ÖZET

Güvenlikli ödeme alıcı cihaz için bir yöntem

Buluş; ödeme yapan temassız ödeme kartlar veya temassız ödeme yapabilen dijital cüzdanlardan (ApplePay, SamsungPay, AndroidPay, GooglePay veya herhangi özel HCE tabanlı veya diğer dijital cüzdanlar) veya EMV tabanlı veya özel desenli QR ile ödeme kabul edebilen herhangi bir mobil cihaz (telefon, tablet, vs.) üzerinde çalışan işletim sistemi (Android, iOS, vs.) üzerinde koşan, yazılım ve cihaz işlemcisi üzerinde yer alan güvenli çalıştırma ortamı (TEE – Trusted Execution Environment) vasıtasıyla kripto anahtarlar, hassas veri ve dijital varlığın güvenliğinin sağlandığı yazılımsal ödeme alıcı cihaz (POS) için bir yöntem ile ilgilidir.

(Şekil 1)

İSTEMLER

1. Ödeme yapan temassız kartlar (1) veya temassız ödeme yapabilen dijital cüzdanlardan veya EMV tabanlı veya özel desenli QR ile ödeme kabul edebilen herhangi bir mobil cihaz (10) üzerinde çalışan işletim sistemi üzerinde koşan kripto anahtarlar, hassas veri ve dijital varlığın güvenliğinin sağlandığı yazılımsal ödeme alıcı cihaz / POS için yöntem olup, özelliği;

- Kart sahibi kuruluşun (20) mobil uygulamayı (100) indirip sisteme başvurusunu yapması (1001),
- Kart sahibi kuruluşun (20) kaydı yapıldıktan sonra hassas verilerin gizliliğinin, bütünlüğünün korunması için gerekli anahtarların sunucu uygulaması (16) tarafından üretilmesi (1002),
- Anahtarların SDK'ya (12) indirilmesinden sonra yazılım tabanlı olarak Kripto Yöneticisine (14) enjekte edilmesi ve cihaza özel tekil veriler ile bağlantılı olarak kaydedilmesi (1003),
- Ödeme kartının (1) mobil cihaza (10) yaklaştırıldığında NFC anteni (15) tarafından algılanıp SDK'ya (12) bildirilmesi (1005),
- SDK'nın (12), çekirdek birimini (13) çağırarak ödeme işlemini başlatması (1006),
- Çekirdek biriminin (13) ödeme kartına (1) gerekli komutları göndererek temassız ödeme işlemi yapması (1007),
- Çekirdek birimi (13) tarafından temassız ödeme işlemi sonucunun SDK'ya (12) aktarılması (1008),
- Ödeme kartından (1) okunan hassas verilerin Kripto Yöneticisi (14) ile Whitebox formundaki anahtarlar ve Whitebox şifreleme algoritması ile korunarak sunucu uygulamasına (16) iletilmesi (1009),
- Sunucu uygulamasından (16) ödeme alıcı kuruluşa (19) ödeme işleminin otorizasyonu için işlem mesajı iletilmesi
    - Ödeme alıcı kuruluş (19) kart sahibi kuruluşa (20) otorizasyon mesajını iletmesi,
    - Kart sahibi kuruluş (20) gerekli kontrolleri yaptıktan sonra otorizasyon sonucunu ödeme alıcı kuruluşa (19) dönmesi,
    - Ödeme alıcı kuruluşun (19), aldığı otorizasyon sonucunu sunucu uygulamasına (16) iletmesi,
    - Sunucu uygulamasının (16) işlem bilgilerini veritabanına (18) kaydettikten sonra SDK'ya (12) işlem sonucunu dönmesi

  (1011),

- SDK (12) işlem sonucunu pos birimine (11) iletmesi ve pos biriminin (11) işlemin sonucuna (başarılı/başarısız) göre ilgili mesajı kullanıcıya göstermesi (1012)

işlem adımlarını içermesidir.

2. İstem 1‘ e uygun yöntem olup, özelliği; 1003 numaralı işlem adımından sonra; kart sahibi kuruluşun (20) pos birimi (11) ekranından ödeme tutarını girmesi ve bu bilginin SDK'ya (12) gönderilerek ödeme işleminin başlatılması (1004) işlem adımını içermesidir.

3. İstem 1‘ e uygun yöntem olup, özelliği; 1009 numaralı işlem adımından sonra; sunucu uygulamasında (16) şifreli alanların donanımsal güvenlik modülü (17) içerisinde cihaz anahtarı ile çözülüp ödeme alıcı kuruluş (19) anahtarlarıyla şifrelenmesi (1010) işlem adımını içermesidir.

TARİFNAME

Güvenlikli ödeme alıcı cihaz için bir yöntem

Teknik Alan

Buluş; ödeme yapan temassız ödeme kartlar veya temassız ödeme yapabilen dijital cüzdanlardan (ApplePay, SamsungPay, AndroidPay, GooglePay veya herhangi özel HCE tabanlı veya diğer dijital cüzdanlar) veya EMV tabanlı veya özel desenli QR ile ödeme kabul edebilen herhangi bir mobil cihaz (telefon, tablet, vs.) üzerinde çalışan işletim sistemi (Android, iOS, vs.) üzerinde koşan, yazılım ve cihaz işlemcisi üzerinde yer alan güvenli çalıştırma ortamı (TEE – Trusted Execution Environment) vasıtasıyla kripto anahtarlar, hassas veri ve dijital varlığın güvenliğinin sağlandığı yazılımsal ödeme alıcı cihaz (POS) için bir yöntem ile ilgilidir.

Tekniğin Bilinen Durumu

Günümüzde kullanılan ödeme alıcı cihazlar tamamen kapalı devre çalışan donanımsal cihazlardır. Dolayısıyla gerekli kriptografik anahtarlar üye işyerine gönderilmeden önce ödeme alıcı kuruluş tarafından belli bir lokasyonda yüklenmektedir. Ödeme alıcı cihazların kurulumu, yazılımlarının güncellenmesi, yazılımsal olarak bozulduğunda, işlev görmediğinde uzaktan müdahale edilemediği için saha operasyon ekiplerine ihtiyaç duyulmaktadır.

Teknik araştırmalar sonucunda ortaya çıkan 2018/08160 numarasına sahip başvurunun özeti; “Açık iletişim ağları üzerinden iletime yönelik ödeme verilerinin güvence altına alınmasına yönelik bir yöntem açıklanır. Yöntem, bir birinci ve ikinci bir alıcı-verici cihaz arasında bir veri bağlantısı kurulmasını içerir, birinci alıcı-verici cihaz, bir satıcı cihazı olarak konfigüre edilir ve ikinci alıcı-verici cihaz, bir müşteri alıcı-verici cihazı olarak konfigüre edilir. Satıcı cihazı, veri bağlantısı üzerinden müşteri alıcı-verici cihazına bir benzersiz satıcı tanımlayıcı ve işlem talebi verisi içeren bir birinci veri paketini iletir. Satıcı cihazı, müşteri alıcı-verici cihazından bir şifreli yazı alır. Şifreli yazı, alınan benzersiz satıcı tanımlayıcı ve geçiş talebi verisi ile birlikte bir gizli anahtar ve bir sayaç değeri kullanılarak oluşturulmuştur. Yöntem, alınan şifreli yazı, satıcı tanımlayıcı ve işlem talebi verilerini alan bir onay talebinin oluşturulması ve söz konusu onay talebinin, söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum ve bir alıcıdan en az birine sunulmasını içerir.”

Teknik araştırmalar sonucunda ortaya çıkan bir diğer başvuru olan 2017/01092 numaralı patentin özeti, “Buluş, müşteri uzaktan servis için ödeme ve iletişim bağlantıları bir sistem ile ilgilidir. Sistem bir satıcı değerlendirmesi üretmek için bir birim oluşur, aşağıdaki birbirine üniteleri içeren tek bir sistem sunucusu: hızlı erişim düğmesi, bir bilgi depolama ünitesi, bir ünite ile donatılmış bir merkezi kontrol ünitesi, emir ve komisyon üretmek için bir birim, bir sorgu yönlendirme bağımsız bir bilgi tedarikçiden bir cevap almak ve bir bildirim üretmek için, cihaz önermek otomatik bir filtre, bir öneri ve tavsiye birimi, emir ve komisyon uygulanması için bir birim içeren söyledi bir alıcı sorunu bir ücretli mektup tek bir sistem sunucuya bağlı olan kredi ve gelecekteki işlemler için şablonlar oluşturmak için bir birim ve alıcı bilgisayarlar, yerel bilgi ve ödeme ağına içi sistem bağlantı kanalları tarafından entegre ve kablosuz bağlantı kanalları boyunca birbirleriyle etkileşim vardır bir satıcı değerlendirmesi üretmek için birim tek bir sunucuya bağlı olan bağımsız bir bilgi ve satıcı değerlendirmesi tedarikçisi, bir sunucu teşkil burada internet.” şeklindedir.

Özetleri verilen mevcut başvurular, yukarıda sözü edilen olumsuzluklara çözüm getirmeyi amaçlayan bir yeniliğe sahip değildir.

Sonuç olarak yukarıda anlatılan olumsuzluklardan dolayı ve mevcut çözümlerin konu hakkındaki yetersizliği nedeniyle ilgili teknik alanda bir geliştirme yapılması gerekli kılınmıştır.

Buluşun Amacı

Buluş, mevcut teknikte kullanılan yapılanmalardan farklı olarak bu alanda yeni bir açılım getiren farklı teknik özelliklere sahip bir yapının ortaya koyulmasını amaçlamaktadır.

Buluşun öncelikli amacı; geleneksel POS cihazlarında donanımsal ve kapalı devre network ile sağlanan güvenliğin, yazılımsal olarak Whitebox kriptografiden ve/veya ilgili mobil işletim sisteminin güvenli çalıştırma ortamının (TEE - Trusted Execution Environment) sunduğu güvenli ortamdan faydalanılarak sağlamaktır

Buluşun bir amacı, mobil aplikasyon formatında olarak yazıldığı mobil işletim sistemi üzerinde çalışan, geleneksel donanımsal POS cihazlarının tüm işlev setini aynen karşılayan bir yöntem ortaya koymaktır.

Buluşun yapısal ve karakteristik özellikleri ve tüm avantajları aşağıda verilen şekiller ve bu şekillere atıflar yapılmak suretiyle yazılan detaylı açıklama sayesinde daha net olarak anlaşılacaktır ve bu nedenle değerlendirmenin de bu şekiller ve detaylı açıklama göz önüne alınarak yapılması gerekmektedir.

Buluşun Anlaşılmasına Yardımcı Olacak Şekiller

Şekil 1,buluşa konu olan yöntemin gerçekleştirilmesini sağlayan unsurların genel gösterimidir.

Şekil 2, buluşa konu olan yöntemin akış diyagramının gösterimidir.

Çizimlerin mutlaka ölçeklendirilmesi gerekmemektedir ve mevcut buluşu anlamak için gerekli olmayan detaylar ihmal edilmiş olabilmektedir. Bundan başka, en azından büyük ölçüde özdeş olan veya en azından büyük ölçüde özdeş işlevleri olan elemanlar, aynı numara ile gösterilmektedir.

Parça Referanslarının Açıklaması

1. Ödeme kartı (temassız kart)
10. Mobil Cihaz
100. Mobil uygulama
11. Pos birimi (UI/UX)
12. SDK
13. Çekirdek birimi (Kernel)
14. Kripto Yöneticisi
15. NFC (Yakın alan iletişim) anteni)
16. Sunucu uygulaması
17. Donanımsal güvenlik modülü (HSM)
18. Veritabanı
19. Ödeme alıcı kuruluş
20. Kart sahibi kuruluş

Buluşun Detaylı Açıklaması

Bu detaylı açıklamada, buluşun tercih edilen yapılanmaları, sadece konunun daha iyi anlaşılmasına yönelik olarak ve hiçbir sınırlayıcı etki oluşturmayacak şekilde açıklanmaktadır.

Ödeme yapacak kart sahibi kuruluş (20), öncelikle ödeme alıcı kuruluşa (19) başvurusunu yapıp gerekli prosedürü yerine getirdikten sonra sisteme kaydını yaptırmaktadır.

Kart sahibi kuruluş (20) buluşa konu olan mobil uygulamayı (100) kullanmak için mobil cihaza (10) sahip olmalıdır. Kart sahibi kuruluş (20) mobil uygulamayı (100) indirir ve mobil cihaza (10) kurulumunu yapar. Bu noktada mobil uygulama (100) üye işyerinin herhangi bir bilgisini içermeden mobil cihazda (10) bulunur.

Kurulum için kart sahibi kuruluş (19) kullanıcısı kimlik doğrulama bilgilerini mobil uygulamadaki (100) pos birimine (11) girer. Pos birimine (11) girilen kimlik bilgileri Ödeme Alıcı Cihaz (POS) Güvenli Hizmet Yöneticisine (TSM), oradan da Ödeme Alıcı Kuruluşa (19) iletilir. Ödeme Alıcı Kuruluş (19) tarafından aynı yolla pos birimine (11) doğrulama mesajı dönüldükten sonra uygulama yapılandırma verisi ve anahtarların indirilmesi talebini TSM'e iletir. TSM ilgili mobil cihaza özel üretilen anahtar ve parametreleri cihazla ilişkilendirir. Cihaz tekil anahtarları ve Level 2, Level 3 katmanları ve POS'a özel yapılandırma parametreleri mobil cihaza (10) iletilir.

Sunucu tarafına yapılan güvenli bağlantıdan sonra mobil cihaz (10) uygunluk ve güvenlik kontrollerinden geçirildikten sonra güvenlik anahtarları ve gerekli parametreler cihaza indirilir. Kullanıcı ana ekrandan hangi işlemi (satış, iade, iptal, vs.) yapacağını seçer. Örneğin satış işleminde tutarı girerek müşterinin kartı yaklaştırmasını ister.

SDK (12), pos uygulamasına API sunmakta ve çekirdek birimi (13) ile ödeme işlemlerini yönetmektedir. Tüm uygulamanın güvenliğini aşağıdaki kontrolleri uygulayarak sağlar;

- Anti Root/Debug/Hook/Emulatör
- Kaynak kod karıştırılması (obfuscation)
- Dosya okuma, bellek yönetimi, vb. Standart Android kütüphanesi fonksiyonlarının yerine her işlemci mimarisi için assembly seviyesinde yazılan sistem çağrı fonksiyonlarının kullanılması

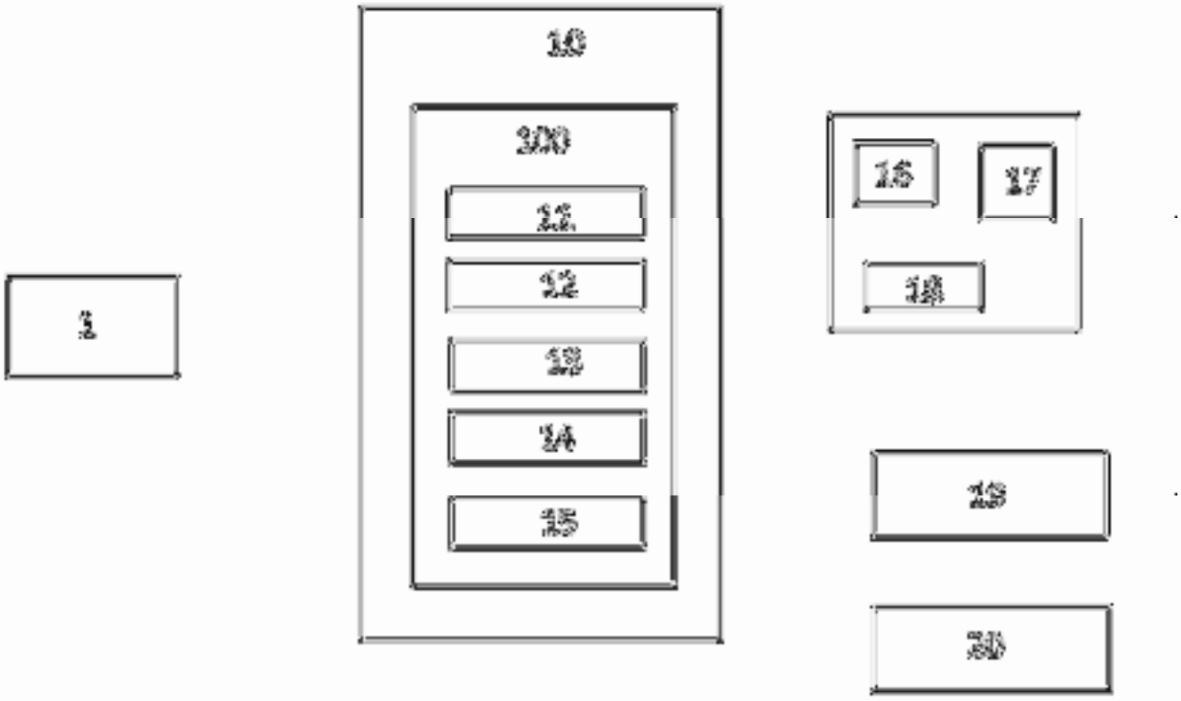
Ödeme şemalarına ait çekirdek uygulamalar çekirdek biriminde (kernel) (13) çalışmaktadır. Kripto yöneticisi (14); geleneksel ödeme alıcı cihazlarda bulunan fiziksel SAM (Secure Access Module) kartın sağladığı güvenlik, anahtar yaratımı ve kriptografik algoritmaların çalışmasını yazılımsal olarak sağlayan kütüphanedir. NFC (15) anteni ile aşağıda belirtilen protokoller ile temassız kartların okunması gerçekleşmektedir; NFC-A, NDEF, NFC-F((JIS) X 6319-4), ISO/IEC 14443(NFC-A ve NFC-B), NFCVE –V.

Buluşa konu olan sistem ile gerçekleştirilen işlem adımları şunlardır;

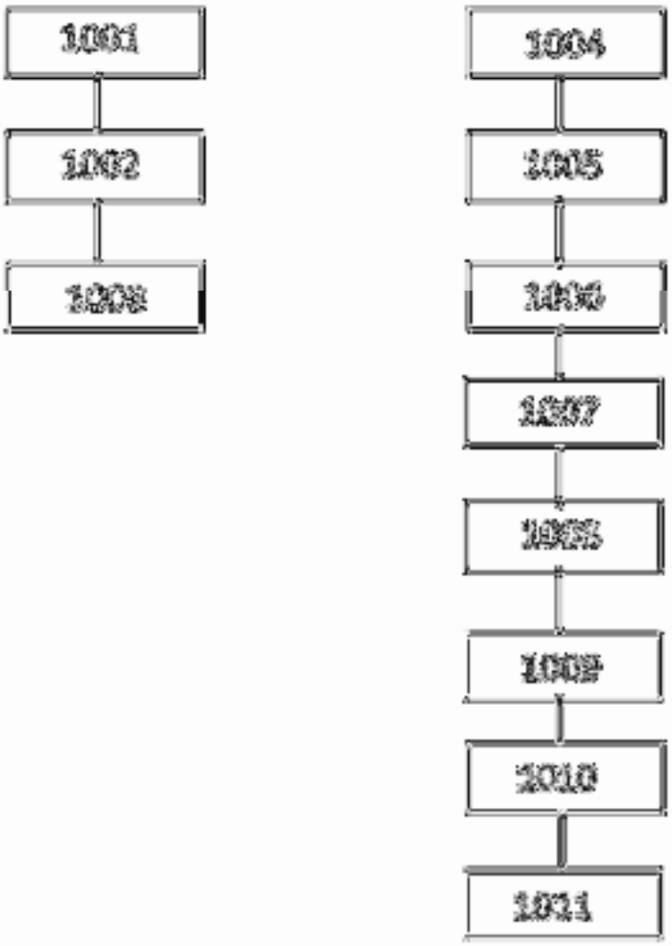
- Kart sahibi kuruluşun (20) mobil uygulamayı (100) indirip sisteme başvurusunu yapması (1001),
- Kart sahibi kuruluşun (20) kaydı yapıldıktan sonra hassas verilerin gizliliğinin, bütünlüğünün korunması için gerekli anahtarların sunucu uygulaması (16) tarafından üretilmesi (1002),
- Anahtarların SDK'ya (12) indirilmesinden sonra yazılım tabanlı olarak Kripto Yöneticisine (14) enjekte edilmesi ve cihaza özel tekil veriler ile bağlantılı olarak kaydedilmesi (1003), (Bu sayede kaydedilen verilerin başka bir cihazda kullanılabilmesi engellenmektedir.)
- Kart sahibi kuruluşun (20) pos birimi (11) ekranından ödeme tutarını girmesi ve bu bilginin SDK'ya (12) gönderilerek ödeme işleminin başlatılması (1004),
- Ödeme kartının (1) mobil cihaza (10) yaklaştırıldığında NFC anteni (15) tarafından algılanıp SDK'ya (12) bildirilmesi (1005),
- SDK'nın (12), çekirdek birimini (13) çağırarak ödeme işlemini (EMV) başlatması (1006),
- Çekirdek biriminin (13) ödeme kartına (1) gerekli komutları göndererek temassız ödeme (EMV) işlemi yapması (1007),
- Çekirdek birimi (13) tarafından temassız ödeme işlemi sonucunun SDK'ya (12) aktarılması (1008),
- Ödeme kartından (1) okunan hassas verilerin Kripto Yöneticisi (14) ile Whitebox formundaki anahtarlar ve Whitebox şifreleme algoritması ile korunarak sunucu uygulamasına (16) iletilmesi (1009), (Bu noktada Whitebox formundaki anahtarlar cihazın belleğinde mobil uygulamanın (100) o anki işlem belirteci (process Id) ile tutulduğundan anahtarlar başka bir cihaz üzerinde veya emülatör üzerinde çalışmamaktadır.)
- Sunucu uygulamasında (16) şifreli alanların donanımsal güvenlik modülü (17) içerisinde cihaz anahtarı ile çözülüp ödeme alıcı kuruluş (19) anahtarlarıyla şifrelenmesi (1010),

- Sunucu uygulamasından (16) ödeme alıcı kuruluşa (19) ödeme işleminin otorizasyonu için işlem mesajı iletilmesi
    - Ödeme alıcı kuruluş (19) kart sahibi kuruluşa (20) otorizasyon mesajını iletmesi,
    - Kart sahibi kuruluş (20) gerekli kontrolleri yaptıktan sonra otorizasyon sonucunu ödeme alıcı kuruluşa (19) dönmesi,
    - Ödeme alıcı kuruluş (19) aldığı otorizasyon sonucunu sunucu uygulamasına (16) iletmesi,
    - Sunucu uygulaması (16) işlem bilgilerini veritabanına (18) kaydettikten sonra SDK'ya (12) işlem sonucunu dönmesi

  (1011),
- SDK (12) işlem sonucunu pos birimine (11) iletmesi ve pos biriminin (11) işlemin sonucuna (başarılı/başarısız) göre ilgili mesajı kullanıcıya göstermesi (1012).



ŞEKİL 1



ŞEKİL 2