haberleşme Protokolü GMP-3, Sürüm 3.0, 12 Nisan 2016.

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

[49] **GİB**, Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezlerinin Başvuru, Test, Denetim Ve Onay Teknik Kılavuz, Sürüm 2.0, 23 Eylül 2016.

[50] **Revenue Administration**, Common Criteria Protection Profile For New Generation Cash Register Fiscal Applicaton Software 2 (NGCRFAS-2 PP), TSE-CCCS/PP-008, Sf.5-10, 6 Mayıs 2015.

[51] **TÜBİTAK BİLGEM Kamu Sertifikasyon Makamı**, Yeni Nesil ÖKC Sayısal Sertifika Yaşam Döngüsü, Sürüm 2.0, 26 Ekim 2015.

[52] **TÜBİTAK BİLGEM Ortak Kriterler Test Merkezi (OKTEM)**, "Kamu SM Sertifikaları ve İşlevleri", Yeni Nesil ÖKC Detay Kılavuzu v1.6, Sf.28-30, 14 Mayıs 2015.

[53] **GİB**, Yeni Nesil Ödeme Kaydedici Cihazlara Ait "Elektronik Kayıt, Aktivasyon Ve Yetkili Servis Listeleri" Teknik Kılavuzu, Sürüm 2.0, Sf.19-21, 20 Ekim 2016.

[54] 6493 sayılı kanun, Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanun, Yayımlandığı R.Gazete : Tarih: 27/6/2013 Sayı : 28690.

[55] *http://www.idealymm.com/yd.php?ydid=60*, alındığı tarih:08.12.2016.

[56] **EPDK**, 1240 Kurul Kararı, İkinci Bölüm, Denetim Sistemi Kurma ve Uygulama Yükümlülüğü, 26574 sayılı Resmi Gazete, 6 Temmuz 2007.

[57] **Maliye Bakanlığı**, E-fatura ve Mali Mühür, Vergi Usul Kanunu Genel Tebliği, Sıra No: 397, 5 Mart 2010.

ÖZGEÇMİŞ

Ad-Soyad **: Hasan Hüseyin SUBAŞI**

Uyruğu **: TC**

Doğum Tarihi ve Yeri **: 28.02.1978 - Denizli**

E-posta **: subasi@gmail.com**

ÖĞRENİM DURUMU:

- **Lisans** **:** 2000, İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Kontrol ve Bilgisayar Mühendisliği
- **Yükseklisans** **:** 2012, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme ABD, Yönetim Organizasyon

MESLEKİ DENEYİM VE ÖDÜLLER:

Yıl	Yer	Görev
2015	**Cardtek A.Ş.**	**Teknoloji Direktörü**
2012	**TÜBİTAK Kamu SM**	**Ankara Yöneticisi**
2006	**E-imza Bilişim**	**Kurucu Ortak ve Müdür Yrd.**
2001	**Nestle Waters A.Ş.**	**Bilgi İşlem Sorumlusu**
2000	**TÜBİTAK UEKAE**	**Araştırmacı**

YABANCI DİL:

İngilizce

Fransızca

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- **Subaşı, Hasan H.,** 2016. Yeni Nesil Ödeme Kaydedici Cihazlar için Hibrit TSM, Ines International Academic Research Congress, November 3-6, Antalya, Turkey**.**

- **Subaşı, Hasan H.,** 2016. Yeni Nesil Ödeme Kaydedici Cihazlar için Tümleşik ve Hibrit TSM Modeli, International Academic Research Congress, 228-234.