ÖZET

AÇIK İLETİŞİM AĞLARI ÜZERİNDEN İLETİME YÖNELİK ÖDEME VERİLERİNİN GÜVENCE ALTINA ALINMASINA YÖNELİK YÖNTEM, CİHAZ VE SİSTEM

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.

İSTEMLER

1. Açık iletişim ağları üzerinden iletilen ödeme verilerini güvence altına almak üzere bir yöntem olup, özelliği yöntemin aşağıdakileri içermesidir:

bir birinci ödeme işlemine yönelik bir satıcı cihazı (10) olarak bir birinci alıcı-verici cihazının (10) seçime bağlı olarak konfigüre edilmesi;

birinci alıcı-verici cihaz ile bir müşteri cihazı (22) olarak konfigüre edilen ikinci bir alıcı-verici cihaz arasındaki bir veri bağlantısının kurulması (44), birinci ve ikinci alıcı-verici cihazlarının her biri, seçime bağlı olarak bir satıcı cihazı (10) veya bir müşteri cihazı (22) olarak konfigüre edilebilir;

veri bağlantısı üzerinden müşteri cihazına (22) bir birinci veri paketini ileten (48) satıcı cihazı (10), bir alıcı tarafından verilen benzersiz statik satıcı tanımlayıcı, işlem talebi verisi ve benzersiz bir dinamik değer içeren birinci veri paketi;

bir satıcı onayı talebini oluşturan ve satıcının kişisel anahtarını kullanarak benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan bir düzenleyen kurumun (30) imzalı bir sertifikasını satıcı cihazından (10) talep etmek üzere satıcı cihazına (10) satıcı onayı talebi ileten müşteri cihazı (22);

satıcı cihazından (10), satıcının kişisel anahtarı kullanılarak, düzenleyen kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketini alan müşteri cihazı (22);

onay kurumunun ortak anahtarı kullanılarak düzenleyen kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının (10) geçerliğini doğrulayan ve doğrulandığında, satıcı ortak anahtarı kullanılarak

birinci veri paketinde alınan benzersiz dinamik değere karşı imzalanan benzersiz dinamik değeri doğrulayan müşteri cihazı (22);

sadece imzalı benzersiz dinamik değerin, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı doğrulanması halinde, satıcı cihazına (22), alınan benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı ileten (48) müşteri cihazı (22), şifreli yazı, müşteri cihazı için bir gizli anahtar, bir hesaplama değeri, alınan benzersiz statik satıcı tanımlayıcı ve işlem talebi verisi kullanılarak oluşturulmuştur;

müşteri cihazından (22) alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğini kontrol eden ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturan ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum (30) ve bir alıcıdan (28) en az birine söz konusu onay talebini sunan (50) satıcı cihazı (10);

işlemin başarılı olup olmadığını gösteren düzenleyici kurumdan bir yanıt alan satıcı cihazı (10); ve

işlemin başarılı olup olmadığını müşteri cihazına (22) bildiren satıcı cihazı (10);

burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı (10) ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı (28) aracılığıyla güvenli bir şekilde tutulur.

2. İstem 1'e göre bir yöntem olup, özelliği birinci ve ikinci alıcı-verici cihazlar (10) arasında bir veri bağlantısı kurulmasının (44), bir temassız bağlantı veya bir temaslı bağlantı kurulmasını içermesidir.

3. İstem 2'ye göre bir yöntem olup, özelliği birinci ve ikinci alıcı-verici cihazlar (10) arasında bir veri bağlantısı kurulmasının (44), temassız bir bağlantı kurulmasını içermesidir ve söz konusu temassız bağlantı, NFC, Bluetooth ve WiFi teknolojilerinden en az birini kullanır.

4. Önceki istemlerden herhangi birine göre bir yöntem olup, özelliği ayrıca müşteri cihazında (22) bulunan bir sayacın kullanılmasını içermesidir.

5. Önceki istemlerden herhangi birine göre bir yöntem olup, özelliği ayrıca müşteri cihazının (22) kullanıcısından bir hesap seçme talebinin alınmasını içermesidir.

6. İstem 5'e göre bir yöntem olup, özelliği hesap seçme talebinin, müşteri cihazının (22) bir kullanıcı arayüzü ile alınmasıdır, yöntem tercihen ayrıca veri bağlantısı üzerinden, kullanıcı tarafından seçilen hesap seçiminin, satıcı cihazına (10) iletilmesini ve satıcı cihazının (10) belleğindeki kullanıcı tarafından seçilen hesabın veri temsilcisinin saklanmasını içerir.

7. İstemler 1 ila 4'ten herhangi birine göre bir yöntem olup, özelliği bir hesap seçme talebinin, satıcı cihazının (10) bir kullanıcı arayüzü ile alınmasıdır, yöntem tercihen ayrıca müşteri cihazının (22) bir belleğinden (16) önceden belirlenen bir varsayılan hesabın alınmasını içerir.

8. İstem 6'ya göre bir yöntem olup, özelliği ayrıca veri bağlantısı üzerinden müşteri cihazına (22) kullanıcı tarafından seçilen hesabın veri temsilcisinin iletilmesini içermesidir.

9. Önceki istemlerden herhangi birine göre bir yöntem olup, özelliği ayrıca işlem talebi verilerinin alınmasını içermesidir, söz konusu işlem talebi verileri, işleme yönelik bir tutar ve döviz kodu, kullanıcı tarafından seçilen hesabın veri temsilcisi ve bir PIN veya biyometrik gibi bir müşteri tanımlayıcı ve bir statik satıcı tanımlayıcı değerden en az birini içerir.

10. Bir açık iletişim ağı üzerinden iletilen bir birinci ödeme işlemine yönelik ödeme verilerini güvence altına almak üzere bir satıcı cihazı (10) olarak seçime bağlı konfigüre edilen bir birinci alıcı-verici cihazının (10) çalıştırılmasına yönelik bir yöntem olup, özelliği yöntemin, aşağıdakileri içermesidir:

bir müşteri cihazı (22) olarak konfigüre edilen ikinci bir alıcı-verici cihaz (10) ile bir veri bağlantısının kurulması (44), birinci ve ikinci alıcı-verici cihazlarının her biri, seçime bağlı olarak bir satıcı cihazı (10) veya bir müşteri cihazı (22) olarak konfigüre edilebilir;

veri bağlantısı üzerinden müşteri cihazına (22) bir birinci veri paketinin iletilmesi (48), bir alıcı tarafından verilen benzersiz statik satıcı tanımlayıcı, işlem talebi verisi ve benzersiz bir dinamik değer içeren birinci veri paketi;

benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve satıcının kişisel anahtarı kullanılarak benzersiz bir dinamik değerin bir imzasını tutan bir düzenleyici kurumun (30) imzalı bir sertifikasını talep eden bir satıcı onay talebinin, müşteri cihazından (22) alınması; ve

müşteri cihazına (22), satıcının kişisel anahtarı kullanılarak, düzenleyen kurumun imzalı sertifikası ve

benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketinin iletilmesi;

burada müşteri cihazının (22), onay kurumunun ortak anahtarı kullanılarak düzenleyen kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının (10) geçerliğini doğrulaması halinde ve doğrulandığında, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı imzalanan benzersiz dinamik değeri doğrular, yöntem ayrıca aşağıdakileri içerir:

müşteri cihazından (22), benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı alınması, şifreli yazı, müşteri cihazı için alınan bir gizli anahtar, bir hesaplama değeri, benzersiz statik satıcı tanımlayıcı ve işlem talebi verisi kullanılarak oluşturulmuştur;

müşteri cihazından (22) alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğini kontrol eden ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturan ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum (30) ve bir alıcıdan (28) en az birine söz konusu onay talebini sunulması (50);

işlemin başarılı olup olmadığını gösteren düzenleyici kurumdan bir yanıt alınması; ve

işlemin başarılı olup olmadığının müşteri cihazına (22) bildirilmesi;

burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı (10) ile bağlı bir satıcının, geçerli bir

satıcı olduğunu doğrulamak üzere alıcı (28) aracılığıyla güvenli bir şekilde tutulur.

11. Bir açık iletişim ağı üzerinden iletilen bir birinci ödeme işlemine yönelik ödeme verilerini güvence altına almak üzere bir müşteri cihazı (22) olarak seçime bağlı konfigüre edilen ikinci bir alıcı-verici cihazının (10) çalıştırılmasına yönelik bir yöntem olup, özelliği yöntemin, aşağıdakileri içermesidir:

bir satıcı cihazı (10) olarak konfigüre edilen bir birinci alıcı-verici cihaz ile bir veri bağlantısının kurulması (44), birinci ve ikinci alıcı-verici cihazlarının her biri, seçime bağlı olarak bir satıcı cihazı (10) veya bir müşteri cihazı (22) olarak konfigüre edilebilir;

veri bağlantısı üzerinden bir birinci veri paketinin, satıcı cihazından (10) alınması (48), birinci veri paketi, bir alıcı tarafından verilen bir benzersiz statik satıcı tanımlayıcı, işlem talebi verileri ve benzersiz bir dinamik değer içerir;

bir satıcı onay talebini oluşturan ve satıcının kişisel anahtarını kullanarak benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan bir düzenleyen kurumun (30) imzalı bir sertifikasını satıcı cihazından (10) talep etmek üzere satıcı cihazına (10) satıcı onay talebi iletilmesi;

satıcı cihazından (10), satıcının kişisel anahtarı kullanılarak, düzenleyen kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketini alınması;

onay kurumunun ortak anahtarı kullanılarak düzenleyen kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının (10) geçerliğini doğrulayan ve doğrulandığında, satıcı ortak anahtarı kullanılarak

birinci veri paketinde alınan benzersiz dinamik değere karşı imzalanan benzersiz dinamik değerin doğrulanması;

sadece imzalı benzersiz dinamik değerin, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı doğrulanması halinde, satıcı cihazına (22), alınan benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı iletilmesi (48), şifreli yazı, müşteri cihazı için bir gizli anahtar, bir hesaplama değeri, alınan benzersiz statik satıcı tanımlayıcı ve işlem talebi verisi kullanılarak oluşturulmuştur; ve

işlemin başarılı olup olmadığını gösteren bir bildirimin satıcı cihazından (10) alınması;

burada şifreli yazı, satıcı cihazının (10), müşteri cihazından (22) alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğini kontrol etmesini sağlar ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturur ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum (30) ve bir alıcıdan (28) en az birine söz konusu onay talebini sunar (50); ve

burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı (10) ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı (28) aracılığıyla güvenli bir şekilde tutulur.

12. Açık iletişim ağları üzerinden iletilen ödeme verilerini güvence altına almak üzere çalıştırılabilen bir birinci alıcı-verici cihaz olup, özelliği birinci alıcı-verici cihazın, bir satıcı cihazı (10) veya bir müşteri alıcı-verici cihazı (22) olarak seçime bağlı

konfigüre edilebilmesidir, birinci alıcı-verici cihaz (10), aşağıdakileri içerir:

diğer alıcı-verici cihazlar (10) ile veri iletişimini sağlamak üzere çalıştırılabilen bir arayüz modülü (12); ve

bir belleğe (16) bağlı bir işlemci (14), bellek (16), işlemci kontrol kodunu saklamak üzere çalıştırılabilir;

burada aşağıdakileri gerçekleştirmeye çalışırken, birinci alıcı-vericinin, bir satıcı cihazı (10) olarak seçime bağlı konfigüre edilmesi durumunda, işlemci kontrol kodu, işlemciyi (14) ve arayüz modülünü (12) seçime bağlı olarak kontrol etmek üzere çalıştırılabilir:

bir müşteri cihazı (22) olarak konfigüre edilen ikinci bir alıcı-verici cihaz ile bir veri bağlantısı kurulması (44);

bellekten (16), benzersiz bir statik satıcı tanımlayıcı alınması, benzersiz statik satıcı tanımlayıcı, bir alıcı (28) tarafından verilmiştir;

veri bağlantısı üzerinden müşteri cihazına (22) bir birinci veri paketinin iletilmesi (48), benzersiz statik satıcı tanımlayıcı, işlem talebi verisi ve benzersiz bir dinamik değer içeren birinci veri paketi;

müşteri cihazından (22), satıcının kişisel anahtarı kullanılarak, benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan bir düzenleyici kurumun (30) imzalı bir sertifikasını talep eden bir satıcı onay talebinin alınması; ve

müşteri cihazına (22), satıcının kişisel anahtarı kullanılarak, düzenleyen kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketinin iletilmesi;

burada müşteri cihazının (22), onay kurumunun ortak anahtarı kullanılarak düzenleyen kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının (10) geçerliğini doğrulaması halinde ve doğrulandığında, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı imzalanan benzersiz dinamik değeri doğrular, işlemci kontrol kodu, aşağıdakileri gerçekleştirmeye çalışırken, işlemci (14) ve arayüz modülünü (12) seçime bağlı olarak kontrol etmek üzere çalıştırılabilir:

müşteri cihazından (22), benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı alınması (48), şifreli yazı, müşteri cihazı için alınan bir gizli anahtar, bir hesaplama değeri, benzersiz statik satıcı tanımlayıcı ve işlem talebi verisi kullanılarak oluşturulmuştur;

müşteri cihazından (22) alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğini kontrol eden ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturan ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum (30) ve bir alıcıdan (28) en az birine söz konusu onay talebini sunulması (50);

işlemin başarılı olup olmadığını gösteren düzenleyen kurumdan bir yanıt alınması ve müşteri cihazının (22) bir kullanıcısının bilgilendirilmesi; ve

işlemin başarılı olup olmadığının müşteri cihazına (22) bildirilmesi;

burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı (10) ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı (28) aracılığıyla güvenli bir şekilde tutulur; veya

burada aşağıdakileri gerçekleştirmeye çalışırken, birinci alıcı-verici cihazının, bir müşteri cihazı (22) olarak seçime bağlı konfigüre edilmesi durumunda, işlemci kontrol kodu, işlemciyi (14) ve arayüz modülünü (12) seçime bağlı olarak kontrol etmek üzere çalıştırılabilir:

bir satıcı cihazı (10) olarak konfigüre edilen ikinci bir alıcı-verici cihaz ile bir veri bağlantısı kurulması (44);

veri bağlantısı üzerinden bir birinci veri paketinin, satıcı cihazından (10) alınması (48), birinci veri paketi, bir alıcı tarafından verilen bir benzersiz statik satıcı tanımlayıcı, işlem talebi verileri ve benzersiz bir dinamik değer içerir;

bir satıcı onay talebini oluşturan ve satıcının kişisel anahtarını kullanarak benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan bir düzenleyen kurumun (30) imzalı bir sertifikasını satıcı cihazından (10) talep etmek üzere satıcı cihazına (10) satıcı onay talebi iletilmesi;

satıcı cihazından (10), satıcının kişisel anahtarı kullanılarak, düzenleyen kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketini alınması;

onay kurumunun ortak anahtarı kullanılarak düzenleyen kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının (10) geçerliğini doğrulayan ve doğrulandığında, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı imzalanan benzersiz dinamik değerin doğrulanması;

bellekten (16) bir hesaplama değeri ve saklanan bir müşteri cihazı kişisel anahtarı alınır;

sadece imzalı benzersiz dinamik değerin, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı doğrulanması halinde, satıcı cihazına (22), alınan benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı iletilmesi (48), şifreli yazı, müşteri cihazı için alınan bir gizli anahtar, alınan bir hesaplama değeri, alınan benzersiz statik satıcı tanımlayıcı ve işlem talebi verisi kullanılarak oluşturulmuştur; ve

işlemin başarılı olup olmadığını gösteren bir bildirimin satıcı cihazından (10) alınması;

burada şifreli yazı, satıcı cihazının (10), müşteri cihazından (22) alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğini kontrol etmesini sağlar ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturur ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum (30) ve bir alıcıdan (28) en az birine söz konusu onay talebini sunar (50); ve

burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı (10) ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı (28) aracılığıyla güvenli bir şekilde tutulur.

13. İstem 12'ye göre bir birinci alıcı-verici cihazı (10) olup, özelliği arayüz modülünün (12), bir temaslı arayüz modülü, bir temassız arayüz modülü veya bir ikili temas ve temassız arayüz modülü şeklinde olmasıdır.

14. İstem 13'e göre bir birinci alıcı-verici cihazı (10) olup, özelliği arayüz modülünün (12), yakın saha iletişimi teknolojisini içeren bir temassız arayüz modülü şeklinde olmasıdır.

15. İstemler 12 ila 14'ten herhangi birine göre bir birinci alıcı-verici cihazı (10) olup, özelliği işlem talebi verilerinin, işlemin bir tutarını ve döviz kodu, zaman damgası ve bir PIN veya biyometrik gibi bir müşteri tanımlayıcıdan en az birini içermesidir.

16. İstemler 12 ila 15'ten herhangi birinde tanımlanan, burada bulunan, bir birinci alıcı-verici cihazını (10) içeren, bir mobil iletişim cihazı, kişisel hesaplama cihazı veya satış noktası cihazıdır.

TARİFNAME

AÇIK İLETİŞİM AĞLARI ÜZERİNDEN İLETİME YÖNELİK ÖDEME VERİLERİNİN GÜVENCE ALTINA ALINMASINA YÖNELİK YÖNTEM, CİHAZ VE SİSTEM

İlgili Başvurulara Çapraz Referans

Mevcut başvuru, AU2010900195'ten rüçhan talep eder.

Teknik Saha

Bu buluş, açık iletişim ağları üzerinden iletime yönelik ödeme verilerinin güvence altına alınmasına yönelik bir yöntem, cihaz ve sistem ile ilgilidir.

Altyapı Tekniği

Şekil 1, bir açık ağ üzerinden alışverişe katılan kuruluşları gösteren tipik bir dördüncü parti ağı şematik olarak gösterir. Ağ, kart düzenleyen kurumlar ve ticari alıcılar, artı kart sahipleri (müşteriler) ve satıcıları içerir. Kart düzenleyen kurum, kartları müşterilere dağıtır, fatura keser ve onlardan ödeme toplar. Ticari alıcılar, satıcıların, kartları kabul etmesine yardım eder ve alışverişin, ağın işleme tesislerine yönlendirilmesinin ön uç servisini sağlar. Alıcı, işlemin, uygun kart düzenleyen kuruma iletilmesinden sorumludur, böylece müşteriye fatura kesilir ve satıcı, satın almaya yönelik fon alır.

Alışveriş prosesi, tipik olarak iki temel parçaya sahiptir. Birincisi, onay verme ve ikincisi tahsil etme ve mahsuplaşmadır. Onay, ödeme için işlem ve kart detayını kabul etmek üzere kartı veren bankadan iznin alınması prosesidir. Onay, bir tüketici, kartını satın almak için satıcıya

gönderdiğinde başlar (1). Geleneksel olarak, işlemin güvence altına alınması, daha yakın zamanda "kart mevcut değil" durumlarında (örneğin, çevrimiçi) tamamlanmasına rağmen, satış noktasında gerçekleşen yetki vermeye yönelik olarak ortaya çıkar. Yakın zamanlarda, çip ve temassız teknolojiler, artan bir şekilde yaygın hale gelmiştir. Ödeme sektörüne özellikle referans olarak, çip tabanlı teknolojiler, verileri daha güvenli bir şekilde saklayabilmeleri ve işleyebilmelerinden dolayı temaslı veya temassız işlemler, geleneksel manyetik şerit teknolojileri üzerinde avantajlara sahiptir.

Temaslı ve temassız durumlarda, satıcılar genel olarak işlem bilgisini elektronik olarak veya alıcının kartı kaydırması veya satış noktasında bir terminalden geçirmesi aracılığıyla veya kartı bir terminal veya okuyucunun çevresine getirerek elektronik olarak elde eder. Kart bilgileri alındıktan sonra, satıcının terminali, kart bilgisini, işlem tutarını ve satıcının kimlik numarasını içeren bir yetki verme talebini toplar ve yetki verme talebini alıcıya gönderir (2). Alıcı, bilgiyi okur ve bir tahsil kartı ağı (3) ile spesifik ilgili bankaya onay talebini gönderir. İlgili banka, dolandırıcılıktan dolayı bir dizi kontrol yürütür ve kart sahibinin hazır fonları veya kredi limitinin, bir yanıt (4) geri göndermeden, onay vermeden veya reddetmeden önce harcamayı karşılamak için yeterli olduğunu doğrular. Ticari alıcı, yanıtı alır ve bunu satıcıya bildirir (5).

Alıcı bankalar, satıcılar ve tüketiciler, internet ve diğer açık ağlar üzerindeki işlemlerin daha güvenli olmasını talep eder. Mevcut temaslı ve temassız işlemler, geleneksel manyetik şerit teknolojisi üzerinden artan güvenlik önerirken, internet veya diğer açık ağlar üzerinden bir işlemin güvenliğini sağlamak üzere gereken güvenlik seviyesini yeterli şekilde adreslemez.

Mevcut sistemler, işlemin güvenilirliğini tehlikeye atan "ortadaki adam saldırılarına" eğilimlidir. Ortadaki adam saldırıları, bir işlemin güvenilirliğinin yanı sıra bunu başlatan satıcının güvenilirliğinin doğrulanmasının zorluğundan faydalanır. Bu tür saldırılar, iki cihaz arasındaki iletişimi engellemek üzere görev yapar. Bu saldırı türünde bir bilgisayarda yerleşik olan kötü amaçlı yazılım, müşteri cihazına satıcı gibi görünmekle birlikte, satıcıya müşteri cihazı gibi görünecek şekilde çalışır. Bu tür yazılım, alıcı tarafın ayrıntılarını veya işlemin değerini değiştirmek üzere kullanılabilir.

US-7024395-B1, bir kredi kartı işlemi yapan bir müşterinin akıllı kartını satıcının sistemine bağlı bir kart okuyucusuna yerleştirdiği bir yöntemi açıklar. Kart okuyucu, müşterinin kartını aktifleştirir ve belirli satıcı bilgilerini iletir. Satıcının sistemi akabinde, müşterinin kartından bir "fatura özeti" talep eder. Fatura özeti, müşterinin kredi kartı hesabına bakan, bağlantılı kredi kartı düzenleyen kuruma bunu (ve müşteri bilgisi ve satıcı bilgisini içeren işlem bilgisini) ileten, satıcının kart okuyucusuna geri gönderilir. Bir düzenlemede, müşteri bilgisi ve satıcı bilgisi şifrelenir. Fatura özetinin alınması üzerine, gerekli olması halinde işlem bilgisinin şifresi çözülür ve kredi kartı düzenleyen kurum, müşterinin hesap numarasını kullanarak müşterinin ana anahtarını arar. Kredi kartı düzenleyen kurum akabinde fatura özetini tekrar hesaplamak (fatura özetinin doğrulanması) üzere işlem bilgisini kullanır ve bu yeni değeri, satıcı tarafından öne sürülen fatura özeti ile karşılaştırır. Doğrulanması durumunda, fatura özeti ve doğrulanan fatura özeti değerleri eşittir, akabinde fonlar aktarılır ve satıcıya bir kabul bildirimi gönderilir. Doğrulanmaması durumunda, satıcıya bir ret bildirimi gönderilir. Güvenlik, fatura özeti oluşturulmasına yönelik olarak kullanılan tekil müşteri

bilgisindeki her işlem için tek bir referans kullanılarak daha da geliştirilir.

US-2008/208759-A1, müşteriler ve satıcılar arasındaki finansal işlemlerin yerine getirilmesine yönelik yöntemler ve sistemleri açıklar. Bir finansal hesap tanımlayıcı, satıcı sisteminde müşteriden alınır. Bir mobil elektronik cihaz veya temassız bir gösterme aracı ile tek kullanımlık bir parola ile sağlanan tek kullanımlık bir parola da satıcı sisteminde müşteriden alınır. Tek kullanımlık parola kullanılarak şifrelenen finansal hesap tanımlayıcıyı içeren bir şifreli yazı oluşturulur. Onay talebi, satıcı sisteminde formüle edilir. Onay talebi, finansal işlemin en az bir kısmını tanımlayan şifreli yazı ve işlem bilgisisini içerir. Onay talebi, finansal işlemin onaylanması için satıcı sisteminden, bir onay işlemcisine iletilir.

US-2009/216680-A1, bir sunucu cihaz ile bağlantıya yönelik olarak konfigüre edilen bir güvenli hesaplama modülünü (SCM) açıklar. SCM, güvenli işlem faaliyetlerinin gerçekleştirilmesine yönelik bir işlemci, sunucu cihaza işlemcinin bağlanmasına yönelik bir sunucu arayüzü ve işlemciye bağlı bir bellek içerir, burada işlemci, mantıklı bir şekilde sunucu cihaz aracılığıyla erişimden belleğin en azından bir kısmını izole eder. SCM, finansal bir işleme yönelik güvenli bir dijital imza oluşturur ve sunucu cihazdan alınan kontrollü içeriği sağlar. Dosya dağıtımı, bir içerik sağlayıcıdan bir alıcıya veya bir yeniden satıcıdan bir alıcıya gerçekleştirilir. Dosya dağıtımı, güvenli dijital imzalar ve imkan dahilinde ileti şifreleme kullanan bir finansal işlemi içerir. Dijital imzalar ve işlem detayları, işlem yapan tarafları onaylamak ve işlemi tamamlamak üzere uygun finansal kuruluşlara iletilir. Kontrollü içerik, içerik sağlayıcı veya yeniden satıcıdan alıcıya aktarılır.

Buluşun Kısa Açıklaması

Mevcut buluşun bir birinci açısına göre, açık iletişim ağları üzerinden iletilen ödeme verilerini güvence altına almak üzere bir yöntem sağlanır, yöntem, aşağıdakileri içerir: bir birinci ödeme işlemine yönelik bir satıcı cihazı olarak bir birinci alıcı-verici cihazının seçime bağlı olarak konfigüre edilmesi; birinci alıcı-verici cihaz ile bir müşteri cihazı olarak konfigüre edilen ikinci bir alıcı-verici cihaz arasındaki bir veri bağlantısının kurulması, birinci ve ikinci alıcı-verici cihazlarının her biri, seçime bağlı olarak bir satıcı cihazı veya bir müşteri cihazı olarak konfigüre edilebilir; veri bağlantısı üzerinden müşteri cihazına bir birinci veri paketini ileten satıcı cihazı, bir alıcı tarafından verilen benzersiz statik satıcı tanımlayıcı, işlem talebi verisi ve benzersiz bir dinamik değer içeren birinci veri paketi; bir satıcı onay talebini oluşturan ve satıcının kişisel anahtarını kullanarak benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan bir düzenleyen kurumun imzalı bir sertifikasını satıcı cihazından talep etmek üzere satıcı cihazına satıcı onay talebi ileten müşteri cihazı; satıcı cihazından, satıcının kişisel anahtarı kullanılarak, düzenleyen kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketini alan müşteri cihazı; onay kurumunun ortak anahtarı kullanılarak düzenleyen kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının geçerliğini doğrulayan ve doğrulandığında, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı imzalanan benzersiz dinamik değeri doğrulayan müşteri cihazı; sadece imzalı benzersiz dinamik değerin, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı doğrulanması halinde, satıcı cihazına, alınan benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı ileten müşteri cihazı, şifreli yazı, müşteri

cihazı için bir gizli anahtar, bir hesaplama değeri, alınan benzersiz statik satıcı tanımlayıcı ve işlem talebi verisi kullanılarak oluşturulmuştur; müşteri cihazından alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğini kontrol eden ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturan ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum ve bir alıcıdan en az birine söz konusu onay talebini sunan satıcı cihazı; işlemin başarılı olup olmadığını gösteren düzenleyici kurumdan bir yanıt alan satıcı cihazı; ve işlemin başarılı olup olmadığını müşteri cihazına bildiren satıcı cihazı; burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı aracılığıyla güvenli bir şekilde tutulur.

Açık ağ, bir mobil veya bir İnternet Protokolü (IP) ağı olabilir.

Şifreli yazıya dahil etmeye yönelik olarak müşteri alıcı-verici cihazına benzersiz satıcı tanımlayıcı ileten satıcı cihazının sağlanması, satıcı ve tüketiciyi işlem için birleştirir ve bir işlemin doğrulanmasında bulunan değişikliklerin sayısını azaltır. Bu, prensip olarak alıcının, satıcının onayını doğrulamak üzere gerekli olmadığından, sadece geçerli bir satıcı olduğundan kaynaklanır. Avantajlı olarak üçüncü taraf dolandırıcılığa yönelik olanak büyük ölçüde azaltılır.

Birinci ve ikinci alıcı-verici cihazlar arasındaki veri bağlantısının kurulması adımı, temassız bir bağlantı veya temaslı bir bağlantı kurulmasını içerebilir. Temassız

bağlantı, NFC, Bluetooth, WiFi, SMS, diğer benzer bir teknoloji veya bunların bir kombinasyonunu kullanabilir. Temaslı bağlantı, teknikte uzman kişilerce iyi bilindiği gibi elektriksel bağlantı kullanabilir.

Yöntem, ayrıca müşteri alıcı-verici cihazında bulunan bir sayacın kullanılmasını içerebilir.

Diğer ilgili veriler, bunlarla sınırlı olmamak üzere, alıcı-verici cihazın teknik kapasitesi ile bağlantılı verileri içeren şifreli yazıda bulunabilir.

Yöntem, ayrıca müşteri alıcı-verici cihazının kullanıcısından bir hesap seçme talebinin alınmasını içerir. Hesap seçme talebi, diğer cihazın bir kullanıcı arayüzü ile alınabilir. Hesap seçme talebinin, müşteri alıcı-verici cihazının bir kullanıcı arayüzü ile alındığı bir düzenlemede, yöntem, ayrıca veri bağlantısı üzerinden satıcı cihazına, kullanıcının seçtiği hesap seçiminin iletilmesini içerebilir. Hesap seçme talebinin,satıcı cihazının bir kullanıcı arayüzü ile alındığı bir düzenlemede, yöntem, ayrıca satıcı cihazının belleğindeki kullanıcı tarafından seçilen hesabın veri temsilcisinin saklanmasını içerebilir. Yöntem, ayrıca veri bağlantısı üzerinden müşteri alıcı-verici cihazına kullanıcı tarafından seçilen hesabın veri temsilcisinin iletilmesini içerebilir.

İsteğe bağlı olarak, yöntem ayrıca önceden belirlenen varsayılan hesabın alınmasını içerebilir. Önceden belirlenen varsayılan hesap, müşteri alıcı-verici cihazındaki bellekte saklanabilir.

Yöntem ayrıca, işlem talebi verilerinin alınmasını içerebilir, söz konusu işlem talebi verileri, işleme yönelik bir tutar ve döviz kodu, kullanıcı tarafından seçilen hesabın veri temsilcisi ve bir PIN veya biyometrik gibi bir müşteri

tanımlayıcı ve bir satıcı tanımlayıcı değerden en az birini içerir.

Satıcı cihazının, veri bağlantısı üzerinden müşteri alıcı-verici cihazına bir birinci veri paketini iletmesi adımı, benzersiz satıcı tanımlayıcı ve işlem talebi verilerini talep eden müşteri alıcı-verici cihazından önce olabilir.

Satıcı cihazının geçerliğinin doğrulanması adımı, tüketici alıcı-verici cihazının, (tanımlanan bir şema içindeki onaylı düzenleyici kurum tarafından verilen) güvenilir bir satıcı cihazı ile iletişim kurmasını sağlar. Bu ayrıca, işlem talebinin bir parçası olarak sağlanan benzersiz kimlik numarasının, imzalı güvenlik modülü sertifikasındaki düzenleyen kurum tarafından imzalanan ile aynı olmasını sağlar.

Mevcut buluşun ikinci bir açısına göre, açık bir iletişim ağı üzerinden iletilen bir birinci ödeme işlemine yönelik ödeme verilerini güvence altına almak üzere bir satıcı cihazı olarak seçime bağlı olarak konfigüre edilen bir birinci alıcı-verici cihazın çalıştırılmasının bir yöntemi sağlanır, yöntem, aşağıdakileri içerir: bir müşteri cihazı olarak konfigüre edilen ikinci bir alıcı-verici cihaz ile bir veri bağlantısı kurulması, birinci ve ikinci alıcı-verici cihazlarının her biri, seçime bağlı olarak bir satıcı cihazı veya bir müşteri cihazı olarak konfigüre edilebilir; veri bağlantısı üzerinden müşteri cihazına bir birinci veri paketinin iletilmesi, bir alıcı tarafından verilen benzersiz statik satıcı tanımlayıcı, işlem talebi verisi ve benzersiz bir dinamik değer içeren birinci veri paketi; müşteri cihazından, satıcının kişisel anahtarı kullanılarak, benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan düzenleyen kurumun imzalı sertifikasını talep eden bir satıcı onay talebinin alınması; ve satıcının kişisel

anahtarı kullanılarak düzenleyici kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketinin, müşteri cihazına iletilmesi; burada müşteri cihazının, onay kurumunun ortak anahtarı kullanılarak düzenleyici kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının geçerliğini doğrulaması halinde ve doğrulandığında satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı imzalanan benzersiz dinamik değeri, doğrular, yöntem ayrıca aşağıdaki adımları içerir: müşteri cihazından, benzersiz statik satıcı tanımlayıcı ve bir şifreli yazının alınması, şifreli yazı, müşteri cihazı için benzersiz bir gizli anahtar, bir sayaç değeri, benzersiz statik satıcı tanımlayıcı ve işlem talebi verileri kullanılarak oluşturulmuştur; müşteri cihazından alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğinin kontrol edilmesi ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturulması ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum ve bir alıcıdan en az birine söz konusu onay talebi sunulması; işlemin başarılı olup olmadığını gösteren düzenleyici kurumdan bir yanıt alınması; ve işlemin başarılı olup olmadığını müşteri cihazına bildirilmesi; burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı aracılığıyla güvenli bir şekilde tutulur.

Mevcut buluşun üçüncü bir açısına göre, açık bir iletişim ağı üzerinden iletilen bir birinci ödeme işlemine yönelik ödeme verilerini güvence altına almak üzere bir satıcı cihazı olarak seçime bağlı olarak konfigüre edilen bir birinci alıcı-verici cihazın çalıştırılmasının bir yöntemi sağlanır, yöntem,

aşağıdakileri içerir: bir satıcı cihazı olarak konfigüre edilen bir birinci alıcı-verici cihaz ile bir veri bağlantısı kurulması, birinci ve ikinci alıcı-verici cihazlarının her biri, seçime bağlı olarak bir satıcı cihazı veya bir müşteri cihazı olarak konfigüre edilebilir; veri bağlantısı üzerinden satıcı cihazından bir birinci veri paketinin, bir alıcı tarafından verilen benzersiz statik satıcı tanımlayıcı, işlem talebi verisi ve benzersiz bir dinamik değer içeren birinci veri paketinin alınması; bir satıcı onay talebinin oluşturulması ve satıcı cihazından, satıcının kişisel anahtarı kullanılarak, benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan düzenleyen kurumun imzalı sertifikası talep etmek üzere satıcı onay talebinin, satıcı cihazına iletilmesi; satıcının kişisel anahtarı kullanılarak düzenleyici kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketinin, satıcı cihazından alınması; onay kurumunun ortak anahtarı kullanılarak düzenleyici kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının geçerliğinin doğrulanması, doğrulandığında, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı imzalı benzersiz dinamik değerin doğrulanması; sadece imzalı benzersiz dinamik değerin, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı doğrulanması halinde satıcı cihazına, alınan benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı iletilmesi, şifreli yazı, müşteri cihazı için benzersiz bir gizli anahtar, bir sayaç değeri, alınan benzersiz statik satıcı tanımlayıcı ve işlem talebi verileri kullanılarak oluşturulmuştur; ve satıcı cihazından, işlemin başarılı olup olmadığını gösteren bir bildirim alınması; burada şifreli yazı, satıcı cihazının, alındığında, müşteri cihazından alınan benzersiz statik satıcı tanımlayıcının, alıcı tarafından verilen benzersiz statik satıcı tanımlayıcı ile eşleşip eşleşmediğini kontrol etmesini sağlar ve böyle

olması durumunda alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verisini içeren bir onay talebi oluşturulması ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyen kurum ve bir alıcıdan en az birine söz konusu onay talebinin sunulması; ve burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı aracılığıyla güvenli bir şekilde tutulur.

Mevcut buluşun dördüncü bir açısına göre, açık iletişim ağları üzerinden iletilen ödeme verilerini güvence altına almak üzere çalıştırılabilen bir birinci alıcı-verici cihaz sağlanır, birinci alıcı-verici cihaz, bir satıcı cihazı veya bir müşteri alıcı-verici cihazı olarak seçime bağlı konfigüre edilebilir, birinci alıcı-verici cihaz, aşağıdakileri içerir: diğer alıcı-verici cihazlar ile veri iletişimini sağlamak üzere çalıştırılabilen bir arayüz modülü; ve bir belleğe bağlı bir işlemci, bellek, işlemci kontrol kodunu saklamak üzere çalıştırılabilir; burada aşağıdakileri gerçekleştirmeye çalışırken, birinci alıcı-vericinin, bir satıcı cihazı olarak seçime bağlı konfigüre edilmesi durumunda, işlemci kontrol kodu, işlemciyi ve arayüz modülünü seçime bağlı olarak kontrol etmek üzere çalıştırılabilir: bir müşteri cihazı olarak konfigüre edilen ikinci bir alıcı-verici cihaz ile bir veri bağlantısı kurulması; bellekten, benzersiz bir statik satıcı tanımlayıcı alınması, benzersiz statik satıcı tanımlayıcı, bir alıcı tarafından verilmiştir; veri bağlantısı üzerinden müşteri cihazına bir birinci veri paketinin iletilmesi, birinci veri paketi, benzersiz statik satıcı tanımlayıcı, işlem talebi verisi ve benzersiz bir dinamik değer içerir; müşteri cihazından, satıcının kişisel anahtarı kullanılarak, benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan bir düzenleyici kurumun imzalı bir sertifikasını talep eden bir

satıcı onay talebinin alınması; müşteri cihazına, satıcının kişisel anahtarı kullanılarak, düzenleyen kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketinin iletilmesi; burada müşteri cihazının, onay kurumunun ortak anahtarı kullanılarak düzenleyen kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının geçerliğini doğrulaması halinde ve doğrulandığında, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı imzalanan benzersiz dinamik değeri doğrular, işlemci kontrol kodu, aşağıdakileri gerçekleştirmeye çalışırken, işlemci ve arayüz modülünü seçime bağlı olarak kontrol etmek üzere çalıştırılabilir: müşteri cihazından, benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı alınması, şifreli yazı, müşteri cihazı için alınan bir gizli anahtar, bir hesaplama değeri, benzersiz statik satıcı tanımlayıcı ve işlem talebi verisi kullanılarak oluşturulmuştur; müşteri cihazından alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğini kontrol eden ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturan ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum ve bir alıcıdan en az birine söz konusu onay talebini sunulması; ve işlemin başarılı olup olmadığını gösteren düzenleyen kurumdan bir yanıt alınması ve müşteri cihazının bir kullanıcısının bilgilendirilmesi ve işlemin başarılı olup olmadığının müşteri cihazına bildirilmesi; burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı aracılığıyla güvenli bir şekilde tutulur; veya burada aşağıdakileri gerçekleştirmeye çalışırken, birinci alıcı-verici cihazının, bir müşteri cihazı olarak seçime bağlı konfigüre edilmesi durumunda, işlemci kontrol kodu, işlemciyi

ve arayüz modülünü seçime bağlı olarak kontrol etmek üzere çalıştırılabilir: bir satıcı cihazı olarak konfigüre edilen ikinci bir alıcı-verici cihaz ile bir veri bağlantısı kurulması; veri bağlantısı üzerinden bir birinci veri paketinin, satıcı cihazından alınması, birinci veri paketi, bir alıcı tarafından verilen bir benzersiz statik satıcı tanımlayıcı, işlem talebi verileri ve benzersiz bir dinamik değer içerir; bir satıcı onay talebini oluşturan ve satıcının kişisel anahtarını kullanarak benzersiz statik satıcı tanımlayıcı ve satıcı ortak anahtarı ve benzersiz dinamik değerin bir imzasını tutan bir düzenleyen kurumun imzalı bir sertifikasını satıcı cihazından talep etmek üzere satıcı cihazına satıcı onay talebi iletilmesi; satıcı cihazından, satıcının kişisel anahtarı kullanılarak, düzenleyen kurumun imzalı sertifikası ve benzersiz dinamik değerin bir imzasını içeren ikinci bir veri paketini alınması; onay kurumunun ortak anahtarı kullanılarak düzenleyici kurumun imzalı sertifikasının doğrulanması aracılığıyla satıcı cihazının geçerliğinin doğrulanması, doğrulandığında, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı imzalı benzersiz dinamik değerin doğrulanması; bellekten bir hesaplama değeri ve saklanan bir müşteri cihazı kişisel anahtarı alınır; sadece imzalı benzersiz dinamik değerin, satıcı ortak anahtarı kullanılarak birinci veri paketinde alınan benzersiz dinamik değere karşı doğrulanması halinde, satıcı cihazına, alınan benzersiz statik satıcı tanımlayıcı ve bir şifreli yazı iletilmesi, şifreli yazı, müşteri cihazı için alınan bir gizli anahtar, alınan bir hesaplama değeri, alınan benzersiz statik satıcı tanımlayıcı ve işlem talebi verisi kullanılarak oluşturulmuştur; ve işlemin başarılı olup olmadığını gösteren bir bildirimin satıcı cihazından alınması; burada şifreli yazı, satıcı cihazının, müşteri cihazından alınan benzersiz statik satıcı tanımlayıcısının, alıcı tarafından verilen benzersiz statik satıcı kimlik belirleyicisi ile eşleşip eşleşmediğini kontrol

etmesini sağlar ve eşleşmesi halinde, alınan şifreli yazı, benzersiz statik satıcı tanımlayıcı ve işlem talebi verilerini içeren bir onay talebi oluşturur ve söz konusu işlem talebi verilerinin doğrulanması ve işlenmesini kolaylaştırmak üzere bir düzenleyici kurum ve bir alıcıdan en az birine söz konusu onay talebini sunar; ve burada benzersiz statik satıcı tanımlayıcının bir kopyası, satıcı cihazı ile bağlı bir satıcının, geçerli bir satıcı olduğunu doğrulamak üzere alıcı aracılığıyla güvenli bir şekilde tutulur.

Birinci alıcı-verici cihazı, bir mobil telefon, cep telefonu veya iPhone gibi bir mobil iletişim cihazına dahil edilebilir. İsteğe bağlı olarak, birinci alıcı-verici cihazı, bir mobil iletişim cihazından ayrılabilir ancak iletişim içinde olabilir. İsteğe bağlı olarak, birinci alıcı-verici cihaz, bir satış noktası cihazına (POS) dahil edilebilir veya ayrılabilir ancak bir POS ile iletişim içinde olabilir. Yine diğer düzenlemelerde, alıcı-verici cihaz, (bir dizüstü, PDA, çağrı cihazı gibi) bir kişisel hesaplama cihazına veya bir kişisel hesaplama cihazından ayrılan ancak bununla iletişim içinde olan bir cihaza entegre edilebilir.

Arayüz modülü, bir temaslı arayüz modülü, bir temassız arayüz modülü veya bir ikili temas ve temassız arayüz modülü şeklinde olabilir. Bir temassız arayüz modülünü kullanan bir düzenlemede, arayüz modülü tercihen, (ISO 7816, NFC, Bluetooth, Wi-Fi, SMS, vb. gibi) iki cihaz arazında veri transferini sağlamak üzere gerekli mekanizmaları içerir. Örneğin, bir bu tür temassız arayüz modeli, bir aktarıcı ve bir anten içerebilir.

İşlem talebi verileri, işlem için bir tutar ve en az bir (veya daha fazla) döviz kodu, bir zaman damgası ve bir PIN veya biyometrik gibi bir müşteri tanımlayıcı ve herhangi diğer ilgili verileri içerebilir.

Şekillerin Kısa Açıklaması

Önceki teknik, Şekil 1'e referans ile açıklanmıştır, bu, bir açık ağ üzerinden bir ödeme işlemindeki tipik dördüncü parti ağ katılımını gösterir.

Buluşun bir örneği, beraberindeki şekillere referans ile bu noktada açıklanacaktır, burada:

Şekil 2, açık ağlar üzerinden işlemlerin güvence altına alınmasına yönelik olarak bir alıcı-verici cihazının bileşenlerini şematik olarak gösteren bir blok diyagramdır.

Şekil 3, açık ağlar üzerinden işlemlerin güvence altına alınmasına yönelik olarak bir sistemin bileşenlerini şematik olarak gösteren bir blok diyagramdır.

Şekil 4, açık ağlar üzerinden işlemlerin güvence altına alınmasında dahil edilen adımların bir akış şemasıdır; ve

Şekil 5, Şekil 4'te gösterilen spesifik adımın bir akış şemasıdır.

Buluşun En Uygun Yöntemi

Şekil 2, açık ağlar üzerinden işlemlerin güvence altına alınmasına yönelik olarak bir alıcı-verici cihazının (10) bileşenlerini gösterir. Açık ağ veya açık iletişim ağı teriminin, İnternet Protokolü (IP) ağı gibi herhangi bir kablosuz, genellikle emniyetsiz ağ olarak kapsamlı bir şekilde tanımlandığı kabul edilmelidir. Örneğin, açık ağ altyapısı, genellikle internet omurgasına ve bir yerel alan ağı (LAN) ve bir geniş alan ağından (WAN) her birine refere eden ağları içerebilir. LAN ve WAN'nin her biri, bir yönlendirici veya Ağ

Adres Çevrimi (NAT) sunucusu aracılığıyla İnternete bağlanır ve her biri, IP çerçevelerini aktarabilir.

Alıcı-verici cihazı (10),bir diğer alıcı-verici cihazı ile iletişim kurmak üzere konfigüre edilen herhangi bir cihazdır. Bu örnekte, alıcı-verici cihaz (10), bir mobil telefon şeklinde bir mobil iletişim cihazına dahil edilen bir cihazdır.

Gösterildiği üzere, alıcı-verici (10), bir temaslı veya temassız arayüz modülü (CIM) (12) şeklindeki bir arayüz modülünü içerir. Bu örnekte CIM(12) temassız bir arayüz modelidir. CIM (12), (ISO 7816, Yakın Saha İletişimi (NFC), Bluetooth, SMS, vb. gibi) iki cihaz arasındaki verilerin transferine yönelik herhangi bir mekanizma olabilir ve bu başvuruda NFC kullanılır. NFC, birbirine birkaç santimetre getirildiğinde cihaz (10) ile komşu cihaz arasında iletişim sağlamak üzere manyetik alan kullanan kısa mesafe kablosuz bağlantı standardıdır (Ecma-340, ISO/IEC 18092). Standart, verileri değiştirmek üzere bir uç birimden uç birime (P2P) ağ kurmak üzere ilgili cihazlara yönelik bir yolu belirtir. P2P ağı konfigüre edildiğinde, Bluetooth gibi bir diğer teknoloji, daha uzun mesafe iletişiminden faydalanabilir.

CIM'ye birleştirilen, cihaz (10) ve belleğin (16) işlemini kontrol eden bir merkezi işlem birimidir (14). İşlem modülü (18), herhangi bir uygun bilgisayar dilini (C, C++, Java, Perl, PHP, vb.) kullanan bir yazılım uygulaması, bilgisayar programları, vb. olarak uygulanır. Yazılım, işlemci (14), belleği okuduğunda, burada açıklanan işlevler, gerçekleştirilecek şekilde belleğe (16) yazılan talimatlar veya komutlar dizisi olarak saklanır.

Belleğin (16) programlanabilir kısmına ek olarak, bellek,

geçici bellek ve kalıcı bellek ve salt okunur bellek gibi farklı bellek tiplerini içerebilir.

Şekil 3, buluşa ait bir düzenlemenin, açık ağlar üzerinden işlemleri güvence altına almak amacıyla kullanılabildiği bir sistemi (20) gösterir. Benzer numaralar, benzer bileşenlere refere eder. Sistem (20), bu örnekte "satıcı cihazı" olarak konfigüre edilen bir birinci alıcı-verici cihazı (10) ve bu örnekte bir "müşteri cihazı" olarak konfigüre edilen ikinci bir alıcı-verici cihazını (22) içerir. Bu örnekte, satıcı cihazı (10) ve müşteri cihazı (22), mobil erişimli NFC özellikli cihazlardır ve her biri, ilgili temassız arayüzleri (12) ile iletişim kurmak üzere konfigüre edilir. Her cihaz (10, 22), Şekil 2'ye göre açıklanan bileşenler ile donatılır.

Satıcı alıcı-verici cihazının (10) bellek birimi (16), işlem tutarının kredilendirileceği satıcıyı tanımlayan benzersiz satıcı tanımlayıcıyı güvenli bir şekilde saklar. Satıcı tanımlayıcı, çıkarma prosesi sırasında cihazın (10) belleğine gömülüdür ve bir kopya, alıcı tarafından güvenli bir şekilde tutulur. Müşteri alıcı-verici cihazının (22) bellek birimi (16), kullanıcının ana hesap numarasını ("PAN"), kullanıcının kişisel kimlik numarasını ("PIN"), bir uygulama işlemi sayacı (ATC) ve bir gizli anahtarı güvenli bir şekilde saklar. Gizli anahtar, çıkarma prosesi sırasında cihazın (22) belleğine gömülüdür ve bir kopya, düzenleyen kurum (30) tarafından güvenli bir şekilde tutulur.

Satıcı cihazı (10), bir ağ (26) üzerinden bir alıcı (28) ve/veya bir düzenleyen kurum (30) ile iletişim kurar. Cihaz, teknikte bilinen herhangi bir uygun şekilde ağa bağlanabilir. Ağ (26), bunlarla sınırlı olmamak üzere yerel alan ağı, geniş alan ağı, telefon ağı ve/veya veri iletmek üzere konfigüre edilen herhangi bir kablolu iletişim ağını içeren herhangi bir tipte dağıtım sistemini içerebilir.

Şekil 4, açık ağlar üzerinden işlemlerin güvence altına alınmasına yönelik olarak bir yöntemin (40) adımlarını gösterir. Yöntem, şekil 3'te gösterilen sistem aracılığıyla uygulanabilir. Yöntem, ön işlem prosesi (adım 42), keşif prosesi (adım 44), başvuru seçimi (adım 46), başvuru işleme (adım 48) ve işlem onayının (adım 50) genel adımlarını içerir.

Ön işlem prosesi (adım 42), (işlem tutarı ve döviz kodunu içeren) çeşitli verileri ve müşteri cihazına (22) gönderilmek üzere gereken statik işlem verilerini toplayan satıcı cihazını (10) içerir. Ek olarak CIM (12), müşteri cihazı (22) ile iletişime yönelik etkinleştirilir.

Adım 44'teki keşif prosesi, adım 42'deki ön işlem prosesini takip eder. Müşterinin cihazı (22), satıcı cihazının (10) mesafesinde olduğunda iletişim, cihazın ilgili CIM'leri (12) ile kurulur. Satıcı cihazı (10), CIM'sini (12) harekete geçirir ve CIM'si (12) aracılığıyla müşteri cihazı (22) ile bir bağlantı kurar. Satıcı cihazının (10), mesafe alanı içinde çoklu temassız cihazları saptaması halinde, satıcı cihazı (10), bu koşulu müşteri cihazının (22) sahibine gösterebilir ve işlem için sadece tek bir cihazın sunulmasını talep edebilir.

İlgili cihazlar arasında iletişim kurulduğunda, satıcı cihazı (10), müşteri cihazına (22) bir başvuru seçimi iletisi toplar ve iletir.

Başvuru seçimi adımı (46), keşif prosesi adımını (44) takip eder ve başvuru seçimi iletisine bir yanıt oluşturulmasını içerir. Başvuru seçimi adımı (Şekil 5'e referans olarak daha detaylı gösterilir), başvuru keşfi (62), güncel başvuru seçimi (64) ve PIN ibrazını (66) içerir.

Başvuru seçimi (60), iki metodolojiden birini kullanabilir. Müşteri cihazının (22), hesapların bir listesini oluşturabilen akıllı bir cihaz olması halinde, müşteri cihazı, uygun hesapların bir listesini oluşturmaya devam eder ve müşteri cihazı, müşteri seçimine (adım 62) yönelik olarak cihazın ekranı üzerinde hesapların listesini gösterir. Bunun üzerine, müşteri cihazının (22) kullanıcısı, muhtemelen cihazın (22) gövdesi üzerindeki bir tuş takımı ile giriş yolu aracılığıyla bir hesabı seçer (adım 64). Tuş takımının, fiziksel bir klavye veya bir sanal klavye olabildiği kabul edilmelidir. Bir hesap seçilmesine yanıt olarak kullanıcı daha sonra, cihazın (22) gövdesi üzerindeki aynı tuş takımında bir PIN girer (adım 66), bunun değeri, akabinde bellekte kayıtlı bir referans değerine karşı kontrol edilir.

Müşteri cihazı (22) daha sonra, başvuru seçimi iletisine yanıt verir ve seçilen hesap bilgisini, satıcı cihazına (10) iletir. Ek olarak, müşteri cihazı (22), güvenli işlemi tamamlamak üzere gereken spesifik bilgiye yönelik olarak satıcı cihazına (10) bir talep gönderir.

Müşteri cihazının (22), gerekli bilgi hizmetine sahip olmaması halinde, başvuru seçimi iletisinin alınmasına yanıt olarak, müşteri cihazı (22), uygun hesapların bir listesini oluşturur ve uygun hesapların listesini, satıcı cihazına (10) iletir. Satıcı cihazı (10) daha sonra, satıcı cihazının (10) desteklediğine karşı müşteri cihazından (22) alınan listelenmiş hesapları karşılaştırır. Satıcı cihazının (10) desteklediği hesapların listesi, daha sonra satıcı cihazının ekranı üzerinde müşteri cihazının (22) kullanıcısına gösterilir (adım 62). Bunun üzerine, kullanıcı, muhtemelen, satıcı cihazının (10) gövdesi üzerindeki bir kullanıcı ekranındaki bir tuş takımı aracılığıyla işlemin değerinin borçlandırılması için bir hesap seçer (adım 64). Bir hesap

seçilmesine yanıt olarak kullanıcı daha sonra bir PIN girer (adım 66). Seçilen hesabın veri göstergesi, daha sonra satıcı cihazındaki (10) belleğe depolanır. Ek olarak, seçilen hesabın ve sunulan PIN'nin veri göstergesi, satı cihazından (10) müşteri cihazına (22) iletilir. Müşteri cihazı, akabinde müşteri cihazının belleğinde saklanan bir referans değere karşı girilen PIN verisini kontrol eder. İlk metodolojideki gibi, hesap seçimi talebine yanıt olarak, müşteri cihazı (22), güvenli işlemi tamamlamak üzere gereken spesifik bilgiye yönelik olarak satıcı cihazına (10) bir talep gönderir.

Kullanılan metodolojiye bakılmaksızın, sonradan toplanan spesifik bilgi, işlemi işlemek üzere gereken spesifik veri ile birlikte satıcı cihazının (10) özellikleri ile ilgili çeşitli detaylar içerecektir.

Başvuru prosesi adımı (48), başvuru seçimi adımını (46) takip eder ve bir komut iletisinin toplanmasını içerir. Güvenli işlemi tamamlamak üzere gereken spesifik bilgiye yönelik olarak müşteri alıcı-verici cihazının (22) talebine yanıt olarak, satıcı cihazı (10), akabinde müşteri alıcı-verici cihazına (22) iletilen bir komut iletisini toplar.

Komut iletisi, birçok veri elemanı veya alan içerir. Bir birinci alana, satıcıyı tanımlayan benzersiz bir değer yerleştirilir. Bu değer, alıcı organizasyonlarca bilinecektir. İkinci bir alana, işlemin bir tutarının veri temsilcisi yerleştirilir. Üçüncü bir alana, işlemin döviz kodunun veri temsilcisi yerleştirilir. Dördüncü bir alana, işlem tutarının borçlandırılacağı müşteri tarafından seçilmiş hesabın veri temsilcisi yerleştirilir. İlave alanlara, işlemi daha da güvenli hale getirmek üzere sağlanan bir benzersiz sayı ile bağlantılı veri, kullanıcı tarafından seçilen hesabın veri temsilcisi ve müşteri cihazı (22) veya satıcı cihazı (10)

üzerinde olan, hesap seçimi zamanında alınabilen bir PIN yerleştirilebilir.

Satıcı cihazı (10), PIN doğrulama girişimlerinin aşılmamış olmasını garanti altına almak üzere ve ortadaki adam saldırıları ve işlemin yarıda kesilmesine karşı korumak üzere birçok risk yönetimi prosesi gerçekleştirir. İşlemin yarıda kesilmesi, işlem tamamlanmadan önce bir alıcı-verici cihazının, bağlantı alanından diğer bir alıcı-verici cihaz ile çıkarıldığı durumu açıklar. İşlem modülü başvurusu, iki cihazın işlemi tamamlamak üzere bir veri iletişim yolunu yeniden oluşturması gerektiğinde, prosesin nerede olduğunu daima bilmesini sağlamalıdır. Aslında, ilgili cihazlar işlemin tamamlanmadığını veya tüm değerlerin işlemin başlamasından önceki değerlere sıfırlandığını varsayılır veya ilgili cihazlar, işlemin diğer cihaza göre tamamlandığını varsayılır ve her bir cihaz, kesinti noktasındaki herhangi bir değişiklik ile bağlantılı verileri saklar. Bir sonraki durumda, bu tür veri, herhangi bir uyuşmazlığı çözmekten sorumlu Düzenleyen kuruma iletilir.

Risk yönetimi prosesinin tamamlanmasının ardından, müşterinin cihazının (22) işlemcisi (14), komut iletisine uygun güvenli yanıtı oluşturur ve güvenli yanıtı, satıcı alıcı-verici cihazına (10) iletir.

Güvenli yanıt, işlemi işlemek üzere benzersiz satıcı tanımlayıcı ve tüm gerekli bilgi ile birlikte müşteri cihazı (22) için benzersiz bir anahtar kullanılarak hesaplanan bir şifreli yazıya bağlıdır. Komut mesajında olduğu gibi, yetkilendirme cevabı, ilk üçü daha önce satıcı cihazından alınan verilerle, benzersiz satıcı tanımlayıcısı, işlem tutarı ve para birimi koduyla doldurulmuş olan bir dizi veri alanı içerir. Ek olarak, komut iletisine güvenli onay yanıtının diğer alanlarına, Müşteri cihazının PAN'si veya kullanıcı

tarafından seçilen hesaba karşılık gelen düzenleyen kurumun başvuru veri yolu (2), bir başvuru işlem sayacı (ATC) ve doğru/yanlış yanıtın PIN doğrulama bilgisi göstergesi yerleştirilir. Müşteri cihazı (22), Başvuru İşlemi Sayacı (ATC) olarak refere edilen bir sayaç değerini yönetir. ATC, şifreli yazı hesaplamasına dahil edilir ve her işlem ile tekrar saldırılarına karşı bir savunma olarak artırılır.

Güvenli yanıt, satıcı cihazına (10) iletilir. Güvenli yanıt ile dahil edilen, satıcıyı tanımlayan benzersiz değer olabilir. Yanıt alındığında, satıcı, yanıtı kontrol eder ve yanıtın, satıcıyı tanımlayan bir değer içermesi halinde, satıcı cihazı (10), alınan değerin, satıcı cihazının belleğinde güvenli bir şekilde saklanan satıcıyı tanımlayan benzersiz tanımlama değerine karşılık geldiğini kontrol eder. Satıcıyı tanımlayan alınan değer ve satıcıyı tanımlayan benzersiz değerin bir ve aynı olması kaydıyla, güvenli yanıt, akabinde alıcı/düzenleyen kuruma gönderilmeye hazırdır.

Müşteri alıcı-verici cihazı (22), bu noktada satıcı alıcı-verici cihazın (10) mesafe alanından uzaklaştırılabilir.

Onay adımı (50), başvuru prosesi adımını (48) takip eder. Satıcı alıcı-verici cihazı (10), güvenli yanıtı, alıcıya ve akabinde doğrulama için düzenleyen kuruma gönderir. Bir işlem alınmasında, düzenleyen kurum, müşteri cihazının anahtarının kopyasını kullanarak şifreli yazıyı yeniden hesaplayabilir. Daha sonra düzenleyen kurumdan alınan bir yanıta bağlı olarak, satıcı alıcı-verici cihazı (10), işlemin başarılı olması halinde müşteri alıcı-verici cihazının (22) kullanıcısını bilgilendirir.

Şifreli yazıdan tekrar hesaplanan veri tam sayılarak, düzenleyen kurum, kullanıcı tarafından seçilen hesaba işlemin değerini ödeyecektir. Alıcı/düzenleyen kurum, müşteri

cihazının (22), daha önce aldığı bilgiyi ve ayrıca işlemden geçirilmesi için sisteminden elde edilen diğer bilgileri satıcı cihazına (10) geri döndürmesi nedeniyle satıcının kimliği ve müşterinin kimliğinin güvencesine sahiptir. Ortadaki adamın mevcut olması halinde, satıcı cihazı, sonrasında uyarılacaktır.

Buluşa uygun metodoloji, ek olarak satıcının geçerliğini onaylayabilir. Bu, benzersiz bir dinamik değerin asimetrik işaretlenmesi aracılığıyla gerçekleştirilebilir.

Alıcı-verici cihazlar (10, 22) çıkarıldığında, bir veya daha fazla onay kurumunun (CA) kişisel anahtarı ile imzalanan bir sertifikada, düzenleyen kurumun (30) ortak anahtarı ile yüklenir. Ek olarak, alıcı-verici cihazlar (10, 22), sertifikada bulunan düzenleyen kurumun (30) ortak anahtarını doğrulamak amacıyla bir veya daha fazla onay kurumuna yönelik ortak anahtar ile yüklenebilir.

Ek olarak, her bir alıcı-verici cihazın (10, 22) güvenli modülü (24), yüklenen kendi ortak/kişisel anahtar çiftine sahiptir. Her bir ilgili güvenli modülün (24) ortak anahtarı, düzenleyen kurumun (30) kişisel anahtarı ile imzalı bir sertifikaya özgü tanımlama değerinde tutulur.

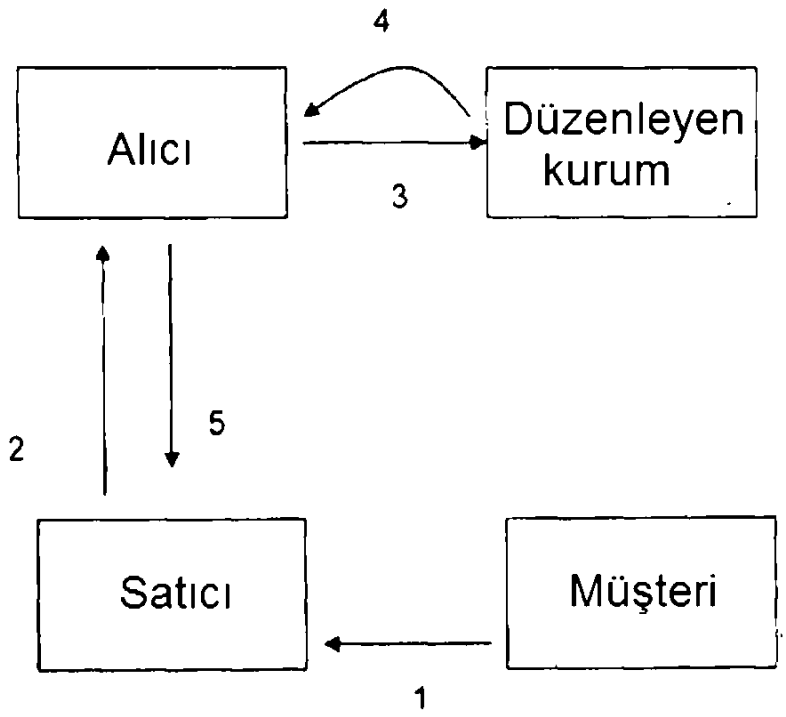
Müşteri alıcı-verici cihazı (22), benzersiz tanımlama numarasını tutan, Düzenleyen kurumun (30) imzalı sertifikasını, satıcı alıcı-verici cihazından (10) talep eder. Ek olarak, satıcı alıcı-verici cihazının (10), güvenli modülün (24) kişisel anahtarı kullanılarak benzersiz dinamik değeri imzalamasını talep eder.

Müşteri alıcı-verici cihazı (22), CA ortak anahtarı kullanılarak CA imzalı Düzenleyen kurum sertifikasını doğrular ve onaylandığında, müşteri alıcı-verici cihazı (22),

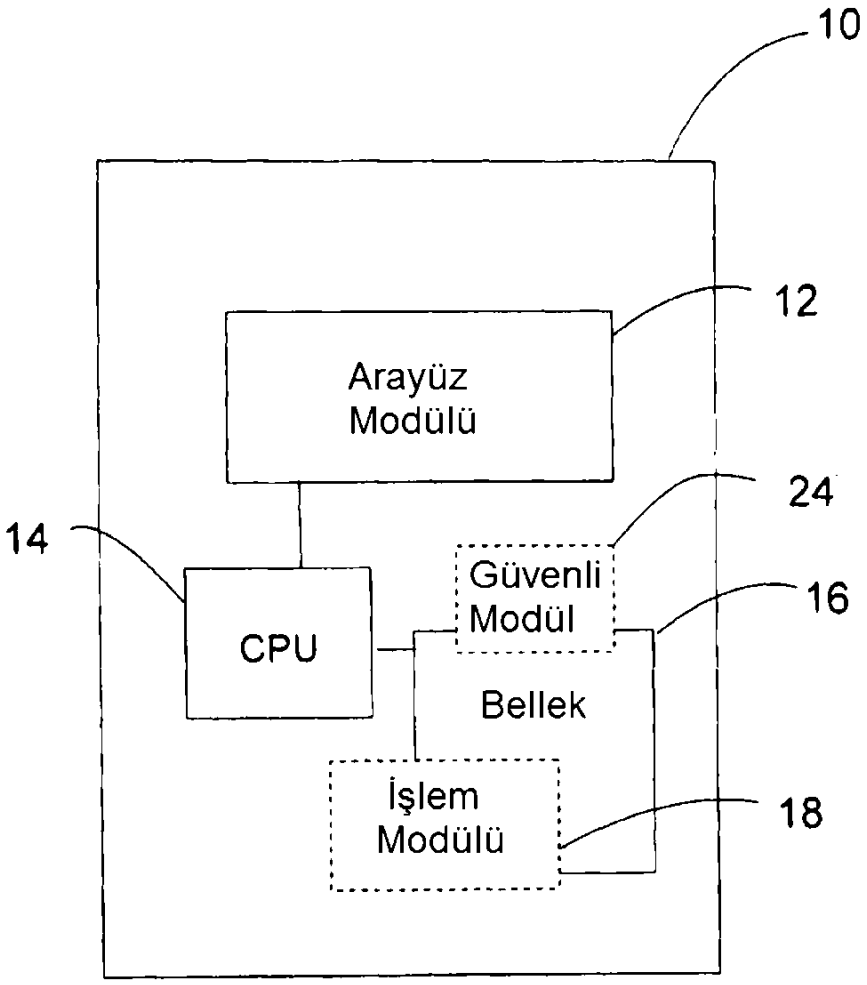
Düzenleyen kurumun ortak anahtarı kullanılarak Düzenleyen kurumun imzalı güvenli modülünü onaylar ve akabinde satıcının düzenleyen kurum tarafından imzalı sertifikasına yüklenen ortak anahtar kullanılarak imzalı benzersiz dinamik değeri onaylar.

Teknikte uzman kişilerce açık olması gerektiği üzere, buluşa ait düzenlemeler, avantajlı olarak örneğin EMV (Europay, Mastercard ve VISA) kullananlar gibi bilinen tekniklerdekinden daha basittir. EMV, satıcıyı ve tüketiciyi tek bir işleme bağlamayı tasarlamaz, bunun tersine EMV, yalnızca bir işlemde geçerli bir kartın kullanıldığını belirtir. Daha sonra, buluşa ait düzenlemeler, belirli bir işlemi güvence altına almak üzere gerekli olan satıcı cihazına dayanmaz, ayrıca satıcı, tüketici ve düzenleyen kurum arasında kurulmuş olan önceden var olan bir ilişkinin koşuluna da dayanmaz.

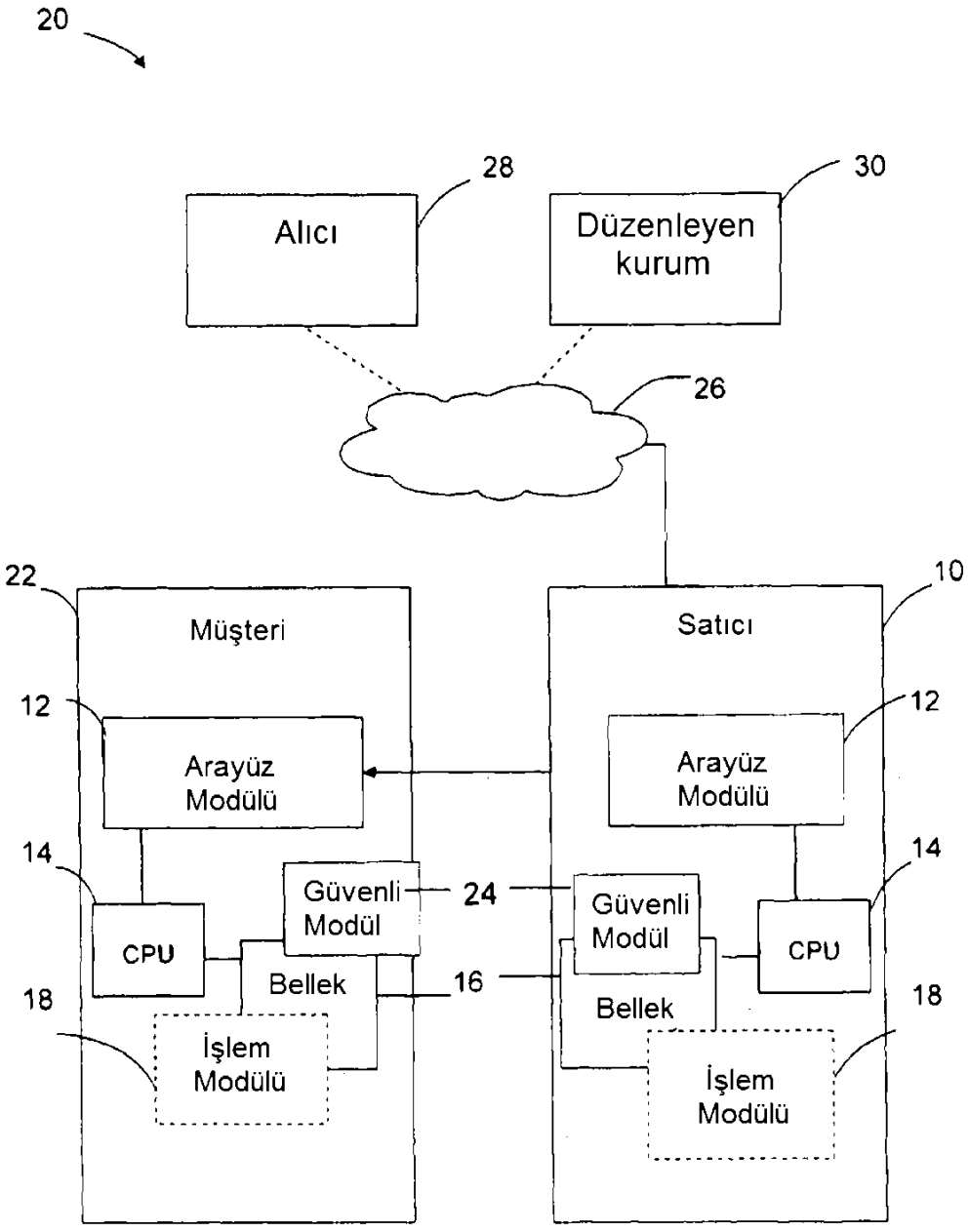
Tanımlanan buluşun kapsamından ayrılmaksızın spesifik düzenlemelerde gösterildiği üzere, buluşa sayısız varyasyon ve/veya modifikasyonun uygulanabileceği, teknikte uzman kişilerce kabul edilecektir. Ayrıca, buluşa ait düzenlemeler, sadece iç piyasa için değil, aynı zamanda uluslararası bağlam dahilinde ödeme şemalarına yönelik olarak da uygundur. Mevcut düzenlemeler bu nedenle, tüm bağlamlarda açıklayıcı olarak kabul edilir ve kısıtlayıcı değildir.



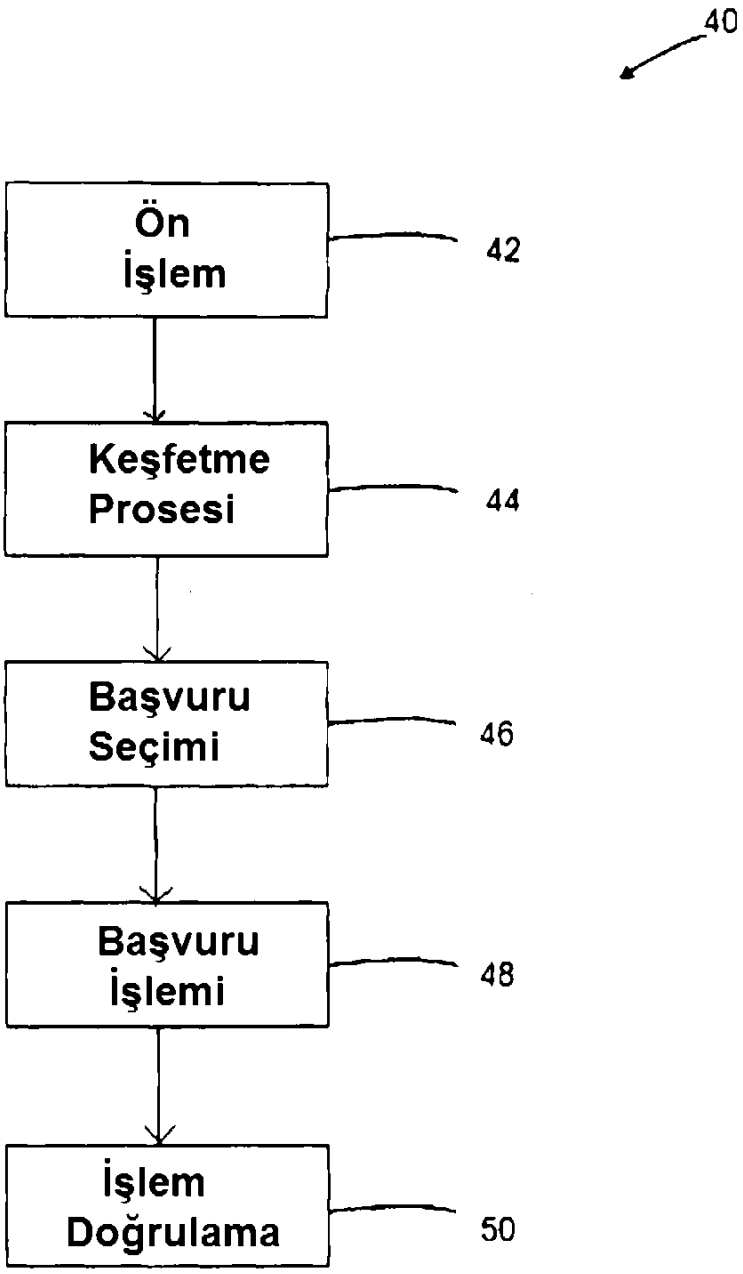
Şekil 1


10
12
Arayüz
Modülü
24
14
Güvenli
Modül
16
CPU
Bellek
İşlem
Modülü
18

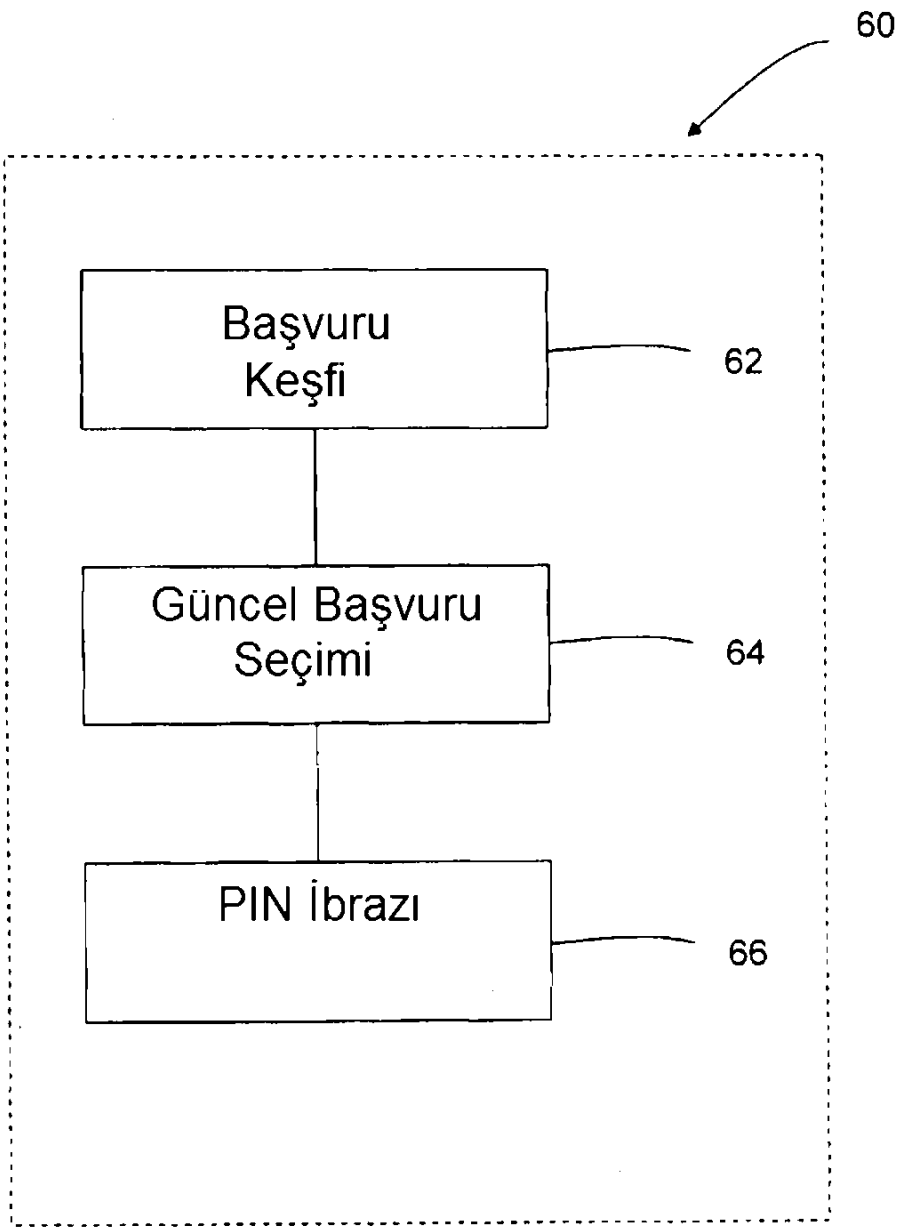
Şekil 2


20
28
Alıcı
30
Düzenleyen kurum
26
22
Müşteri
10
Satıcı
12
Arayüz Modülü
12
Arayüz Modülü
14
CPU
Güvenli Modül
24
Güvenli Modül
CPU
14
Bellek
16
Bellek
18
İşlem Modülü
18
İşlem Modülü

Şekil 3


40
Ön İşlem
42
Keşfetme Prosesi
44
Başvuru Seçimi
46
Başvuru İşlemi
48
İşlem Doğrulama
50

Şekil 4



Şekil 5