Mobil Se-Cüzdan Mimari Tasarımı ve Uygulaması

Rifat ÇÖLKESEN, Ege KİPMAN

Beykent Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ayazağa, 34396, İstanbul.

rifat@colkesen.com, ege_kipman@hotmail.com

Özet: Bu çalışmada, daha önce geliştirilen bir sanal Elektronik Cüzdan (sE-Cüzdan) uygulamasına mimari eklemeler yapılmış ve cüzdana POS makinalarından kablosuz arayüz erişim mekanizması önerilmiştir. Mobil sE-Cüzdan, hem yapısal hem de davranışsal olarak ceplerde taşınan cüzdanların sanal ortamda gerçekleştirilmiş halidir; ödemeler ceplerimizdeki cüzdanlar arasında olduğu gibi karşılıklı yapılmakta veya istenirse, etkileşimlerin kayıt altına alınması istenirse, banka üzerinden yapılmaktadır. Mobil sE-Cüzdan'ı, daha önce yapılan çalışmalardan ayıran en önemli özelliği erişim arayüzüdür; bu amaçla yeni bir kablosuz POS makinası önerilmiş ve cüzdanla etkileşim ilkelleri belirlenmiştir. Daha önceki çalışmamızda, sE-Cüzdan mimarisi bölge kavramına dayandırılmıştı: Askeri, sahip, serbest, banka ve arayüz/taşıyıcı olarak adlandırılan beş adet bölge olup bölgelere erişim farklı erişim haklara dayanılarak yapılabilmekteydi. Bu çalışmamızda cüzdanın mimarisinde ve veri yapısında iyileştirmeler gerçekleştirilmiş ve arayüz/taşıyıcı bölgesi yenilenmiştir. Mobil sE-Cüzdan'ın (Mobile virtual Electronics Wallet) erişim arayüzü kablosuz olarak gerçekleşitirilmekte ve erişim noktalarına en yakın olan, en güçlü sinyali alınan cüzdan'ın sahibi POS makinası üzerinden cüzdanını kullanmaktadır.

Böylesi çalışmaların sonucu elde edilen başarı, e-ödemelerin merkezi olmaktan çıkıp dağıtılmış olmasına öncülük etmesi, bankaların e-etkileşim sayısını azaltması ve fiziksel paranın bankalarda tutulması konularına kaynak olacaktır.

Anahtar Sözcükler: sE-Cüzdan, vE-Wallet, kablosuz erişim, sanal nesne (s-nesne), e-ticaret, e-para.

1. Giriş

Elektronik cüzdan, İngilizce olarak electronics-wallet sözcükleri, genel olarak, elektronik sistemler üzerinden uzaktan ödeme araçları için kullanılması alışagelmiştir. Ancak, yapılan çalışmalara ve uygulamalara bakıldığında bu tür e-cüzdanların, aslında, cebimizdeki cüzdanla pek fazla ilgisi olmadığı, önceden doldurulan nakitlerin harcanması veya kredi kartı benzeri merkezi sisteme bağlanıp ödeme yapılması şeklinde olduğu görülmektedir [Frolund ve ark.-2002][Sakamura ve ark.-2001] [Trichina ve ark.-2001]. Çalışmalarımızda, kısaca "sE-Cüzdan" olarak isimlendireceğimiz elektronik cüzdan sözcüklerine gerçek anlamını verip cebimizde taşıdığımız cüzdanların hem işlevsel hem de davranışsal olarak sanal ortamda uygulamasını gerçekleştirmekteyiz. sE-Cüzdan, cüzdanlarımızda olduğu gibi nakit para, kredi kartı, kimlik kartı, küçük notlar gibi unsurları içermekte ve bunlara ek olarak elektronik dünyasının gelişmelerine ait çeşitli sayısal kimlik ve şifreleri de tutmaktadır.

Bilgisayar ağ ortamlarının yakın zamanda kabuk değiştireceği çeşitli kaynaklarda sıkça dile getirilmektedir. Örneğin, bugüne kadar WAN, LAN, kampüs ağ ve uzak bağlantı olarak yapılan ağ sınıflaması şekil değiştirmiş ve PAN, FAN, CAN olarak yapılmaya başlanmıştır [Çölkesen ve ark.-2008]. PAN (Personel Area Network), kişisel alan ağı; FAN (Family Area Network), ailesel alan ağı ve CAN (Commer-

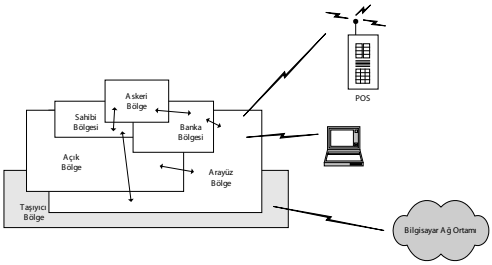
ce Area Network) da Ticari Alan Ağı olarak nitelendirilmektedir. Ağ ortamından beklenen uçtan uca yüksek hızlı geniş-band iletişimin yapılabilmesidir. Dolayısıyla yeni nesil ağ alt yapısının kullanılmasıyla ağ üzerinde elektronik nesnelerin dolaşmasına tanık olacağız ve bunlardan birisi de sE-Cüzdan olacaktır. Kişisel alan ağları, ailesel alan ağları ve ticari alan ağları, IPv6 ve mobil sanal nesneler, yeni nesil ağ uygulamalarının bunlar üzerine kurulacağını öngörmekteyiz ve bizi böylesi çalışmaya iten düşünce de budur.

Görülmüştür ki, ticarette de elektronik ortama geçiş hızlı bir sürece girmiş ve hem kurumsal çalışmalar hem de tüketiciye ulaşma için bu ortam önemli bir araç olmuştur. Günümüzde elektronik ortam üzerinden ticaret yapılması yönündeki engellerden birisinin ödeme şekli olduğu görülmektedir. Özellikle küçük değerli alışverişlerde kredi kartı benzeri araçlar etkileşim maliyeti açısından yeterli olamamakta ve çoğu zaman ödenmesi gereken komisyonlardan dolayı kullanılmamaktadır. Örneğin 10 Ykrş'luk bir alışverişin ödenmesinde zorluklar yaşanmaktadır ve bu da küçük ödemeli alış-verişler için engel olmaktadır. Halbuki, İnternet üzerinden veya genel olarak sanal ortamlardan küçük miktardaki ödemelerin kolayca yapılabilmesi ve bu ödemeler için peşin ödemelerde olduğu gibi herhangi bir masraf verilmemesi ticaretin boyutunu oldukça genişletecektir. [Çölkesen ve ark. - 2002]

2. sE-Cüzdan Mimarisi

sE-Cüzdan, hem yapısal hem de davranışsal olarak ceplerde taşınan cüzdanların benzerinin sanal ortamda bilgisayar ağına bağlı sayısal ortamlarda uygulamasıdır. sE-Cüzdan'ı, daha önce yapılan çalışmalardan ayıran en önemli özelliği TCP/IPv6 ağlar üzerinde hareketli bir nesne olması ve e-etkileşimlerinin cüzdanlar arasında gerçekleştirilmesidir.[Pays ve ark. 1996][Daswani ve ark.-1998]

sE-Cüzdan mimarisi daha önce Çölkesen ve Kipman [2002] tarafından Şekil 1'de görüldüğü gibi bölge (zone) kavramına dayandırılmıştır. Bu bölgeler askeri bölge (militarized zone), sahibi bölgesi (owner zone), açık bölge (public zone), banka bölgesi (bank zone) ve arayüz/taşıyıcı bölgesi (interface/carrier) olarak adlandırılmıştır. Bu bölgelerden arayüz/taşıyıcı bölgesi (interface/carrier zone) birbirinden ayrıştırılarak ikiye ayrılmış ve bölge sayısı 6'ya çıkarılmıştır: arayüz bölgesi (interface zone) ve taşıyıcı bölgesi (carrier zone) olarak ayrı ayır ele alınmıştır. Arayüz bölgesi, cüzdanın sahibi olan kullanıcının cüzdanla etkileşimde bulunmasını, taşıyıcı bölgesi de cüzdanın hareketli nesne olmasını sağlayan taşıma işlemini yapmaktadır. Bu çalışmamızda, arayüz bölgesi için kablosuz POS makinası arayüzü ele alınmıştır. Yani, cüzdana POS benzeri cihazlar üzerinden erişilmesi üzerine geliştirmeler yapılmıştır.



Şekil 1. sE-Cüzdan mimarisi bölgeler

En içteki bölge, askeri bölge (militarized zone) olup mali değeri olan tüm bilgilerin tutulduğu değişkenlerin saklandığı bölgedir. Çeşitli para birimlerine ait değişkenler ve kıymetli kağıtlara ait değişkenler bu bölge içerisinde tutulmaktadır. Bu bölgeye, yalnızca, banka veya cüzdan sahibine ait bölgeler içerisinden "erişim ilkelleri" aracılığıyle erişilebilinir. Diğer bölgeler üzerine askeri bölgeye erişim engellenmiştir.

Sahibi bölgesinde (owner zone) cüzdan sahibine ait özel bilgiler, yalnızca sahibi tarafından görülmesi, erişilmesi istenen bilgiler bulunur. Cüzdan sahibi bu bölgede bulunan bilgilere kendisi erişebildiği gibi bir başkasına da geçici olarak açabilmektedir. Kredi kartlarının elektronik uygulaması olabilecek e-kredi kartları da bu bölgede tutulur.

Banka bölgesinde ise, cüzdanı ilk oluşturan oluşturan veya cüzdana banka yetkileriyle ulaşmaya izni olan banka bilgileri ve temel kontrol bilgileri bulunur. Bu bölgeye yalnızca merkezi otoritenin izin verdiği bankalar erişebilir. Banka bölgesi üzerinden de güvenlik sorgulaması altında askeri bölgeye erişilebilir. Dolayısıyla bir bankanın askeri bölgeye erişmesi için iki düzeyli güvenlik uygulanmaktadır.

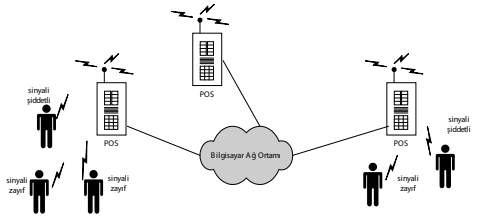
Serbest bölge ise, genele açık bilgilerin bulunduğu bölgedir; bu bölgeye cüzdan kimliğini bilen herkese erişim hakkı vardır. Uygulamaya göre, gerekirse, cüzdan sahibinin fotografı, kimlik bilgileri ve duyuruları koyulabilir..

Taşıma bölgesi (carrier zone) cüzdanın ağ üzerinde IPv6'ya göre cüzdan sahibinin gittiği yere taşınmasını sağlar. Cüzdana yapılan erişimlerin yerel olması sağlayabilmek amacıyla sE-Cüzdan TCP/IPv6 ağ üzerinde hareket edebilme özelliği düşünülmüştür. sE-Cüzdan, temelde sayısal bir nesnedir; elektronik ortamda veriler kopyalandığı her şekilde kopyalanabilir ve taşınabilir.

Arayüz bölgesi (interface zone) cüzdana ait işlevlerin kullanılması için bir arayüz ortamı sunar; arayüz olarak Çölkesen ve arkadaşları [2002] tarafından daha önce cep telefonu, bilgisayar gibi sistemler düşünülmüştür.Bu çalışmada, temel farklılık cüzdana erişimin uç sistemlerle (cüzdanlarla) kablosuz erişim sağlayan POS makinaları aracılığıyla olmaktadır.

Arayüz Bölgesi (Interface Zone)

Arayüz bölgesi, sE-Cüzdan'ın kullanıcı arayüzünü oluşturur; çeşitli arayüz erişim yöntemleri önerilmiştir. Kullanıcı-cüzdan arası etkileşimler arayüz işlevleri aracılığıyla gerçekleştirilir. Yeni öneride, arayüz erişiminin Şekil 2'de gösterildiği gibi uç kullanıcı erişimlerinin kablosuz gerçekleştirildiği POS makinaları üzerinden sağlanmasıdır.



Şekil 2. POS cihazı üzerinde erişim

3. sE-Cüzdan İşlevleri

Mimari yapısı Şekil-1'de verilen sE-Cüzdan'ın içereceği bilgiler ve işlevleri, temel olarak, Tablo-1'de verilmiştir.

§ İçerisinde sanal para (e-para) veya kıymetli evrak (e-evrak) taşıyabilmeli

§ Sanal banka veya kredi kartları (e-kart) taşıyabilmeli

§ Sanal çek defteri (e-çek) taşıyabilmeli

§ Küçük notlar içeren belgeler taşıyabilmeli

§ Bireysel veya Kurumsal e-para aktarımı yapılabilmeli

§ Kolay kullanılabilir ve erişilebilir kullanıcı arayüzü: Cep telefonu, bilgisayar, POS

§ Mahremiyet özelliğini sağlayabilmeli

§ sE-Cüzdan nesnesinin sayısal ortamlar üzerinde taşınabilmesi ve hareket etmesi özelliği
§ Fiziksel olarak kullanılan cüzdanın tüm işlevsel özelliklerini sağlamalı
§ Cüzdan kaybolduğunda veya çalındığında kolayca bulunabilmeli ve kayıplar en az olmalı
§ İşaret şiddetine duyarlı kablosuz arayüz erişim özelliği

Tablo 1. sE-Cüzdan'da olması gereken özellikler

4. E-Etkileşim

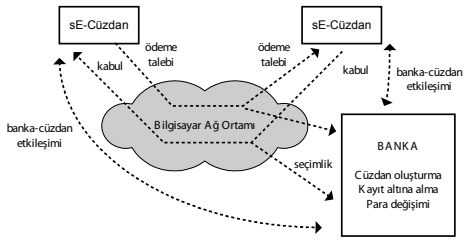
Cüzdanlararası işlemler veya cüzdan ile erişim arayüzü arasındaki işlemler önceden tanımlanmış iletişim ilkelleri aracılığıyla yapılır. İki cüzdan arasında etkileşim (para aktarımı vs.) yapılabilmesi için önce arayüz bölgeleri arasında oturum (session) kurulur. Bu oturum için herhangi bir güvenlik sorgulamasına gerek duyulmaz. Kimliği bilinen herhangi bir cüzdanın arayüz bölgesine oturum kurulabilir. Oturum kurulduktan sonra açık bölgedeki sahip bilgilerine ulaşılabilir. Ancak, daha iç bölgelere erişim yapılabilmesi için "erişim hakkı" sınaması yapılır. En iç bölge olan askeri bölgeye erişim iki düzeyli güvenlik sorgulaması üzerinden yapılır.

Ödemeler ceplerimizdeki cüzdanlar arasındaki olduğu gibi karşılıklı yapılmaktadır. sE-Cüzdan, merkezi yönetimli olmayıp dağıtılmış bir mimariye sahiptir. Merkezi otorite konumdaki bankaların işlevleri ise ilk olarak cüzdanın yaratılması, fiziksel para-sanal para dönüşümünün yapılması ve cüzdan sahibinin istemesi durumunda cüzdanlar arası e-etkileşiminin kayıt altında tutulmasıdır.

e-Etkileşim, Şekil 3'te görüldüğü gibi cüzdanlararası veya cüzdan ile banka arasında olmaktadır. Cüzdanlararası e-etkileşim, daha çok para gibi mali değeri olan bilgilerin değiş-tokuşunda gerekli iken; cüzdan ile banka arasındaki e-etkileşim cüzdana e-para koyulması, e-paranın fiziksel para haline dönüştürülmesi, cüzdanının yasallığının denetimi gibi işlemler için gerekmektedir.

sE-Cüzdan – Banka

sE-Cüzdan teknolojisinde bankaların görevleri kredi kartlarında olduğu gibi aktif değildir. sE-Cüzdan'ın mimarisi dağınık yapıda olduğundan herhangi bir aktarım genel olarak iki cüzdan arasındadır; her e-etkileşimde bankaya başvurulmaz, işlemler cüzdanlararası kotarılır. Ancak, cüzdan sahibi, isterse, seçimlik olarak kendi cüzdanının e-etkileşimlerini gözetim altında tutmak için bankayı devreye sokabilmektedir. Bu durum özellikle kurumsal amaçlı kullanılan sE-Cüzdan'lar için istenecek bir özelliktir. [Çölkesen ve ark. - 2002]

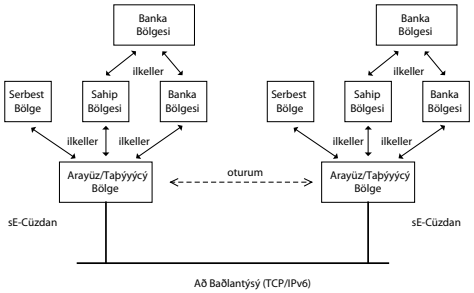


Şekil 3. Cüzdanlararası ve banka-cüzdan etkileşimi

Önerilen yapıda, Bankaların diğer görevleri ise sE-Cüzdan'ın oluşturulması, kaybolması veya çalınması durumunda cüzdanın yok edilmesi, sanal paranın nakit paraya çevrilmesi olarak belirlenmiştir.

Oturum Kurulması ve İletişim İlkelleri

Internet gibi dağınık özellikte bir ağ üzerinde hareket edebilen sE-Cüzdan ile iletişimde bulunabilinmesi için herşeyden önce ilgili cüzdanın arayüz bölgesiyle bağlantı oturumu kurulması gerekir. Bu oturum, iletişimde bulunacak iki uç düğüm arasında hatadan arınmış bir veri aktarım kanalı kurar. Şekil 4'te iki tane sE-Cüzdan arasında oturum kurulması ve oturum kurulduktan sonra yapılabilecek iletişim düzeyleri gösterilmiştir.



Şekil 4. Bağlantı oturumu kurulması ve iç-iletişim

Oturum kurulabilmesi için, oturumu başlatacak olan uç cüzdan karşı cüzdanın ağ üzerindeki kimlik numarasını bilmeli ve oturum başlatılması isteğinde bulunması gerekir. Oturum, iki farklı amaç için kurulmaktadır:

- Cüzdan sahibi ile arayüz bölge arasında
- İki farklı cüzdanın arayüz bölgeleri arasında.

İlki, cüzdan sahibinin cüzdan üzerinde işlem yapma komutlarını verebilmesi, ikincisi ise cüzdanlararası aktarım yapılması için kurulur. Oturum birkez kurulduktan sonra gerekli tüm işlemler bölgelerarası iletişim için tanımlanmış ilkeller aracılığıyla gerçekleştirilir.

Bölgelerarası ilkeller, bölgelerarasında yapılacak işlemleri belirleyen iletişim tanımlamalarıdır. sE-Cüzdan üzerinde yapılacak olan tüm işlemler parametreleri değiştirilerek bu ilkeller aracılığıyla yapılır. İletişimde bulunacak her bölge çifti arasında, benzer ilkeller olsa da, ilkeller farklıdır. Örneğin aşağıda sahip bölgesi ile askeri bölge arasına geçerli ilkellerden birkaç tanesi verilmiştir: (bölgeler askeri 0, banka 1, sahip 2, serbest 3 ve arayüz 4 olmak üzere numaralandırılmıştır)

- **b02.öde** *birim miktar*
- **b02.al** *birim miktar*
- **b02.göster** *birim*
- **b02.arşivle** *birim*

Burada, birim para vs. gibi mali değeri olan büyüklüğün türünü gösterirken, miktar ise belirtilen birimden ne kadar olacağını belirtir; birim yerine * koyulduğu tüm birimler anlamına gelmektedir.

Aşağıda ise, banka bölgesi ile askeri bölge arasındaki ilkellerden birkaç tanesi verilmiştir:

- **b01.yarat** *birim*
- **b01.ilk** *birim miktar*
- **b01.al** *birim miktar*
- **b01.arşivle** *birim*

Askeri bölge, iki düzeyli güvenlik altında tutulan bölgedir. Güvenlik kontrolü bu bölgeye erişim ilkelleri içerisine gömülmüştür. Dolayısıyla her erişim ilkeli kullanılmasında güvenlik denetimi yapılmaktadır. Şekil-1'de de görüleceği gibi askeri bölgeye erişmek için önce banka veya sahip bölgelerine erişilmesi gerekir. Bu bölgelerde erişmek için güvenlik kontrolu yapılmaktadır. Cüzdanlararası erişimde güvenlik gereksinimim sağlanması için açık anahtar (public key) yöntemi kullanılabilirken, bir cüzdan içerisinde bölgeler arası güvenlikte şifreleme yöntemi kullanılabilir.

5. Sonuç ve Öneriler

Günümüzde her ne kadar sanal para uygulamaları gittikçe yaygınlaşarak kullanılsa da, insanlar yanlarında "nakit para" taşıma ihtiyacı hissetmektedir. Bunun temel nedeni, sanal para teknolojisinin her durumda ve ortamda kullanılamamasıdır. Çünkü günümüzdeki uygulamalarda her türlü sanal para aktarımında aracı kurum olan bankayla bağlantı kurulması zorunludur. sE-Cüzdan teknolojisinde alıcı ve verici taraflar sanal cüzdan kullanır ve alışveriş doğrudan bu cüzdanlar arasında olur.

Tasarlanmaya çalışılan sE-Cüzdan, karşılıklı ödemelerde bankayı devre dışı bırakmaktadır.

Ancak bu yalnızca karşılıklı ödeme etkileşimleri içindir. Böylesi bir sistemde bankacılık yine de önemli bir yer tutmaktadır. Çünkü sE-Cüzdan'ı ilk oluşturan ve sE-Cüzdan içersindeki sanal paranın karşılığı olan fiziksel parayı tutan bankalar olacaktır. Böylesi bir sistem bankalarda bilişim sistemlerini de rahatlatacaktır. Ayrıca, bu yapı coğrafi koşulların elverişsiz olduğu yerlerde bile rahatlıkla kullanılabilecektir.

Gerekli durumlarda sE-Cüzdan başka cihazlara ve ortamlara taşınabilmeledir. Ayrıca kaybolan cüzdanın, banka tarafından kolaylıkla bulunabilmesi yada iptal edilebilmesi gerekmektedir.

Sanal Para ve sE-Cüzdan'nın günlük hayatta kullanılımasıyla birlikte, kapkaç gibi adi suç oranlarının önemli oranda düşeceği, ticaret hacminin genişleyeceği tahmin edilmektedir. Bununla birlikte Sanal Para ve sE-Cüzdan'nın günlük yaşama geçirebilmesi için, ilgili kurum ve kuruluşların, gerekli yasal düzenlemeleri yapması gerekmektedir.

Bu çalışmamızda sE-Cüzdan'a, işaret şiddetine duyarlı kablosuz arayüz erişim özelliği eklenmiştir.

KAYNAKÇA

[1] Frolund, S. and Guerraoui R., 2002. e-Transtions: End-to-End Reliability for Three-Tier Architecture, IEEE Transacions on Software Engineering, vol.28, no.4, 378-395.

[2] Sakamura, K. and Koshizuak, N., 2001. The ETORN Wide-Area Distrubuted - System Architecture for E-Commerce, IEEE Micro, vol.21, no.6, 7- 13.

[3] Trichina, E., Bucci, M. and Luzzi, R., 2001. Supplemental Cryptographic Hardware for Smart Cards, IEEE Micro, vol.21, no.6, 7-13,

[4] Pays, P. A. and de Comarmond, F., 1996. "An Intermediation and Payment System Technology", Fifth Int. World Wide Web Conference, May 6-10, Paris-France.

[5] Daswani, N., Boneh, D., Garcia-Molina, H., Ketchpel, S. and Paepcke, A., 1998. SWAPEROO: A Simple Wallet Architecture for Payments, Exchanges, Refunds, and Other Operations, Proceedings of the 3rd USENIX Workshop on Electronic Commerce, Boston, Massachusetts, USA, August 31-September 3.

[6] Çölkesen, R. ve Kipman, E., 2002. Bir Sanal Elektronik Cüzdün Mimarisi, Akademik Bilişim 2002, Konya, Türkiye, 6-8 Şubat 2002.

[7] Çölkesen, R., Örencik, B. ve Kipman, E., 2002. Taşınabilir Sanal Elektronik Cüzdan (sE-Cüzdan) Mimarisi, Bilişim Zirvesi, İstanbul, Türkiye, 28-30 Eylül 2002.

[8] Kipman, E., 2004. Sanal Cüzdan Mimarisi ve Gerçekleştirilmesi, Beykent Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği, Yüksek Lisans Tezi.

[9] Çölkesen, R. ve Örencik, B., 2008 (4. Basım). Bilgisayar Haberleşmesi ve Ağ Teknolojileri, Papatya Yayıncılık Eğitim, İstanbul..