Bankacılık İşlemlerinde Güvenli İletişim için Melez Güvenli Servis Sağlayıcı Modeli Tasarımı

Hybrid Trusted Service Manager Model Design For Secure Communication at Banking Transactions

Hasan Hüseyin SUBAŞI

TOBB Ekonomi ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ankara, TÜRKİYE
subasi@gmail.com

Öz

Bu çalışma ile önerilen sistem, bankacılık sektöründe kullanılan ve POS cihazlarında iletilen finansal işlemlerin, benzer şekilde Yeni Nesil Ödeme Kaydedici Cihazlar (YN ÖKC) üzerinde iletilirken kriptografik olarak daha güvenli hale getirilmesini ve kullanılmasını amaçlamaktadır. Çalışma öncelikle, YN ÖKC ile Güvenli Servis Sağlayıcı (GSS) merkezlerinin güvenli iletişim altyapısını anlatacaktır ve sonrasında bankacılıkta kullanılan finansal işlemler için güvenli bir Melez GSS (H-GSS) çalışma modeli önerecektir. Önerilen bu model aynı zamanda Gelir İdaresi Başkanlığı tarafından istenen her 2 (iki) mali GSS çalışma modeline uyacaktır.

Anahtar Sözcükler: Güvenli Servis Sağlayıcı (GSS), Yeni Nesil Ödeme Kaydedici Cihaz (YN ÖKC), Asimetrik Şifreleme, Güvenli Anahtar Yönetimi.

Abstact

The system proposed in this study, aims to make the financial transactions used in banking sector and transmitted via POS devices, more cryptographically secure while transmitting similarly on the New Generation Electronic Cash Register (NG-ECR). This study initially explains secure communication infrastructure between New Generation Electronic Cash Register and Trusted Service Manager (TSM) centers and afterwards will propose a secure TSM (H-TSM) model for financial transactions in banking. This model will also support the two TSM working model that has been demanded by Revenue Administration (GİB).

Gönderme ve kabul tarihi: 16.11.2017-23.05.2018

Keywords — Trusted Service Manager (TSM), New Generation Electronic Cash Register (NG-ECR), Asymmetric Encryption, Secure Key Management.

1. Giriş

Günümüzde vergiler, devletlerin ekonomik olarak ayakta kalmasında en önemli gelir kalemlerinden biri, belki de en önemlisidir. Devletler kayıtdışı 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 Cihaz, diğer bilinen adıyla yazarkasa POS cihazıdır.

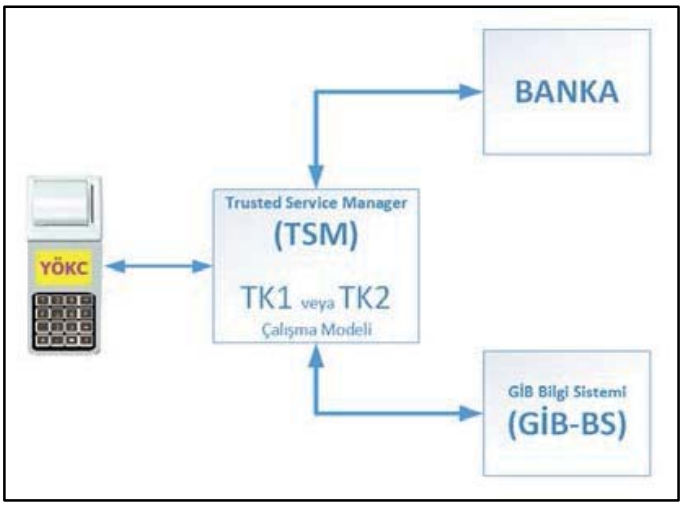
Bankalar, geleneksel POS (Point of Sale) haberleşme dünyasını kendi başlarına yönetmektedirler. POS üzerinde koşan banka uygulamalarının ve parametrelerinin yüklenmesi ile anahtar yönetimi bankanın belirlediği kriterlere göre POS üreticileri tarafından sağlanan altyapı ve geliştirmelerle gerçeklenmektedir. Ancak geçmiş teknolojilere bağımlılık ve banka sistemlerinin büyüklüğünden dolayı, POS cihazları ve bu cihazların iletişim içinde olduğu banka sunucuları arasında, sertifika içeren asimetrik algoritma temelli güçlü ve güvenli bir anahtar yönetimi bulunmamaktadır.

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 ve sonrasında bütün mükelleflerin, kullandıkları yazarkasalar yerine Dünyada bir ilk olarak POS özelliği olan 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 merkezlerin 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. Bunun için etkin bir izleme ve değerlendirme sisteminin oluşturulması gerektiği belirtilmektedir [6 ve 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.

YN ÖKC, yazarkasa ve POS (Point of Sale) özelliğini tek bir cihazda barındıran ve her türlü fiş çıktısını mali uygulamadan bastıran ve kayıt altına alan bir cihazdır. Geleneksel POS cihazları doğrudan banka sunucuları ile ISO-8583 [8] finansal mesajlaşma formatı kullanarak haberleşirken, banka ile YN ÖKC iletişiminde arada Trusted Service Manager (TSM) denilen merkezlerin bulunması zorunlu hale getirilmiş ve YN ÖKC'lerin dolaylı olarak bankaya bağlantı kurması yayınlanan mevzuat ve teknik kılavuzlarla tariflenmiştir (Şekil 1).

Bu çalışmada YN ÖKC ile banka haberleşmesinin TSM altyapısında kurgulanması önerilecek ve güçlü bir anahtar yönetim mekanizmasının Gelir İdaresi Başkanlığı Bilgi Sistemiyle (GİB-BS) ve her iki model TSM yapısıyla nasıl çalışabileceği aktarılacaktır.



Şekil 1. YN ÖKC İletişim Genel Mimari Yapı

Yayınlanan teknik kılavuzlarla [4,5,9,10] GİB'in mükelleflerden talep etmiş olduğu bilgiler ile YN ÖKC, TSM vee Gelir İdaresi Başkanlığı Bilgi Sistemleri (GİB-BS) mesajlaşma standartları bütünüyle tariflenmiştir. İlgili teknik kılavuzlarda YN ÖKC ile Banka haberleşmesinde mesajlaşma standartları belirtilmemiş ancak TSM'in, bankacılık mevzuatlarına ek olarak PCI DSS güvenliğini ve Uluslararası Ödeme Kuruluşlarına uyumluluğu sağlaması istenmiştir [11,12].

POS cihazları, kredi/debit(banka) kartlarının hassas bilgilerini içeren Track alanlarını mesajlarla bankaya taşırlar. Bu alanlarda Kart Numarası (PAN-Primary Account Number), Kart Sahibinin Adı, Son Kullanım Tarihi, PIN bloğu vb. hassas veriler bulunur [13,14]. Bu alanların POS tarafından bankaya kadar güvenli olarak taşınması için bir şifre anahtarı kullanılır. PIN bloğu ise ayrı bir simetrik anahtar ile şifrelenir ve şifreli PIN bloğu olarak track verisi içinde bulunur. Kullanılan algoritmalar anahtar uzunluğu nedeniyle zayıf olduğu bilinen DES (56 bit) ve Double DES (112 bit) gibi algoritmalardır [13,14,15,16]. Bu anahtar uzunlukları özellikle günümüz işlemci hızları göz önüne alındığında, brute force (kaba kuvvet) saldırılarına belli bir süre dayanabilir. Dolayısıyla yerlerine daha güçlü ve anahtar uzunluğu daha uzun algoritmalar kullanılmalıdır. POS cihazında çalışan bankacılık uygulamaları her cihazda aynı ve/veya tek bir anahtarlarla şifreleme altyapısı sağlayacak kadar basit bir şekilde olabildiği gibi her cihaz içerisinde farklı anahtarlarla şifreleme sağlayacak altyapıda da olabilmektedir. Kullanılan bu anahtarlar cihazın

kullanım ömrü süresince değiştirilmez ve uzaktan anahtar yükleme/güncelleme henüz bankacılık sektörü için yeni ve yavaş yaygınlaşmaya geçilen bir özelliktir. Hatta sertifika temelli anahtar yönetim altyapısı neredeyse hiçbir POS cihazında mevcut değildir.

Bu çalışmada önerilen modelin özgünlüğü; ödeme sistemini gerçekleyen banka uygulamasından bağımsız olarak anahtar yönetiminin, YN ÖKC ve TSM üzerinden sertifika temelli ve açık anahtar yönetim sistemi kullanarak tam uyumlu olarak tasarlanmasıdır. Sağlanan güçlü anahtar yönetim altyapısının bütün uygulamalar (bankacılık uygulamaları ve diğer katma değerli servisi uygulamalar) için aynı seviyede güvenlik sunmasıdır. Böylelikle farklı ve görece zayıf anahtar yönetimine sahip bankacılık sistemlerinin POS tabanlı finansal işlemleri daha güçlü bir kriptografik seviyeye çıkarılmış olacaktır.

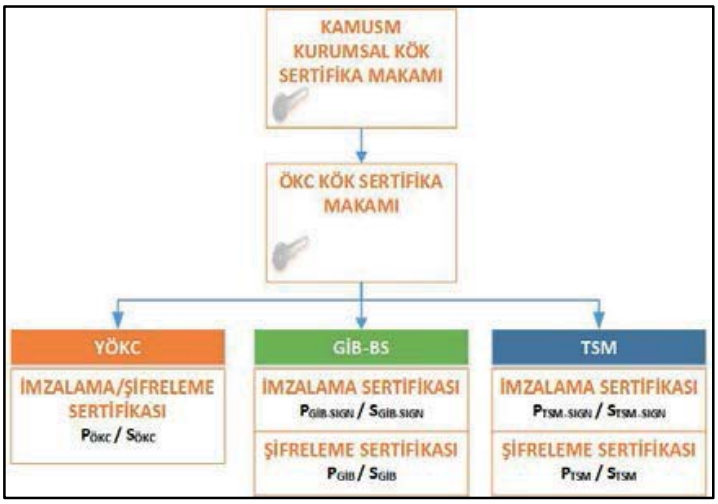
Bu çalışmanın 2. bölümünde mali işlemlerin iletimi için kullanılan YN ÖKC, TSM ve GİB-BS arasındaki haberleşme altyapısı anlatılacaktır. 3. bölümde bankacılık için çalışan TSM modeli detaylı bir şekilde anlatılacak sonrasında bu altyapıda taşınan finansal işlemlerin nasıl güvenli taşınacağına yönelik bir model sunulacaktır. 4. bölümde sonuçlar paylaşılacak ve sonraki diğer çalışmalar için yapılabilecek çalışmalar hakkında bilgiler sunulacaktır.

2. YN ÖKC, TSM ve GİB-BS Haberleşme ve Güvenli İletişim Altyapısı

YN ÖKC, TSM ve GİB-BS, haberleşmede TLV (Tag-Length-Value) mesaj formatında GİB Mesajlaşma Protokolü (GMP) kullanmaktadır. Maksimum paket boyutu 2048 bayt olarak belirlenmiştir. Her paketin başında hexadecimal formatta 2 bayt uzunluğunda paket uzunluğu bilgisi yer alır. Her paketin sonunda 1 bayt uzunluğunda LRC (Longitudinal Redundancy Check) alanı yer alır. YN ÖKC ile TSM paket iletişim genel yapısı Uzunluk, TPDU, Terminal Serino, Mesaj ve LRC şeklindedir. TPDU alanı 1 bayt 0x60 değeri, 2 bayt hedef adres bilgisi, 2 bayt kaynak adres bilgisi olarak tanımlanmıştır. TPDU alanı kaynaklarından farklı gelebilecek mesajları birbirinden ayırt etmek için kullanabilir.

TSM, 2 model olan Teknik Kılavuz 1 (TK1) ve Teknik Kılavuz 2 (TK2) çalışma modellerinden birinde uyumlu olarak çalışmalıdır.

Sayısal Sertifika Koruma Kılavuzu ve Teknik Kılavuzlarda [4,5,17] ifade edildiği gibi YN ÖKC'lere ilk kurulum sırasında güvenli odada ITU X.509 v3 formatı ile uyumlu mali sayısal sertifikalar yüklenmektedir. Bu sertifika temel olarak kimlik doğrulama, YN ÖKC'lerin onaylanmış saha kullanım süresini denetleme, GİB-BS ve TSM Merkezi ile güvenli haberleşme için belirtilen diğer kontrollerde kullanılmaktadır. YN ÖKC için elektronik sertifikalar, GİB tarafından yetkilendirilmiş Elektronik Sertifika Hizmet Sağlayıcısı - ESHS (bu makale hazırlandığı sırada sadece TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi (Kamu SM) yetkilidir) tarafından YN ÖKC üreticisine sertifika yaşam döngüsü kılavuzuna [5] uygun olarak teslim edilerek cihaza özel üretilmektedir. Asimetrik anahtar çiftleri için üretilen sertifikaların doğrulama zincirindeki kök sertifika otoritesi Kamu SM olduğu durumda aşağıdaki şekilde gösterildiği gibidir (Şekil 2).



Şekil 2. Yetkilendirilmiş ESHS Sertifika Otoritesi Sertifika Yapısı

Bu sertifikalar ve hangi amaçla kullanıldığı kısaca aşağıda tanımlanmıştır [18].

- Kamu SM Kurumsal KÖK Sertifikası (Üst Kök) : Sertifika zinciri doğrulama işlemlerinde gereklidir.

- ÖKC KÖK Sertifikası (Alt Kök) : Sertifika zinciri doğrulama işlemlerinde gereklidir.
- YN ÖKC Sertifikası: GİB-BS ve TSM ile kurulacak olan bağlantılarda kimlik doğrulama ve onaylanmış 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.
- TSM İmza Sertifikası ($P_{TSM\text{-}SIGN}$): TK1 için SSL (Secure Socket Layer) haberleşmesinde ve parametrelerin imzasının kontrol edilmesi için kullanılır. İlk kurulum sırasında cihaza yüklenmesine gerek yoktur, iletişim anında TSM tarafından online gönderilebilir. TK2 için ise bu sertifika TSM ile şifreleme anahtarının paylaşımı esnasında imza doğrulaması amacıyla kullanılır.
- TSM Şifreleme Sertifikası (P_{TSM}): Bu sertifika anahtar paylaşımı esnasında anahtarları şifrelemek için kullanılır.
- GİB İmza Sertifikası ($P_{GİB\text{-}SIGN}$): Bu sertifika GİB-BS ile şifreleme anahtarının paylaşımı esnasında imza doğrulaması için gereklidir.
- GİB Şifreleme Sertifikası ($P_{GİB}$): Bu sertifika GİB-BS ile şifreleme anahtarının paylaşımı esnasında kullanılır. YN ÖKC'ler bu sertifika anahtarını kullanarak ürettikleri "Terminal Random Master Key-TRMK" anahtarını şifrelemekte ve GIB-BS'ye iletmektedir.

Ancak mali işlemler için kullanılan bu sertifikaların finansal işlemler için kullanılması ise anahtarları sağlayan ve yönetimini yapan kuruluşun, PCI DSS kapsamında VISA tarafından akredite olan "Visa Approved PIN Security Assessors (PIN SA)" kuruluşları aracılığı ile denetlettirmesi ve olumlu sonuç raporunu alması durumda mümkündür [2 ve 3]. Şu anki anahtarlar ve sertifikalar Tübitak Kamu SM tarafından sağlanmaktadır ve bu kurumun bahse konu olan olumlu sonuç raporuna sahip olmamasından dolayı VISA tarafında akredite yeni bir finansal elektronik sertifika hizmet sağlayıcısının (ESHS) kurulması gerekliliği vardır. TSM merkezleri bu otoriteleri genellikle kendileri kurmuşlardır. Önerilecek modelde, bu modele uygun olacak sertifika yönetim yapısı makalenin 3. bölümünde açıklanacaktır.

GİB Bilgi Sistemlerine veri aktarma, ilgili dokümanlarda [4,5] 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 Ortak Kriter Koruma Kılavuzuna uygun şartları [11,12] da sağlamalıdır.

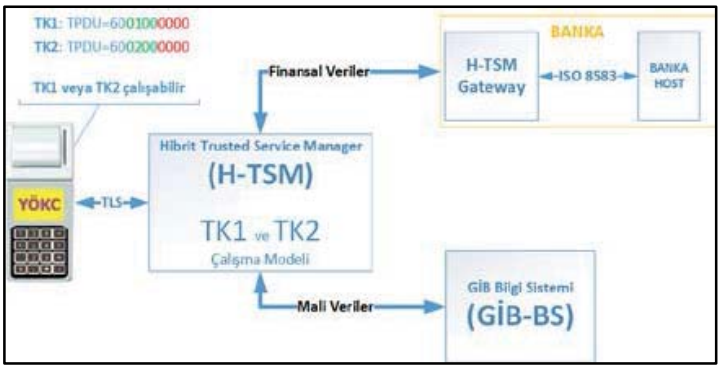
GİB'in yayınladığı teknik kılavuzlara göre [2 ve 3] TSM, 2 (iki) modelde çalışmaktadır. Günümüzde bazı YN ÖKC üreticileri TK1 çalışma modeliyle çalışırken bazıları da TK2 çalışma modeliyle çalışmaktadır. Her ne kadar TSM, tanım olarak her iki modelde [2 ve 3] aynı şekilde tanımlanmış olsa da yapısal olarak farklı işleyişlerde olmaya yatkındır. Sistem münhasırlığı sağlandığı müddetçe TSM'ler birden fazla YN ÖKC üreticisine hizmet verebilir. Dolayısıyla gerekli sistem münhasırlığını sağlayarak aynı TSM yapısını melez çalıştırmak veya aynı üreticinin farklı çalışma modelini destekleyen farklı modelleri için aynı TSM sistemini melez çalıştırmak bu önerilen model ile mümkün olacaktır. Böylelikle mali işlemler ve mesajlar için maliyetler ortaklaştırılabilecek ve yönetim kolaylaşabilecektir.

3. Melez TSM (H-TSM) Modeli

Yukarıdaki bölümlerde aktarıldığı gibi GİB tarafından yayınlanmış teknik kılavuzlara göre 2 (iki) model olarak ayrı TSM merkezleri olarak çalışabilmektedir. Mevcut durumda her iki modeli destekleyen bir TSM olmadığı görülmektedir. Ancak detaya girilmeksizin incelendiğinde bu 2 (iki) modelin birbirinden çok farklı olmadığı ve melez bir TSM modelinin tasarlanmasının mümkün olduğu düşünülmektedir. TSM merkezlerinin her bir YN ÖKC üreticisi (farklı cihazlar) için sistem münhasırlığını sağlaması gerekmektedir. Bir TSM merkezi fiziksel ve/veya sanal sistem ayrımını sağladığı müddetçe istediği kadar YN ÖKC üreticisinin TSM merkezi olabilmektedir [12]. Eğer bir YN ÖKC üretici firmasının, hem TK1 hem de

TK2 çalışma modeli TSM altyapısına uygun çalışabilir cihaz modelleri mevcutsa, önerilen bu H-TSM ile sistem, daha etkin ve az maliyetli olarak kullanılabilir. Çünkü TSM merkezinin, aynı YN ÖKC üreticisi firma için yeniden ikinci bir sistemi TK1 veya TK2 çalışma modeli olarak kurmasına gerek kalmayacaktır. Melez çalışan bir sistem ile kurulmuş tek bir sistem üzerinden 2 (iki) TSM çalışma modelini gerçekleyebiliyor olacaktır.

Bununla birlikte oluşturulacak bu H-TSM modelinin PCI-DSS [19] ve PIN güvenlik gereksinimlerini [20] karşılayacak güçlü bir anahtar yönetim mekanizmasını da sağlaması, esnek ve tümleşik bir TSM merkezinin kurgulanmasına salık verecektir. Günümüzde halen kullanımda olan geleneksel POS cihazları doğrudan bankaya bağlı olan sistemlerdir. Ancak YN ÖKC ile arada TSM merkezleri olduğundan taşınan finansal işlemlerin ekstra güvenli hale getirilmesi ve araya adam girme saldırılarına karşı güçlü bir şifreleme altyapısına sahip olması gerekmektedir. Böylelikle TSM merkezlerinin finansal işlemlerdeki sorumluluğuna karşılık çok gizli finansal iletişim bilgisinin güvenli hale getirilmesi sağlanmış olacaktır. Günümüzde bankacılık uygulamalarında mesajlaşma için kullanılan genel ISO 8583 mesaj formatında, bankaya özel alanların (reserved) her bankada farklı kullanılması bu mesaj formatında farklı ek işlemleri yapan tek bir formatı mümkün kılamamaktadır. Bankaların yürüttüğü bankacılık işlemleri, yazılım ve parametre yükleme/güncelleme işlemleri, gün sonu işlemleri ve anahtar yönetim işlemleri bulunmaktadır. Ancak bankaların, POS yazılımı ile haberleşmesinde araya giren TSM merkezinden dolayı bu işlemleri TSM'e devretmesi veya TSM bilgisi dahilinde dolaylı yönetmesi gerekmektedir. Dolayısıyla yeni geliştirmelerin yapılması ve bu YN ÖKC dünyasına uyarlanması gerekecektir. Tüm bu ihtiyaçlar çerçevesinde TLV mesaj iletişim yapısıyla işleyen H-TSM çalışma modeli önerilmektedir (Şekil 3). Bu modelle birlikte GMP ile Bankacılık iletişim altyapısının tümleştirilmesi ve birleştirilmesi mümkün hale gelmiş olacaktır.



Şekil 3. H-TSM Genel Mimari Yapı

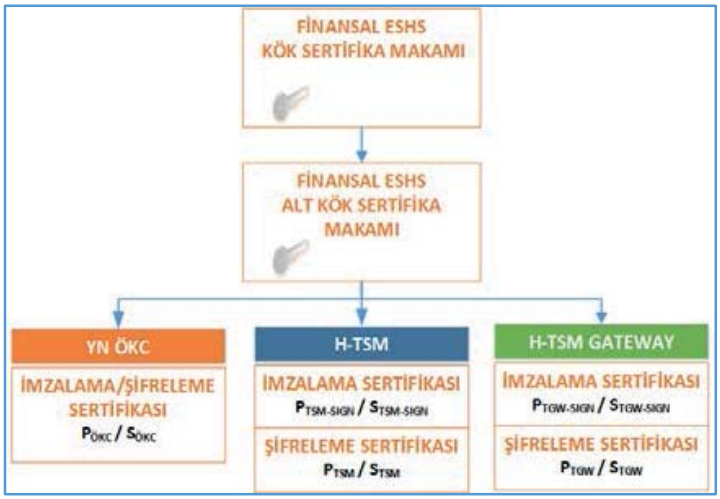
Bu yapıya göre Banka lokasyonunda konumlandırılan, YN ÖKC bankacılık parametre yönetimini ve ISO 8583 mesajlaşma formatını [8] iki yönlü olarak TLV mesaj formatına dönüştüren ve güvenli mesajlaşma yapısını Banka tarafına taşıyan bir H-TSM gateway düşünülmüştür. Böylelikle YN ÖKC-Banka arasında şeffaflık sağlanacak ve aynı zamanda yönetimi kolaylaştıracak kendi içinde güvenli bir iletişim ekosistemi oluşturulmuş olacaktır. Geleneksel POS mimarisine yatkın olan bankacılık uygulamalarının ISO 8583 formatındaki mesajlarının uçtan uca TLV olarak taşınması ve hem H-TSM gateway tarafında hem de YN ÖKC üzerinde koşan Bankacılık uygulamalarıyla haberleşecek küçük dönüştürme uygulamalarıyla sağlanacaktır. TK1 ile TK2 TSM modelinin en bariz farkı olan TLS (Transport Layer Security) v1.2'nin YN ÖKC ile TSM arasında tesis edilmesiyle melez TSM merkezinin desteklenmesi ve TLV tipinde bankacılık mesajlaşma altyapısının birleştirilmesi mümkün olacaktır. Bu melez TSM modeli mevzuatlar ve teknik kılavuzlarla kendisi için tanımlanmış sorumlulukları, bankanın banka uygulaması tarafındaki müdahilinin az veya çok olmasına bakılmaksızın esnek ve tümleşik olarak sağlar niteliktedir. GMP protokolünün mesaj yapısında bahsedilen ve YN ÖKC ile TSM arasında kullanılması öngörülen TPDU değeri, TK1 ve TK2 çalışma modeli seçiminde mesaj bazında ayrım için kullanılacaktır. Toplam 5 bayt olarak tanımlanan ve her GMP mesajında olan bu başlık sayesinde gelen mesajdan hangi modelde çalışan TSM'in seçimini yapmak mümkün olacaktır.

3.1. Finansal Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)

Bankacılık sisteminde debit/kredi kartlarının 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 uzun vadede sağlaması zorlanmaktadır. Mevcut geleneksel POS'larda sertifika temelli güçlü bir anahtar yönetim alt yapısı henüz bulunmamaktadır.

Bu mimari yapıda banka, POS dünyasında kendisinin yaptığı işlemleri yine yapabilir olacaktır. Ancak anahtar yönetimini H-TSM, bankanın altyapısına bakmaksızın kendi iletişim ekosistemi içerisinde güçlü bir şekilde yapabilecektir. Banka kendi anahtar yönetimini banka tarafında konumlandırılan H-TSM Gateway (TGW) ile, anahtar yönetimi basit veya karmaşık olmasına bağlı olmaksınız ISO-8583 formatına veya başka bir yöntemle uygun bir şekilde devam edebilir olacaktır. TGW, üzerinde yazılım koşan bir sunucu rolündedir. TGW, banka içerisinde konumlanacağı için bankacılık işlemlerinde banka sunucuları ile iletişimde basit anahtar yönetimi yapması sorun teşkil etmeyecektir. H-TSM bu haberleşmenin önüne bir katman daha koyarak 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 standartlarına karşılar nitelikte olmuş olacaktır.

Visa anahtar değişimi için 3 (üç) yıllık kullanım süresinin geçmemesini önermektedir. Ancak YN ÖKC için verilen sertifikalar daha önceki bölümlerde de belirtildiği gibi YN ÖKC ekonomik ömrü kadar, yani 10 (on) yıllıktır. Kurulacak olan yeni sertifika otoritesi mali sertifika otoritesine benzer mimaride olacaktır (Şekil 4). Böylelikle bu yapı GİB tarafından yetkilendirilmiş ESHS olarak tanınması durumunda ileride mali sertifikalar için de kullanılabilir olması mümkün olacaktır.



Şekil-4: Finansal ESHS ile Genişletilmiş Sertifika Yapısı

PCI-DSS isterlerine uygun olarak hassas verilerin terminalden bankaya kadar uçtan uca şifreli ve ayrıca TSM merkezlerinin de içeriğini elde edemeyeceği bir şekilde taşınıyor olması sağlanacaktır. Bunun için H-TSM Gateway ucu da ayrı bir host gibi sertifikalandırılacaktır. H-TSM Gateway tamamen bankanın kontrolünde olan ve sunucu anahtarların yönetimini bankaya sunan bir alt yapıda olacaktır.

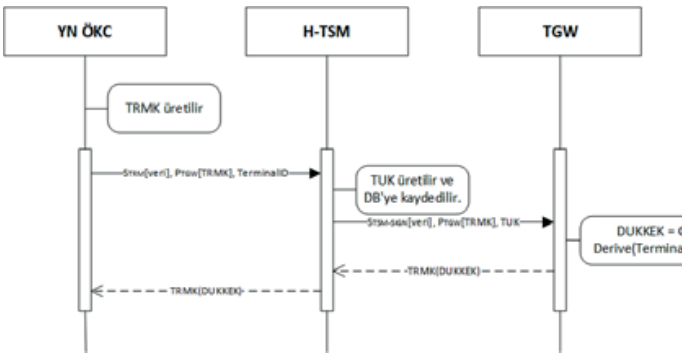
3.2. Anahtar ve Sertifika İlk Kurulumları

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. (P: Public - açık anahtar gösterimi, S: Secret - gizli anahtar gösterimi, C: certificate - Sertifika gösterimidir)

H-TSM Gateway, banka için tıpkı uzaktaki bir POS cihazı gibidir. H-TSM Gateway (TGW), 2 dünyayı birbirinden ayırarak dönüşümleri gerçekleyecektir. H-TSM Gateway ilk kez bankaya kurulurken, Banka hostu ile güvenli iletişim için ZMK (Zone Master Key) simetrik anahtar yüklemesi yapılması gerekmektedir. Bankalar güvenli anahtar paylaşımında bu güvenli alanı oluşturmak için ZMK simetrik anahtarını kullanmaktadır. ZMK, banka sunucusundaki HSM (Hardware Security Module) tarafından 3 anahtar komponenti olarak üretilir. HSM cihazı, güçlü kriptografik işlemleri yapabilen özelleşmiş bir donanımsal güvenlik cihazıdır. Üretilen ZMK, 3 komponent olarak banka anahtar

sorumluları gözetiminde H-TSM Gateway sunucusuna ait HSM cihazına tek tek girilir. İlk kurulumda H-TSM Gatewaye (TGW) ait imzalama ve şifreleme açık anahtarları ($P_{TGW-SIGN}$, $S_{TGW-SIGN}$,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) adında bir simetrik anahtar üretilir. 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 şifreli veya HSM cihazında güvenli bir şekilde kayıtlı olmalıdır. Böylelikle TGW ilk haberleşmesinde H-TSM merkezi ile anahtar değişimi yaparak H-TSM'e ait sertifikaları kendisine alabilir olacaktır.

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 blok değerini şifrelemek için kullanılır. 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 aşağıdaki akıştaki gibi paylaşmalıdır (Şekil 5).



Şekil-5: YN ÖKC – TGW arasında veri anahtarı paylaşımı.

TGW'de herhangi bir veritabanı bulunmaz. Böylelikle işlemleri şifreleme, şifresini çözme ve dönüştürme süreci görevleri dışında herhangi bir veritabanı kaydı yapmayacağından hızlı işlem iletimini de sağlamış olacaktır. YN ÖKC ile TGW arasında ortak anahtar H-TSM tarafından gönderilen bilgilere göre GMK anahtarından türetilir. Derived Unique Key - Key Encryption Key (DUKKEK), GMK anahtarından türetilen simetrik bir anahtardır. Terminal Unique Key (TUK) türetme için kullanılan ve türetmeyi farklılaştıran başka bir anahtardır.

3.3. PIN Anahtar Paylaşımları

YN ÖKC ile banka arasında PIN bilgisi paket şifresinden bağımsız ayrı bir simetrik anahtarla şifrelenerek iletilmelidir. Önerilen modelde bu anahtarın yönetimi H-TSM ile yapılır. Bankacılık uygulaması sadece H-TSM gateway ile anahtar yönetimi yaparken, YN ÖKC ile H-TSM Gateway arası iletişim anahtar yönetimi bu model içindedir. PIN blok 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 veritabanında LMK (Local Master Key) ile şifreli olarak saklanır. LMK, gizli anahtarları şifreli olarak tutmak için kullanılan bir anahtardır. İşlemler esnasında ilgili uçlara ait gizli anahtar (Sembolü S) ile veriler imzalanır ve bu verilerin uçlar tarafından gönderen açık anahtarı ile (Sembol P) doğrulanması sağlanır. İlgili işlemler aşağıdaki çizelgede sunulmuştur.

Çizelge-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.	-
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.

3.4. Güvenli Finansal İşlem

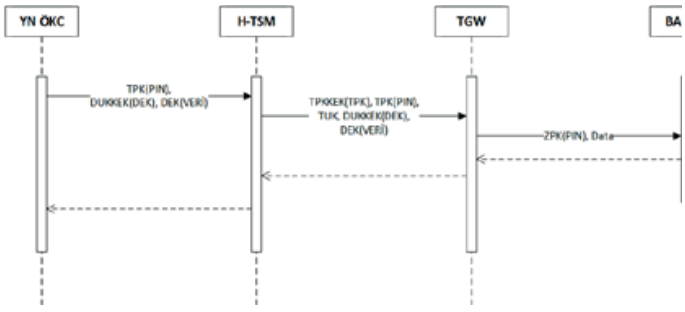
YN ÖKC ile kredi/debit kartıyla yapılan ödemelerde TSM üzerinden bankaya bir finansal işlem akışı söz konusudur. Bu çalışmada önerilen H-TSM ile PIN içeren bir finansal işlemin, nasıl güvenli olarak ve PIN güvenlik standartlarına uygun olarak iletildiği açıklanacaktır. Öncesinde gerekli anahtarlar uçlar arasında güvenli bir şekilde paylaşılmış ve güvenli saklama yöntemleriyle saklanmıştır. Nihai durumda modelimizde bulunan uçların sahip olduğu anahtar çizelgesi aşağıda sunulmuştur.

Çizelge-2: Güvenli Finansal İşlemde İlk Anahtarlar

YN ÖKC	H-TSM	TGW	BANK A
$S_{ÖKC}$	$S_{TSM-SIGN}$ S_{TSM}	$S_{TGM-SIGN}$ S_{TGM} ZMK GMK	ZMK
Sonraki işlemlerle aşağıdaki anahtarlar üretilir.			
DUKKEK TPK	TPKKEK TPK TUK	ZPK TPKKEK DUKKEK *	ZPK

*: DUKKEK = GMK Derive(TerminalD, TUK)

İşlem anında finansal akış aşağıdaki şekildedir (Şekil6).



Şekil-6: PIN İçeren Güvenli Finansal İşlem

PIN blok 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 anahtarını 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 anahtarı ile açar. Hassas veri grubundan TPK(PIN) bilgisini kendisine H-TSM ile gönderilen TPK ile açar. Öncesinde tabii ki TPK'yı kendisinde bulunan TPKKEK anahtarı ile açmıştır. Bankaya finansal işlemi göndermeden önce ZPK ile PIN blok bilgisini tekrar şifreler. Böylelikle hassas veri H-TSM üzerinden görülmeden, YN ÖKC ile Banka arasında iletilmiş olur.

Sonuç olarak YN ÖKC – H-TSM ile YN ÖKC – Banka iletişimde güvenli ve birbirinden bağımsız mesajlaşması mümkün olmaktadır. TGW, mesajları banka hostuna iletirken H-TSM ekosisteminden mesajı çıkaracak ve bankaya ait ekosisteme göre tekrar kodlayacaktır. Bu sayede banka bağımsız olarak sistemin her YN ÖKC ve bankaya göre kolayca çalışması mümkün hale gelmiş olacaktır.

4. Sonuç ve Öneriler

TSM merkezlerinin esas kuruluş amacı ödeme iletişimi altyapısı sağlayarak, ödeme iziyle mali izi örtüştürmek ve takip etmek adına aracılık yapmaktır. Yeni nesil ödeme kaydedici cihazlar ileriki yıllarda yaygınlaşarak bütün sektörlerde kullanılabilir olacaktır. Akaryakıt sektörü ve 6493 sayılı kanunla kurulmuş elektronik para kuruluşları bunlardan bazılarıdır. 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 uygulamalarında 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. Örneğin akaryakıt satışına özgü bilgilerin TSM üzerinden akması ile petrol şirketlerinin yürüttüğü sadakat kartı, hediye kartı, vb. kart bilgilerinin güvenli olarak taşınması ve petrol

şirketlerine iletilmesinde de TSM kullanılabilir. Sadakat sisteminde müşteri bilgileri de aynı banka bilgileri hassasiyeti ile ilgili petrol şirketleriyle yapılacak güvenli haberleşme altyapısıyla iletilmesi sağlanabilir.

Ülkemizde kullanılan diğer bir hizmet ise e-fatura hizmetidir. E-fatura, Vergi Usul Kanunu 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 [21]. Sonuç olarak e-fatura kullanabilen mükelleflerin müşterileri de, YN ÖKC ile alışverişlerinde e-faturalarını TSM vasıtasıyla mail adresine alabiliyor olması da, entegrasyonlarla mümkündür.

Bu çalışmada önerilen bu güvenli H-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 ve uyabileceği söylenebilir. Özellikle her türlü ödeme bilgisinin 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.

Teşekkür

Bu çalışmada ve bu konunun seçiminde bana yardımcı olan ve etkin yönlendirmesi ile her anlamda destek olan değerli hocam Prof. Dr. Ali Aydın SELÇUK'a teşekkürü bir borç bilirim.

5. Kaynaklar

[1] 69,70 seri No'lu ÖKC Genel Tebliğleri ve 426-427-435-437-450-451-465-466 Sıra No'lu VUK 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 Yayın No: 87, "Kayıtdışı Ekonomiyle Mücadele Stratejisi Eylem Planı (2008-2010)", 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

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

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

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

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

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

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

[16] MasterCard, M/Chip Program Guide, 29.01.2015.

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

[18] TÜBİTAK BİLGEM Ortak Kriterler Test Merkezi (OKTEM), "KamuSM Sertifikaları ve İşlevleri", Yeni Nesil ÖKC Detay Kılavuzu v1.6, s.28-30, 14 Mayıs 2015.

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

[20] Payment Card Industry (PCI) PIN Security Requirements, Version 2.0, Aralık 2014

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