

ÖZET

MAMUL ÜRÜNLERİ FİZİKSEL KARAKTERİSTİĞİ KULLANARAK İŞARETLEMELİK İÇİN YÖNTEM VE TERTİBAT

- Mevcut buluş, mamul ürünleri işaretleme için yöntemlere ve tertibata ilişkindir. Mevcut
- 5 buluş bilhassa ambalajlı ürünlerin işaretlenmesine ilişkindir. Yöntem şunları içerir: bir mamul ürün için benzersiz bir ürün tanımlayıcısının oluşturulması; bir veya birkaç şifreleme anahtarının oluşturulması; benzersiz ürün tanımlayıcısı ve bir veya birkaç şifreleme anahtarı kullanılarak bir gizli anahtarın üretilmesi; gizli anahtar ve benzersiz ürün tanımlayıcısı kullanılarak bir sistem gürültü değerinin üretilmesi; mamul ürünün ölçülen bir
- 10 fiziksel niteliğinden bir fiziksel anahtarın üretilmesi; fiziksel anahtar ve benzersiz ürün tanımlayıcısı kullanılarak bir fiziksel gürültü değerinin üretilmesi; ve mamul ürünün üzerine bir işaretin yerleştirilmesi.

İSTEMLER

- 1) Yöntem olup, bir mamul ürünü işaretlemek içindir ve şunları içerir:
bir mamul ürün için benzersiz bir ürün tanımlayıcısının (UPI) oluşturulması;
bir veya birkaç şifreleme anahtarının (209, 219) oluşturulması;
5 benzersiz ürün tanımlayıcısı ve bir veya birkaç şifreleme anahtarı kullanılarak bir gizli anahtarın (223) üretilmesi;
gizli anahtar ve benzersiz ürün tanımlayıcısı kullanılarak bir sistem gürültü değerinin (225) üretilmesi;
mamul ürünün ölçülen bir fiziksel niteliğinden bir fiziksel anahtarın (207) üretilmesi;
10 fiziksel anahtar ve benzersiz ürün tanımlayıcısı kullanılarak bir fiziksel gürültü değerinin (227) üretilmesi;
sistem gürültü değerini ve fiziksel gürültü değerini oluşturmak üzere, yöntemde yer değiştirme, ikame etme, tabloda ikame etme ve indeksleme ya da benzersiz ürün tanımlayıcısının gizli anahtar ile kombinasyonunda ve benzersiz ürün tanımlayıcısının
15 fiziksel anahtar ile kombinasyonunda kriptografik bir özet fonksiyonu kullanılır;
gizli anahtardan ve fiziksel anahtardan türetilen veya bunları içeren güvenli bir tanımlayıcının (251, 271, 281) üretilmesi; güvenli tanımlayıcı, sistem gürültü değerinden türetilir veya bunu içerir ve güvenli tanımlayıcı fiziksel gürültü değerinden türetilir veya bunu içerir; ve
20 mamul ürünün üzerine bir işaretin yerleştirilmesi (319, 355); işaret, güvenli tanımlayıcıyı veya güvenli tanımlayıcıdan türetilmiş bir tanımlayıcıyı içerir.
- 2) İstem 1'e uygun yöntem olup, özelliği güvenli tanımlayıcının benzersiz ürün tanımlayıcıyı içermesidir.
- 3) İstem 2'ye uygun yöntem olup, özelliği güvenli tanımlayıcıyı üretme adımının, benzersiz
25 ürün tanımlayıcısının sistem gürültü değeriyle birlikte şifrlenmesi suretiyle birinci bir tanımlayıcının üretilmesini (311, 313) ve birinci tanımlayıcının fiziksel gürültü değeriyle birlikte şifrlenmesi (317) suretiyle güvenli tanımlayıcının üretilmesini içermesidir.
- 4) İstem 3'e uygun yöntem olup, özelliği şunlardır:
- benzersiz ürün tanımlayıcısını sistem gürültü değeriyle birlikte şifreleyerek birinci
30 tanımlayıcıyı üretme adımı, bir kod üretici gizleme anahtarı (CGOK) ile şifreleme (313) yoluyla gerçekleştirilir;
- birinci tanımlayıcı ardından fiziksel gürültü değeri ve bir kod üretici tanımlayıcısı (233) ile birleştirilir;

- birinci tanımlayıcı, fiziksel gürültü değeri ve kod üretici tanımlayıcısının kombinasyonu ardından güvenli tanımlayıcıyı 251 üretmek üzere bir genel anahtar (235) kullanılarak şifrelenir (317).
- 5) İstem 4'e uygun yöntem olup, özelliği şunlardır: kod üretici gizleme anahtarı önceden yüklenmiş olduğu bir kod üreticine (111) özgüdür ve genel anahtar bir veya birkaç üretim merkezinin tümü için ortaktır.
- 6) İstem 3'e uygun yöntem olup, ayrıca mamul ürünün kimliğinin bir doğrulama merkezinde doğrulanmasını içerir, özelliği kimlik doğrulama adımının şunları içermesidir:
 - 10 ürün üzerindeki işaretin tanımlanması (321);
 - birinci tanımlayıcıyı ve fiziksel gürültü değerini türetmek için işaretin şifresinin çözülmesi (323);
 - benzersiz ürün tanımlayıcısını ve sistem gürültü değerini türetmek için birinci tanımlayıcının şifresinin çözülmesi (325);
 - 15 mamul ürünün ölçülen bir fiziksel niteliğinden yeni bir fiziksel anahtarın üretilmesi (327);
 - yeni fiziksel anahtar ve türetilen benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek fiziksel gürültü değerinin yeni bir kopyasının üretilmesi (329);
 - 20 fiziksel gürültü değerinin yeni kopyasının türetilen fiziksel gürültü değeri ile karşılaştırılması (331); ve
 - türetilen fiziksel gürültü değerinin, fiziksel gürültü değerinin yeni kopyasıyla aynı olup olmadığına veya bağıntı kurup kurmadığına ilişkin bir göstergenin sağlanması (339).
- 7) İstem 6'ya uygun yöntem olup, özelliği kimlik doğrulama adımının ayrıca şunları içermesidir:
 - 25 benzersiz ürün tanımlayıcısından ve bir veya birkaç şifreleme anahtarından gizli anahtarın yeni bir kopyasının üretilmesi (333);
 - gizli anahtarın yeni kopyası ve benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek sistem gürültü değerinin yeni bir kopyasının üretilmesi (335);
 - 30 sistem gürültü değerinin yeni kopyasının türetilen sistem gürültü değeri ile karşılaştırılması (337); ve
 - sistem gürültü değerinin yeni kopyasının ve türetilen sistem gürültü değerinin aynı olup olmadığına ilişkin bir göstergenin sağlanması (339).

- 8) İstem 2'ye uygun yöntem olup, özelliği güvenli tanımlayıcıyı üretme adımının şunları içermesidir:
- benzersiz ürün tanımlayıcısının sistem gürültü değeri ile birlikte şifrenmesi (241) suretiyle birinci bir güvenli tanımlayıcının üretilmesi;
- 5 benzersiz ürün tanımlayıcısının fiziksel gürültü değeri ile birlikte şifrenmesi suretiyle ikinci bir güvenli tanımlayıcının üretilmesi (261); ve
- mamul ürünün üzerine bir işaretin yerleştirilmesi (355); işaret, birinci ve ikinci güvenli tanımlayıcıları ya da birinci ve ikinci güvenli tanımlayıcılardan türetilmiş bir tanımlayıcı veya tanımlayıcılar içerir.
- 10 9) İstem 8'e uygun yöntem olup, özelliği şunlardır:
- sistem gürültü değeri benzersiz ürün tanımlayıcısı ile birleştirilir; sistem gürültü değeri ve benzersiz ürün tanımlayıcısının kombinasyonu ardından birinci bir tanımlayıcıyı üretmek (241) için bir kod üretici gizleme anahtarı (CGOK) ile şifrenir (343);
 - 15 - birinci tanımlayıcı ardından bir kod üretici tanımlayıcısı (CGID) ile birleştirilir ve birinci bir güvenli tanımlayıcıyı üretmek için bir genel anahtar (235) ile şifrenir (347);
 - fiziksel gürültü değeri, ikinci bir tanımlayıcıyı (261) üretmek için benzersiz ürün (351) ile birleştirilir;
 - 20 - ikinci tanımlayıcı, ikinci bir güvenli tanımlayıcıyı (281) üretmek için genel anahtar (235) ile şifrenir.
- 10) İstem 8'e uygun yöntem olup, ayrıca mamul ürünün kimliğinin bir doğrulama merkezinde doğrulanmasını içerir, özelliği kimlik doğrulama adımının şunları içermesidir:
- 25 ürün üzerindeki işaretin tanımlanması (401);
- benzersiz ürün tanımlayıcısını, sistem gürültüsünü ve fiziksel gürültüyü üretmek için işaretin şifresinin çözülmesi (403, 405);
- benzersiz ürün tanımlayıcısından ve bir veya birkaç şifreleme anahtarından gizli anahtarın yeni bir kopyasının üretilmesi (413);
- 30 gizli anahtarın yeni kopyası ve benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek sistem gürültü değerinin yeni bir kopyasının üretilmesi (415);
- sistem gürültü değerinin yeni kopyasının türetilen sistem gürültü değeri ile karşılaştırılması (417);

- mamul ürünün ölçülen bir fiziksel niteliğinden yeni bir fiziksel anahtarın üretilmesi (407);
- yeni fiziksel anahtar ve türetilen benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek fiziksel gürültü değerinin yeni bir kopyasının üretilmesi (409);
- 5 fiziksel gürültü değerinin yeni kopyasının türetilen fiziksel gürültü değeri ile karşılaştırılması (411); ve
- hem sistem gürültü değerinin yeni kopyasının türetilen sistem gürültü değeriyle aynı olup olmadığına hem de fiziksel gürültü değerinin yeni kopyasının türetilen fiziksel gürültü değeri ile aynı olup olmadığına veya bağıntı kurup kurmadığına ilişkin bir göstergenin sağlanması (419).
- 10
- 11) Önceki istemlerden herhangi birine uygun yöntem olup, özelliği şunlardır: bir veya birkaç şifreleme anahtarı bir statik anahtar (209) ve bir dinamik anahtar (219) içerir ve mamul ürünlerin her bir partisii için yeni bir dinamik anahtar oluşturulur.
- 15
- 12) Önceki istemlerden herhangi birine uygun yöntem olup, özelliği benzersiz ürün tanımlayıcısının, ürünün ait olduğu ürün partisii tanımlayan bilgiler içermesidir.
- 13) Önceki istemlerden herhangi birine uygun yöntem olup, özelliği şunlardır: bir gürültü değeri bir özet değeridir ya da anahtarlanmış bir özet değeridir ya da doğrudan bir özet değerinden ve bir gizli anahtardan türetilmiş bir değer veya karakter dizisidir.
- 20
- 14) Önceki istemlerden herhangi birine uygun yöntem olup, özelliği mamul ürünün ölçülen fiziksel niteliğinin, mamul ürünün yüzey dokusu temelinde olmasıdır.
- 15) Tertibat olup, bir mamul ürünü işaretlemek içindir ve şunları içerir:
- şifreleme anahtarları üreten yapıda bir anahtar üretici (115);
- her bir mamul ürün için benzersiz bir ürün tanımlayıcısı üreten yapıda bir kod üretici (111);
- 25 her bir mamul ürünün ölçülen bir fiziksel niteliğinden fiziksel anahtarlar üreten yapıda bir fiziksel anahtar üretici (112);
- işleme aracı (111) şunları gerçekleştiren yapıdadır:
- benzersiz ürün tanımlayıcısı ve bir veya birkaç şifreleme anahtarını kullanarak her bir mamul ürün için bir gizli anahtar (223) üretmek;
- 30 gizli anahtar ve bir benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek her bir mamul ürün için bir sistem gürültü değeri (225) üretmek;
- fiziksel anahtar ve benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek her bir mamul ürün için bir fiziksel gürültü değeri (227) üretmek;

gizli anahtardan ve fiziksel anahtardan türetilen veya bunları içeren bir güvenli tanımlayıcı (251, 271, 281) üretmek; güvenli tanımlayıcı, sistem gürültü değerinden türetilir veya bunu içerir ve güvenli tanımlayıcı fiziksel gürültü değerinden türetilir veya bunu içerir; ve

- 5 her bir mamul ürünü güvenli tanımlayıcı veya güvenli tanımlayıcıdan türetilmiş bir tanımlayıcı ile işaretlemek (319, 355) için bir işaretleyici.

16) İstem 15'e uygun tertibat olup, özelliği mamul ürünün ölçülen fiziksel niteliğinin, mamul ürünün yüzey dokusu temelinde olmasıdır.

MAMUL ÜRÜNLERİ FİZİKSEL KARAKTERİSTİĞİ KULLANARAK İŞARETLEMELİK İÇİN
YÖNTEM VE TERTİBAT

5 Mevcut buluş, mamul ürünleri işaretleme için yöntemlere ve tertibata ilişkindir. Mevcut buluş bilhassa ambalajlı ürünlerin işaretleme ile ilişkindir.

Sahte veya kaçak mallar, müşteriler, üreticiler ve devlet otoriteleri için küresel bir sorundur. Genellikle düşük kaliteli malların izinsiz üretimleri olan sahte mallar tüm dünyada yasa dışı olarak satılmaktadır. Bu mallar müşteriye zarar verir, çünkü düşük kalitede olabilirler, bu da tehlikeli olabilir (bu bilhassa ilaçlar veya diğer tüketim malları gibi ürünler için önemlidir).

10 Sahte mallar üreticilere zarar verir, çünkü üreticiler itibar kaybına, ürünlerinin yasa dışı üreticilerce üretilmesi nedeniyle rekabette bir artışa ve diğer yasal hakların ihlaline maruz kalabilirler. Vergilerden veya resmi düzenlemelerden kaçmak amacıyla üretilen mallar olan kaçak mallar, üreticiler ve devlet otoriteleri için de önemli bir sorundur. Bu mallar yasa dışı olarak amacından saptırılır, ticareti yapılır veya ithal edilir; bu da uygunsuz harç veya vergi

15 tahsilatı nedeniyle devlet otoriteleri için önemli miktarda gelir kaybıyla sonuçlanır.

Her benzersiz işareti ürünlerin kimliğinin doğrulanacağı yerde depolamak zorunda kalmadan, mamul ürünlerin kimliğini ürünler üzerinde benzersiz işaretler kullanarak doğrulayabilmek elverişlidir. Ayrıca, otantik bir ürünün benzersiz işaretinin kopyalandığı ürünlerin veya sahte ürünlerin, her benzersiz işaretin kimlik doğrulama kaydını saklamaya

20 gerek duymadan tespit edilebilmesi de istenir.

WO 01/43086 sayılı Uluslararası Patent Başvurusu Yayını, her ürün numunesi için modifiye edilmiş özgün bir doku üzerinde üretilen bir görüntü kullanılarak ürünlerin işaretleme ile açıklar.

WO 97/24699 sayılı Uluslararası Patent Başvurusu Yayını, ürünlerin kimliğinin, ürünlerin

25 fiziksel veya kimyasal bir karakteristiğinin şifreli olarak kodlanması yoluyla doğrulanmasını açıklar.

US 6.212.638 sayılı Amerika Birleşik Devletleri Patenti, bir ürünü tanımlamak için öngörülemez bir sembol dizisinin üretilmesini açıklar.

M.Lehtonen, N. Oertel, H. vogt, "Features, Identity, Tracing, and Cryptography in Product Authentication", 13th International Conference on Concurrent Enterprising, 4 June 2007,

30 ürün kimlik doğrulama tekniğine genel bir bakışı açıklar.

Buluşun bir yönüne göre, bir mamul ürünü işaretleme üzere istem 1'e uygun bir yöntem sağlanır.

Burada kullanıldığı üzere, "benzersiz ürün tanımlayıcısı", bir mamul ürünü benzersiz bir biçimde tanımlayan bir tanımlayıcı anlamına gelir. Her bir mamul ürüne farklı bir benzersiz ürün tanımlayıcısı verilir. Benzersiz ürün tanımlayıcısı tipik olarak sayısal veya alfanümerik bir dizi veya değerdir.

- 5 Burada kullanıldığı üzere, "şifreleme", bilgiyi, o bilgiyi bir şifreleme anahtarı biçiminde özgün bilgiye sahip olanlar haricinde herkes için okunamayacak hale getirmek için bir algoritma kullanarak dönüştürme işlemi anlamına gelir. Şifre çözme ters işlemdir. Bir "şifreleme anahtarı", bilgileri şifrelemek veya şifresini çözmek için bir şifreleme algoritmasıyla birlikte kullanılan bir bilgi parçasıdır. Bir şifreleme anahtarı tipik olarak
- 10 sayısal veya alfanümerik bir dizi veya değerdir.

- Burada kullanıldığı üzere "gizli anahtar" terimi, benzersiz bir ürün tanımlayıcısı ve bir veya birkaç ilave anahtar veya veri parçası kullanılarak üretilen anahtarlanmış bir özet içerisinde kullanılan bir anahtar tarif etmek için kullanılır. Oluşturulduğu sırada, gizli anahtar, gizli anahtar oluşturan taraftan başka hiçbir tarafça bilinmez. Bu bağlamda "gizli anahtar"
- 15 teriminin anlamı, asimetrik bir şifreleme şeması bağlamında özgün bir anahtar ile sınırlı değildir.

- Burada kullanıldığı üzere bir "özet fonksiyonu", giriş verilerini özet değeri adı verilen, (genellikle giriş verilerinden daha küçük olan) sabit boyutlu bir çıktı ile eşleyen bir fonksiyondur. Bir özet fonksiyonu tipik olarak, özet değerini veya gürültü değerini
- 20 oluşturmak üzere bilgiyi ikame eder veya yerini değiştirir ya da ikame eder ve yerini değiştirir. Tercihen, özet fonksiyonu kriptografik bir özet fonksiyonudur. Kriptografik özet fonksiyonu, giriş verilerinin bir parmak izini veya sağlama toplamını oluşturur. Aynı kriptografik özet fonksiyonu kullanılarak aynı özet değerini üretilenlerse iki veri parçasının aynı olduğu varsayılabilir. Elverişli olarak, özet fonksiyonu tek yönlü bir özet fonksiyonudur;
- 25 bu, özet değerinden giriş verileri türetmenin hesaplama yoluyla imkansız olduğu anlamına gelir. Bu nitelikler, açıklanacağı üzere bir kimlik doğrulama işleminde kullanılabilir. Bir özet fonksiyonu, anahtarlanmış bir özet değeri veya gürültü oluşturmak için bir gizli anahtar ile bir giriş mesajı birleştirilerek anahtarlanabilir.

- Burada kullanıldığı üzere "gürültü değeri" ifadesi, bir özet değeri veya anahtarlanmış bir
- 30 özet değeri ya da doğrudan bir özet değerinden ve bir gizli anahtardan türetilmiş bir değer veya karakter dizisi anlamına gelir.

Mamul ürünün ölçülen fiziksel niteliği, ölçülen herhangi bir fiziksel nitelik olabilir ve kütle, boyut, biçim, yüzey dokusu veya deseni, renk, kimyasal bileşim, veya bir uyarana verilen yanıt, örneğin elektriksel, manyetik veya optik bir uyarana verilen yanıt temelinde olabilir.

Ölçülen fiziksel nitelik, tercihen, her mamul ürün için benzersiz olmasının muhtemel olacağı veya hiç değilse herhangi iki mamul ürün için aynı olandan farklı olmasının daha muhtemel olacağı bir çözünürlükte seçilir ve ölçülür. Ölçülen fiziksel nitelik tercihen mamul ürün için fiziksel bir imza sağlar. Tercih edilen bir uygulamada, ölçülen fiziksel nitelik, mamul ürünün ambalajının bir kısmının görüntüsüdür.

Güvenli tanımlayıcı, herhangi bir tanımlayıcı türü olabilir, ancak tercihen sayısal veya alfanümerik bir dizi veya değerdir. İşaret ayrıca bir karakter veya sayı dizisi olabilir ya da bir veya iki boyutlu barkod gibi grafiksel bir gösterim olabilir.

Bir uygulamada, güvenli tanımlayıcıyı üretme adımı, benzersiz ürün tanımlayıcısının sistem gürültü değeriyle birlikte şifrelenmesi suretiyle birinci bir tanımlayıcının üretilmesini ve birinci tanımlayıcının fiziksel gürültü değeriyle birlikte şifrelenmesi suretiyle güvenli tanımlayıcının üretilmesini içerir.

Bu uygulamada, yöntem ayrıca, mamul ürünün kimliğinin bir doğrulama merkezinde doğrulanmasını içerebilir, kimlik doğrulama adımı şunları içerir: ürün üzerindeki işaretin tanımlanması; birinci tanımlayıcıyı ve fiziksel gürültü değerini türetmek için işaretin şifresinin çözülmesi; benzersiz ürün tanımlayıcısını ve sistem gürültü değerini türetmek için birinci tanımlayıcının şifresinin çözülmesi; mamul ürünün ölçülen bir fiziksel niteliğinden yeni bir fiziksel anahtarın üretilmesi; yeni fiziksel anahtar ve türetilen benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek fiziksel gürültü değerinin yeni bir kopyasının üretilmesi; fiziksel gürültü değerinin yeni kopyasının türetilen fiziksel gürültü değeri ile karşılaştırılması; ve türetilen fiziksel gürültü değerinin, fiziksel gürültü değerinin yeni kopyasıyla aynı olup olmadığına veya bağıntı kurup kurmadığına ilişkin bir göstergenin sağlanması.

Karşılaştırma adımı, bir bağıntı puanı türetilmesini içerebilir ve bir gösterge sağlama adımı, bağıntı puanının bir eşik değerden daha büyük olup olmadığına ilişkin bir gösterge sağlanmasını içerir.

Bu uygulamada, kimlik doğrulama adımı ayrıca şunları içerebilir: benzersiz ürün tanımlayıcısından ve bir veya birkaç şifreleme anahtarından gizli anahtarın yeni bir kopyasının üretilmesi; gizli anahtarın yeni kopyası ve benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek sistem gürültü değerinin yeni bir kopyasının üretilmesi; sistem gürültü değerinin yeni kopyasının türetilen sistem gürültü değeri ile karşılaştırılması; ve sistem gürültü değerinin yeni kopyasının ve türetilen sistem gürültü değerinin aynı olup olmadığına ilişkin bir göstergenin sağlanması.

Başka bir uygulamada, güvenli tanımlayıcıyı üretme adımı şunları içerir: benzersiz ürün tanımlayıcısının sistem gürültü değeri ile birlikte şifrlenmesiyle birinci bir güvenli tanımlayıcının üretilmesi; benzersiz ürün tanımlayıcısının fiziksel gürültü değeri ile birlikte şifrlenmesiyle ikinci bir güvenli tanımlayıcının üretilmesi; ve mamul ürünün üzerine bir
5 işaret yerleştirilmesi; işaret, birinci ve ikinci güvenli tanımlayıcıları ya da birinci ve ikinci güvenli tanımlayıcılardan türetilmiş bir tanımlayıcı veya tanımlayıcılar içerir.

Bu uygulamada, yöntem ayrıca, mamul ürünün kimliğinin bir doğrulama merkezinde doğrulanmasını içerebilir, kimlik doğrulama adımı şunları içerir: ürün üzerindeki işaretin tanımlanması; benzersiz ürün tanımlayıcısını, sistem gürültü değerini ve fiziksel gürültü
10 değerini türetmek için işaretin şifresinin çözülmesi; benzersiz ürün tanımlayıcısından ve bir veya birkaç şifreleme anahtarından gizli anahtarın yeni bir kopyasının üretilmesi; gizli anahtarın yeni kopyası ve benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek sistem gürültü değerinin yeni bir kopyasının üretilmesi; sistem gürültü değerinin yeni kopyasının türetilen sistem gürültü değeri ile karşılaştırılması; mamul ürünün
15 ölçülen bir fiziksel niteliğinden yeni bir fiziksel anahtarın üretilmesi; yeni fiziksel anahtar ve türetilen benzersiz ürün tanımlayıcısı üzerinde bir özet fonksiyonu gerçekleştirilerek fiziksel gürültü değerinin yeni bir kopyasının üretilmesi; fiziksel gürültü değerinin yeni kopyasının türetilen fiziksel gürültü değeri ile karşılaştırılması; ve hem sistem gürültü değerinin yeni kopyasının türetilen sistem gürültü değeriyle aynı olup olmadığına hem de fiziksel gürültü
20 değerinin yeni kopyasının türetilen fiziksel gürültü değeri ile aynı olup olmadığına veya bağıntı kurup kurmadığına ilişkin bir göstergenin sağlanması.

Her iki uygulamada, birinci güvenli tanımlayıcıyı üretme adımı, bir kod üretici anahtarı kullanılarak benzersiz ürün tanımlayıcısının ve sistem gürültü değerinin şifrlenmesini içerebilir; burada ikinci güvenli tanımlayıcıyı üretme adımı, birinci güvenli tanımlayıcının ve
25 fiziksel gürültü değerinin bir kod üretici kimliği ile birlikte birleştirilmesini içerir ve burada kod üretici anahtarı, kod üretici kimliği kullanılarak bir doğrulama merkezindeki bir arama tablosundan türetililebilir veya elde edilebilir.

Her iki uygulamada, yöntem ayrıca bir veya birkaç şifreleme anahtarını bir doğrulama merkezinde depolama adımını içerebilir. Bir veya birkaç şifreleme anahtarı, bir statik
30 anahtar ve bir dinamik anahtar içerebilir ve burada mamul ürünlerin her bir partisi için yeni bir dinamik anahtar oluşturulurken, mamul ürünlerin birçok partisi için ise aynı statik anahtar kullanılır.

Benzersiz ürün tanımlayıcısı, ürünün ait olduğu bir ürün partisini tanımlayan bilgileri içerebilir.

5 Buluş, hem üreticiden gelen bilgiler, yani çeşitli şifreleme anahtarları temelinde hem de ürünün fiziksel bir niteliği temelinde kimlik doğrulama yeteneği sağlar. Bu, iki kademeli kimlik doğrulama sağlar ve orijinal ürünler üzerindeki tanımlayıcıların klonlanmasının saptanmasını sağlar, ancak kimlik doğrulama kodlarının büyük ölçekli depolanmasını gerektirmez.

Buluşun başka bir yönüne göre, bir mamul ürünü işaretlemek üzere istem 15'e uygun bir tertibat sağlanır.

10 Bir düzenlemede, işleme aracı şunları gerçekleştiren yapıdadır: benzersiz ürün tanımlayıcısını gizli anahtar veya sistem gürültü değeriyle birlikte şifreleyerek her bir mamul ürün için birinci bir tanımlayıcıyı üretmek; ve birinci tanımlayıcıyı fiziksel gürültü değeriyle birlikte şifreleyerek her bir mamul ürün için güvenli tanımlayıcıyı üretmek.

15 Başka bir düzenlemede işleme aracı şunları gerçekleştiren yapıdadır: benzersiz ürün tanımlayıcısını gizli anahtar veya sistem gürültü değeriyle birlikte şifreleyerek her bir mamul ürün için birinci bir güvenli tanımlayıcıyı üretmek; ve benzersiz ürün tanımlayıcısını fiziksel anahtar veya fiziksel gürültü değeriyle birlikte şifreleyerek her bir mamul ürün için ikinci bir güvenli tanımlayıcıyı üretmek; ve işaretleyici, her bir mamul ürünü birinci güvenli tanımlayıcı ve ikinci güvenli tanımlayıcı ya da birinci ve ikinci güvenli tanımlayıcılardan türetilmiş bir tanımlayıcı veya tanımlayıcılar ile işaretleyen yapıdadır.

20 Mamul ürün, tütün ürünü içeren bir kap olabilir. Tütün ürünlerinin örnekleri şunlardır: sigara, gevşek yapraklı tütün, puro ve elektrikle ısıtılan sigara içme sistemleri veya diğer elektronik sigara sistemleri için kovan veya kartuş.

25 Buluş, mamul ürünlerin kimliğinin büyük miktarlarda bilgi depolama gerekmeden doğrulanmasını sağlar. Bu, büyük miktarda üretilen ürünlerin kimliğinin doğrulanması için uygun olan herhangi bir pratik sistem için önemlidir. Ayrıca, benzersiz bir ürün tanımlayıcısı (UPI) ile birlikte bir fiziksel anahtarın kullanılması güvenliği artırır ve sahte ve kaçak malların üretimini daha da zorlaştırır. Fiziksel bir anahtarın eklenmesi, klonlamayı saptayabilen ve kopyalaması zor olan bir sistem sağlar. Bir sahtekar fiziksel anahtarı üretmek için kullanılan belirli bir araca ilişkin bilgi sahibi olsa bile, bir tanımlayıcı üretmek için fiziksel anahtarın bir UPI ile birleştirilmesi klonlamayı neredeyse imkansız kılar. Buluş 30 ayrıca, kimlik doğrulama işleminin çevrimiçi olarak, yani sistem gürültü değerine dayalı bir iletişim ağı üzerinden bir doğrulama merkezine bağlı olarak gerçekleştirilmesini sağlamanın yanı sıra, kimlik doğrulama işleminin fiziksel gürültü değerine dayalı olarak çevrimdışı gerçekleştirilmesini sağlar. Her üründe gerekli olan işaret sadece bir veya birkaç koddur ve

bu nedenle, çoğaltılması teknik açıdan zor olan pahalı etiketlere dayanan diğer bazı çözümlere nispeten, her ürüne çok az masraf ekler.

Buluşun uygulama/düzenlemeleri şimdi yalnızca örnek yoluyla ekteki çizimlere atıfla açıklanacaktır, bu çizimlerde:

- 5 Şekil 1 buluşun bir düzenlemesine uygun bir işaretleme sisteminin şematik görünümüdür; Şekil 2 sistem gürültü değerinin ve fiziksel gürültü değerinin nasıl türetildiğini gösterir; Şekil 3 Şekil 1'deki sistemde gerçekleştirilebilen, buluşun bir uygulamasına ait bir işaretleme yöntemini gösteren bir akış şemasıdır; Şekil 4 Şekil 1'deki sistemde gerçekleştirilebilen, Şekil 3'te gösterilen buluşa ait uygulama
- 10 için bir kimlik doğrulama yöntemini gösteren bir akış şemasıdır; Şekil 5 Şekil 1'deki sistemde gerçekleştirilebilen, buluşun başka bir uygulamasına ait bir işaretleme yöntemini gösteren bir akış şemasıdır; ve Şekil 6 Şekil 1'deki sistemde gerçekleştirilebilen, Şekil 5'te gösterilen buluşa ait uygulama için bir kimlik doğrulama yöntemini gösteren bir akış şemasıdır;
- 15 Mamul ürünler üzerindeki benzersiz işaretler, ürünlerin izlenmesi için kullanılabilir. Örneğin, bir müşteri siparişi, sipariş edilen malları içeren belirli bir nakliye kutusunun veya kutularının tanımlayıcı etiketine veya etiketlerine bağlanabilir. Bu bağlamda "mallar", dağıtım veya müşterilere satış amaçlı mamul ürünler veya diğer ürünler anlamına gelir. Bu, müşterinin, üreticinin ve aracılarnın gerekli malların konumunu sürekli olarak izlemesini sağlar. Bu,
- 20 tanımlayıcıları tarama ve bir doğrulama merkezi ile iletişim kurma amaçlı tarayıcılar kullanılarak gerçekleştirilebilir. Alternatif olarak, tanımlayıcılar bir insan tarafından okunabilir, bu insan daha sonra bir doğrulama merkezi ile manuel olarak iletişim kurabilir. Tanımlayıcılar, belirli bir ürünün orijinal ürünler içerdiğini doğrulamak için müşteriler, ulusal otoriteler ve diğer taraflarca da kullanılabilir. Örneğin, bir taraf, bir nakliye kutusu üzerindeki
- 25 tanımlayıcıyı okumak için bir tarayıcı kullanabilir (veya tanımlayıcı yukarıda anlatıldığı gibi bir insan tarafından okunabilir). Tanımlayıcı bilgileri bir doğrulama merkezine gönderilebilir. Doğrulama merkezi ardından tanımlayıcı bilgilerini arayıp bulabilir veya başka bir şekilde işleyebilir, nakliye kutusu üretim bilgilerini belirleyebilir ve bu bilgileri tarayıcıya gönderebilir, böylece tarafın nakliye kutusunu ve içinde bulunan ürünleri orijinal olarak doğrulamasını
- 30 sağlar. Merkezi veri tabanının tanımlayıcıyı tanımaması durumunda, taraf söz konusu ürünlerin sahte olduğunu varsayabilir. Tanımlayıcılar, ürünlerin izlenmesi için de kullanılabilir. Örneğin, üreticinin ürünleri belirli sayıda nakliye kutusundan geri çağırması gerekiyorsa, bu nakliye kutuları kendi tanımlayıcıları kullanılarak izlenebilir.

Şekil 1 buluşun bir düzenlemesine uygun bir işaretleme sisteminin şematik görünümüdür.

- 35 Bu düzenlemede, sistem 101, mamul ürünleri 109 üretmek için bir veya birkaç üretim

merkezi 103, 105, 107 içerir. Her bir üretim merkezi, bir sigara üretim ve ambalajlama hattı olabilen bir üretim hattı veya tesisi içerebilir. Tercihen, üretim partiler halinde gerçekleştirilir, her bir parti belirli sayıda münferit mamul ürünün üretimine tayin edilmiştir. İki veya daha fazla üretim merkezi varsa, bunlar fiziksel olarak aynı veya farklı üretim tesislerinde yer alabilirler. Tercih edilen bu düzenlemede, sistem, üretim merkezlerini 103, 105, 107 içerir ancak buluş aslında bir ithalat noktasında, bir dağıtım noktasında, bir alıcıda, bir toptancıda veya tedarik zincirindeki başka herhangi bir noktada gerçekleştirilebilir.

Her bir üretim merkezi, mamul ürünler 109 için kodlar üretmeye yönelik bir kod üretici 111 içerir. Tercihen, kod üretici 111 belirli bir üretim merkezine tayin edilmiş tamamen otonom bir bilgisayar veya mikrodenetleyicidir. Her bir üretim merkezi ayrıca, her bir mamul ürünün fiziksel bir niteliğini ölçen veya kodlayan ve bunu bir fiziksel anahtara 207 dönüştüren bir fiziksel anahtar üretici 112 içerir. Kod üretici 11, ürünlerin üzerine işaretlenecek kodlar üretmek üzere fiziksel anahtarlar kullanır.

Bu düzenlemede, fiziksel anahtar üretici WO2007/071788'de açıklanan tiptedir. Her ürünün ambalajının bir kısmı aydınlatılır ve aydınlatılan kısmın bir görüntüsü bir dijital görüntü sensörü tarafından yakalanır. Ambalaj kısmı zamanla değişmeyen, kaotik mikro yapısı dolayısıyla seçilir. Kağıt ve karton gibi malzemeler, ürünün "parmak izi" olarak kullanılabilir kaotik bir mikro yapıya sahiptirler. Ürün kısmının mikro yapısının görüntüsü, WO2007/071788'de açıklandığı gibi, alfanümerik bir değer veya matris biçiminde fiziksel bir anahtara veya imzaya dönüştürülür. Bu tipte bir fiziksel anahtar üretici, Signoptic Technologies, Savoie Technolac, 5 allée Lac d'Aiguebelette BP340 F-73375, LE BOURGET-DU-LAC, Fransa'dan temin edilebilir. Ancak, herhangi bir tip fiziksel anahtar üretici kullanılabilir ve anahtar ürünün kütle veya biçim gibi diğer fiziksel niteliklerine dayanabilir ve hatta ürünün kimyasal veya biyolojik niteliklerine dayanabilir.

Bu düzenlemede, her bir üretim merkezi ayrıca, üretilen kodları mamul ürünlerin 109 üzerine işaretlemek için bir işaretleyici 113 içerir. İşaretleyici 113, uygun herhangi bir işaretleme aracını, örneğin sınırlayıcı olmamak kaydıyla sürekli bir mürekkep püskürtmeli yazıcıyı, talep üzerine damlamalı bir mürekkep püskürtmeli yazıcıyı, bir holografik yazıcıyı, bir lazer yazıcı ya da üretilen kodların münferit mamul ürünlerin üzerine basılmasını veya işaretlenmesini sağlayan başka herhangi bir yazıcı ya da işaretleyiciyi kapsayabilir. Üretilen kodların baskısı veya işareti, her bir ürün üzerinde, harici bir ambalaj üzerinde, etiketler üzerinde veya başka herhangi bir uygun şekilde olabilir. Bir uygulamada, üretilen kodlar, mamul ürünlere tercihen çıkarılamaz bir şekilde uygulanacak olan yapışkanlı fişlerin veya etiketlerin üzerine basılır. Bir uygulamada, üretilen kodlar, mamul ürünün üzerine veya

ürünün ambalajı üzerine çöktürülen lazere duyarlı bir malzeme katmanı üzerine bir lazer ışını ile basılır. Bu yöntem, kodun şeffaf bir ambalaj katmanı arasından basılmasını sağlar.

Sistem 101 ayrıca bir doğrulama merkezi 114 içerir, doğrulama merkezi ise mamul ürünlerin işaretlenmesi ve kimliğinin doğrulanmasında kullanılmak üzere anahtarlar 209, 211 üretmek için bir anahtar üretici 115 ve merkezi bir sunucu 117 içerir. Bu düzenlemede, kod üretici 111, güvenli bir internet bağlantısı 119 ve üretim merkezine yerel bir sunucu 121 üzerinden veya başka veri iletişim araçları vasıtasıyla doğrulama merkezi 114 ile iletişim kurabilir. Alternatif olarak, kod üretici 111 bir veya birkaç üretim merkezine tayin edilmiş bir üretim portalı üzerinden doğrulama merkezi ile iletişim kurabilir.

10 Anahtar üretici 115, burada statik anahtar olarak anılan kriptografik bir anahtar üretir. Anahtar üretici 115, statik anahtarın şifrelenmemiş bir versiyonunu ve statik anahtarın şifrelenmiş bir versiyonunu üretir. Burada etkin statik anahtar 209 olarak anılan statik anahtarın şifrelenmemiş versiyonu, Şekil 1'de düz bir sınır ile gösterilir. Burada etkin olmayan statik anahtar 211 olarak anılan statik anahtarın şifrelenmiş versiyonu, Şekil 1'de 15 noktalı bir sınır ile gösterilir. Etkin statik anahtar 209, yani statik anahtarın şifrelenmemiş versiyonu, anahtar üreticinde 115 üretilir ve bu nedenle merkezi sunucu 117 tarafından erişilebilir. Anahtar üretici 115, etkin olmayan statik anahtarı 211 üretim merkezindeki 103, 105, 107 kod üreticisine 111 gönderir.

Etkin olmayan statik anahtar 211, anahtar üreticiden 115 kod üreticisine 111 uçucu olmayan bir veri desteği, örneğin bir CD-Rom, bir DVD-Rom veya çıkarılabilir bir sabit disk 20 vasıtasıyla gönderilebilir. Veri desteği fiziksel olarak üretim merkezindeki 103, 105, 107 kod üreticisine 111 aktarılır. Alternatif olarak, etkin olmayan statik anahtar 211, anahtar üreticiden 115 kod üreticisine 111, güvenli bir ağ bağlantısı, örneğin şifrelemeyi içeren bir ağ bağlantısı üzerinden gönderilebilir. Bu, kod üreticiden 111 alınan talep üzerine olabilir. 25 Bu, statik anahtarın özgünlüğünü, gizliliğini ve bütünlüğünü sağlar.

Anahtar üretici 115 ayrıca, etkin statik anahtarı 209 oluşturmak üzere etkin olmayan statik anahtarın 211 şifresini çözme amaçlı anahtar veya kodu içeren etkinleştirme kodunu 213 üretir. Bu etkinleştirme koduna 213 ayrıca merkezi sunucu 117 tarafından erişilebilir. Tercihen, etkin statik anahtar 209 ve etkinleştirme kodu 213, tayin edildikleri üretim 30 merkezinin 103, 105, 107 tanımlamasıyla birlikte depolanır.

Bir uygulamada, statik anahtar birkaç kısım içerir. Birincil kısım, birçok gizli kod, örneğin bir tuz matrisi olabilir. Bir tuz matrisi, örneğin, rastgele veya sözde karakter rakamlarından oluşan uzun bir dizi olabilir. Kısımların numarası ayrıca statik anahtar için benzersiz bir tanımlayıcı, statik anahtarın (aşağıda anlatılan) dinamik bir anahtar ile nasıl birleştirileceğini

tanımlayan seri hale getirilmiş bir kod, statik anahtarın benzersiz tanımlayıcısını birleştiren dijital bir kriptografik sertifika ve yukarıda üretilen dijital kriptografik sertifikayı içeren bir statik anahtar ilkesi veya lisansı içerir.

5 Etkin olmayan statik anahtar, yani statik anahtarın şifrelenmiş versiyonu ve bilhassa birçok gizli kod, tercihen güçlü bir şifre kullanılarak şifrelenir. Uygun bir şifrenin bir örneği, Üçlü DES (Veri Şifreleme Standardı) blok şifresi veya Üçlü DES/Rijandel blok şifresidir. Her ikisi de Veri Şifreleme Standardı şifreleme algoritmasını her veri bloğuna üç kez uygular ve Üçlü DES/Rijandel, IBM tarafından geliştirilen Üçlü DES'in küçük bir varyasyonudur. Bu durumda, Üçlü DES veya Üçlü Des/Rijandel anahtarı, etkinleştirme kodunu 213 içerir.

10 Böylece, tercih edilen bir uygulamada, etkin statik anahtar 209 şifrelenmez, etkin olmayan anahtar 211, Üçlü DES veya Üçlü Des/Rijandel anahtarı kullanılarak şifrelenir ve etkinleştirme kodu 213, Üçlü DES veya Üçlü Des/Rijandel anahtarını içerir.

Sonraki adım 203'te, kod üretici 111 tarafından alınan etkin olmayan statik anahtar 211 kaydedilir. Bu, kod üretici 111 tarafından, alınan statik anahtar ve ilgili tüm makine bilgileri

15 (gösterilmez) hakkındaki bilgiler 215 doğrulama merkezine 114 gönderilerek yapılır. Bu, tercihen Şekil 1'de gösterildiği gibi güvenli internet bağlantısı 119 üzerinden gönderilir, ancak başka bir uygun yol aracılığıyla gönderilebilir. Doğrulama merkezi 114, etkinleştirme kodunu 213 kod üreticisine 111 geri gönderir. Etkinleştirme kodu 213 etkin olmayan statik anahtarın 211 etkinleştirilmesini sağlar ve bu, 217 ile şematik olarak gösterilir. Etkinleştirme

20 kodu 213 tercihen, Şekil 1'de gösterildiği gibi güvenli internet bağlantısı 119 üzerinden de gönderilir. Kayıt prosedürü tercihen, etkin statik anahtar 209 asla internet üzerinden aktarılmayacak şekilde düzenlenir.

Kayıt prosedürü, alışlagelmiş bir ortak/özgün anahtar çifti değişim mekanizması biçimini alabilir. Bu, yukarıda anlatıldığı gibi, statik anahtarın bir parçasını oluşturan dijital

25 kriptografik sertifika ile ilişkilendirilmiş asimetrik bir anahtar çifti kullanabilir. Bu durumda, asimetrik anahtar çiftinin ortak anahtarı, üçüncü bir tarafça, örneğin bir devlet otoritesince verilen bir anahtar biçiminde olabilir. Kod üreticiden 111 doğrulama merkezine 114 gönderilen, alınan statik anahtar hakkındaki bilgiler 215, yukarıda anlatıldığı gibi statik anahtarın bir parçasını oluşturan statik anahtar benzersiz tanımlayıcısını içerebilir. Yine kod

30 üreticiden 111 doğrulama merkezine 114 gönderilen ilgili makine bilgileri (gösterilmez), kod üretici 111 veya üretim merkezi için benzersiz bir tanımlayıcı veya sertifika içerebilir. Bu benzersiz tanımlayıcı, üretim için önceden yetkilendirilmiş kod üreticinin veya üretim merkezinin yeri ve kimliği hakkında bilgiler içerebilir. Tercihen, statik anahtar benzersiz tanımlayıcısı ve kod üretici veya üretim merkezi tanımlayıcısı, statik anahtarın sertifikasıyla

35 ilişkilendirilmiş asimetrik anahtar çiftinin ortak anahtarı kullanılarak şifrelenir.

Doğrulama merkezi 114 şifrelenmiş statik anahtar benzersiz tanımlayıcısını ve kod üretici veya üretim merkezi tanımlayıcısını aldığı anda, doğrulama merkezi 114, statik anahtarın sertifikasıyla ilişkilendirilmiş asimetrik anahtar çiftinin özgün anahtarını kullanarak şifreyi çözebilir. Doğrulama merkezi ardından statik anahtar benzersiz tanımlayıcısının ve kod
5 üretici veya üretim merkezi tanımlayıcısının geçerli olduğunu kontrol edebilir. Ardından, doğrulama merkezi 114, etkinleştirme kodunu 213 kod üreticisine 111 geri gönderir. Daha önce bahsedildiği gibi, etkinleştirme kodu 213 tercihen bir Üçlü DES veya Üçlü DES/Rijandel şifresi biçimindedir. Doğrulama merkezi, etkinleştirme kodunu (örneğin, Üçlü DES veya Üçlü DES/Rijandel şifresi), statik anahtarın sertifikasıyla ilişkilendirilmiş asimetrik
10 anahtar çiftinin ortak anahtarıyla şifreler. Bu, etkinleştirme kodunun (örneğin, Üçlü DES veya Üçlü DES/Rijandel şifresi) şifresinin, statik anahtarın sertifikasıyla ilişkilendirilmiş asimetrik anahtar çiftinin özgün anahtarı kullanılarak kod üretici tarafından çözülmesini sağlar. Ardından, etkin olmayan statik anahtar 211, etkin statik anahtarı 209 oluşturmak üzere şifresi çözülmüş etkinleştirme kodu 213 kullanılarak etkinleştirilebilir.

15 Kod üreticindeki 111 etkin olmayan statik anahtar 211 etkinleştirildiğinde, üretim merkezi, ürünler üretebilir ve kod üreticinde 111 mamul ürünler için kodlar üretebilir.

Kod üretici 111, burada mamul ürünlerin her bir partisi için dinamik anahtar 219 olarak anılan yeni bir anahtar üretir. Dinamik anahtar 219 tercihen rastgele bir sayı gibi rastgele bir gizli koddur. Kod üretici, bir gizli anahtar 223 üretmek üzere, bir parti için dinamik
20 anahtarı 219 etkin statik anahtar 209 ile birlikte kullanır. Gizli anahtar 223, o partideki mamul ürünlerin üzerine işaretlenecek kodları (221) (örneğin, alfanümerik kodları) üretmek üzere her bir ürün için fiziksel anahtarlar ve bir benzersiz ürün tanımlayıcısı (UPI) ile birlikte kullanılan'dır. Bu uygulamada, her bir ürün için UPI, aynı üretim merkezi tarafından tek bir zaman dilimi içinde üretilen ürünleri ayırt etmek üzere üretim süresini artan bir sayaç
25 değeriyle birlikte tanımlayan üretim bilgilerini içerir.

Kod üretici, UPI'nin gizli anahtarla kombinasyonunda ve UPI'nin fiziksel anahtarla kombinasyonunda kriptografik bir özet fonksiyonu kullanır. Bu, ürün için burada "gürültü değerleri" olarak anılan dijital parmak izlerini oluşturur ve bu gürültü değerleri, işaretleyiciler
30 113 vasıtasıyla ürünlerin üzerine işaretlenen kodları 221 üretmek için kullanılır. Yaygın olarak kullanılan kriptografik özet fonksiyonlarına ek olarak, özet değerlerini veya gürültü değerlerini üretmek üzere sınırlayıcı olmadan yer değiştirme, ikame etme, tabloda ikame etme ve indeksleme dahil çeşitli teknikler mevcuttur.

Şekil 2, kod üretici 111 tarafından gerçekleştirilen gürültü değerleri üretme yöntemini gösterir. Sistem gürültü değerini 225 üretmek üzere, gizli anahtar ilk olarak etkin statik

anahtar 209, dinamik anahtar 219 ve UPI'den 221 türetilir. Dinamik anahtar 219 ve etkin statik anahtar 209 sadece doğrulama merkezi 114 ve kod üretici 111 tarafından bilinir. Adım 301'de, dinamik anahtar ve UPI, statik anahtarda bulunan tuz matrisinden gizli anahtarı, statik anahtarın içindeki seri hale getirilmiş koda göre çıkarmak için kullanılır. Gizli
5 anahtar 223 ve UPI 221 ardından, ürün için sistem gürültüsünü üretmek üzere adım 303'te özetlenir. Fiziksel gürültü değerini 227 üretmek üzere, fiziksel anahtar 207, adım 305'te UPI 221 ile özetlenir. Sistem gürültü değerini üretmek için kullanılan özet fonksiyonu, fiziksel gürültü değerini üretmek için kullanılan özet fonksiyonu ile aynı veya bundan farklı olabilir.

Şekil 3, buluşun birinci bir uygulamasına uygun olan, her bir ürün için güvenli bir tanımlayıcı
10 üretmek üzere sistem gürültü değerinin ve fiziksel gürültü değerinin kullanıldığı yöntemi gösterir. Adım 311'de, sistem gürültü değeri 225 ve UPI 221 birleştirilir. Adım 313'te birleştirilmiş sistem gürültü değeri ve UPI, birinci bir tanımlayıcıyı 241 üretmek için kod üretici gizleme anahtarı (CGOK) 231 ile şifrelenir. CGOK, kod üreticisine özgüdür ve kod üreticisine önceden yüklenmiştir. Birinci tanımlayıcı 241 ardından fiziksel gürültü değeri 227
15 ve bir kod üretici tanımlayıcısı 233 ile birleştirilir. Kod üretici tanımlayıcısı (CGID) 233, kimlik doğrulama sırasında CGOK'nin elde edilmesini sağlayacaktır. İlk tanımlayıcı, fiziksel gürültü değeri ve CGID'nin kombinasyonu ardından güvenli tanımlayıcıyı 251 üretmek için adım 317'de bir genel anahtar 235 kullanılarak şifrelenir. Genel anahtar 235, tüm üretim merkezleri için ortaktır ve doğrulama merkezi tarafından bilinen simetrik veya asimetrik bir
20 anahtar çiftinin parçası olabilir. Güvenli tanımlayıcı 251 ardından adım 319'da işaretleyici 113 tarafından ürünün üzerine işaretlenir.

Kod üretici 111 veya üretim merkezi 103, 105, 107, mamul ürünün üzerine işaretlenen kodların sayısını tutar. Buna ek olarak, kod üretici 111, her parti için dinamik anahtar 219 parti ile ilgili bilgilerle (gösterilmez) birlikte doğrulama merkezine 114 gönderir. Bu, güvenli
25 internet bağlantısı 119 aracılığıyla gerçekleştirilebilir. Parti ile ilgili bilgiler, çeşitli bilgi parçaları, örneğin sınırlayıcı olmadan marka, hedeflenen pazar veya hedeflenen varış yerini içerebilir. Dinamik anahtarların 219 doğrulama merkezine 114 gerçek zamanlı olarak gönderilmesine gerek yoktur ve doğrulama merkezine uygun herhangi bir zamanda, örneğin aylık olarak iletilebilirler. Doğrulama merkezine 114 gönderilen dinamik anahtarlar 219, doğrulama
30 merkezinde 114 bulunan veya doğrulama merkezinden erişilebilen bir veri tabanında (örneğin merkezi sunucuda 117) depolanır. Her parti için dinamik anahtar 219 tercihen, doğrulama merkezine 114 aynı anda gönderilen parti bilgileriyle birlikte depolanır.

Tercihen, etkin statik anahtar 209, belirli bir üretim merkezindeki 103, 105, 107 kod üretici 111 hizmet dışı bırakıldığında silinir. Bu, kötü niyetli bir kullanıcının uygun kayıt olmadan
35 etkin statik anahtara 209 erişmesini önler. Kod üreticinin 111 devre dışı bırakılması ve kod

üreticinin 111 ve üretim merkezinin izinsiz kullanımının önlenmesi için ek araçlar sağlanabilir.

Şekil 4, bir kullanıcı 601 Şekil 3'teki yöntemle uygun olarak işaretlenen münferit bir mamul ürünün kimliğini doğrulamak istediğinde doğrulama merkezi 114 ve kullanıcı 601 tarafından gerçekleştirilen adımları gösterir. Kullanıcı 601, ürün üzerindeki kodu 221 okur ve doğrulama merkezine 114 gönderir. Bu, Şekil 1'de gösterilir. Kullanıcı 601, kodu güvenli veya güvenli olmayan bir internet bağlantısı gibi uygun herhangi bir araçla doğrulama merkezine 114 gönderebilir.

Doğrulama merkezi, adım 321'de güvenli tanımlayıcıyı alır. Fiziksel gürültü değerini 227 ve birinci tanımlayıcıyı 241 ortaya çıkarmak üzere, güvenli tanımlayıcının şifresi, adım 323'te genel anahtar 235 (veya asimetrik anahtarlar kullanılıyorsa anahtar çiftindeki ilgili anahtar) kullanılarak çözülür. CGID de ortaya çıkarılır. Bir arama tablosu kullanılarak, CGOK 231 ardından CGID'den elde edilir. Ardından sistem gürültüsünü 225 ve UPI'yi 221 ortaya çıkarmak üzere birinci tanımlayıcının şifresi CGOK 231 kullanılarak adım 325'te çözülür. Bu bilgilerle, etkin statik anahtar 209 ve dinamik anahtar 219 ve yeni bir fiziksel anahtar ile birlikte, hem fiziksel gürültü değeri hem de sistem gürültü değeri, ürünün kimliğini doğrulamak için yeniden oluşturulabilir.

Fiziksel gürültü değerini yeniden oluşturmak üzere, kullanıcı 601 adım 327'de ürünün bir kısmının görüntüsünü aynı yolla ve orijinal fiziksel anahtarı 207 üretmek için kullanılanla aynı koşullar altında kaydederek yeni bir fiziksel anahtar elde etmek zorundadır. UPI ve yeni fiziksel anahtar ardından adım 329'da yeni bir fiziksel gürültü değeri üretmek için özetlenir. Adım 331'de, yeni fiziksel gürültü değeri, adım 323'te ortaya çıkarılan çıkarılmış fiziksel gürültü değeri ile karşılaştırılır. Yeni fiziksel gürültü değeri çıkarılan fiziksel gürültü değerine yeterince benziyorsa, bu durumda kimlik doğrulama işleminin bir kısmı tamamlanır. Yeni fiziksel gürültü değeri çıkarılan fiziksel gürültü değerine yeterince benzemiyorsa, bu durumda adım 339'da ürünün özgün olmadığı belirlenir.

Ürünün özgün kabul edilmesi için yeni fiziksel gürültü değerinin çıkarılan fiziksel gürültü değeri ile aynı olması gerekebilir. Ancak, ürünü özgün olarak kabul etmek için bir bağıntı puanı kullanarak ve bir eşik bağıntı puanı talep ederek yeni fiziksel gürültü değeri ile çıkarılan fiziksel gürültü değeri arasında bazı farklılıklara izin verilebilir. US2005/0257064, bir fiber ortamının ölçülmüş fiziksel niteliklerinden türetilen iki dijital imza arasındaki bağıntı derecesini veya benzerliği hesaplamak için uygun bir istatistiksel yöntemi açıklar.

Kullanıcının 601 veya doğrulama merkezinin 114 adım 329 ve 331'i gerçekleştirmesi mümkündür. Kullanıcıya 601 doğrulama merkezi tarafından UPI sağlanırsa, son kullanıcı,

fiziksel gürültü değeri temelinde ürünün kimliğini doğrulayabilir. Benzer şekilde, yeni fiziksel anahtar doğrulama merkezine 114 sağlanırsa, doğrulama merkezi, fiziksel gürültü değeri temelinde ürünün kimliğini doğrulayabilir.

- 5 Sistem gürültü değerini yeniden oluşturmak üzere, gizli anahtar, adım 333'te UPI ve CGID kullanılarak yeniden üretilmelidir. Doğrulama merkezi 114, dinamik anahtarı 219 ve etkin statik anahtarı 209 doğrulama merkezinde tutulan kayıtlardan alabilir. Gizli anahtar ardından UPI 221, dinamik anahtar 219 ve etkin statik anahtar 209 kullanılarak yeniden üretilebilir. Adım 335'te, UPI ve gizli anahtar özetlenerek yeni bir sistem gürültü değeri yeniden oluşturulur. Adım 337'de, yeni sistem gürültü değeri, adım 325'te çıkarılan sistem gürültü değeri ile karşılaştırılır. Yeni sistem gürültü değeri ve çıkarılan sistem gürültü değeri aynıysa, adım 339'da ürünün özgün olduğu belirlenebilir.

Bir uygulamada, bir ürünün özgün kabul edilmesi için hem fiziksel gürültü değeri hem de sistem gürültü değeri karşılaştırmaları gereklidir. Ancak, istenirse, bu denetimlerin sadece biri temelinde kimlik doğrulaması sağlanabilir.

- 15 Etkin statik anahtarlar tercihen ilgili üretim merkezlerinin bilgileriyle birlikte doğrulama merkezinde depolandığından, ürünün üretildiği üretim merkezi 103, 105, 107 elde edilen etkin statik anahtardan 209 belirlenebilir. Dinamik anahtarlar doğrulama merkezinde tercihen ilişkili parti bilgisiyle birlikte depolandığından, ürün için parti bilgisi, türetilen dinamik anahtardan 219 belirlenebilir. Böylece, doğrulama merkezi 114, kullanıcı 601 tarafından gönderilen koddan 221 münferit ürün hakkında çeşitli bilgi parçaları 603 türetebilir ve ürünün özgünlüğünü denetleyebilir. Ardından ürünün özgün olup olmadığına ilişkin bir gösterge içeren bilginin 603 tümü veya seçili kısımları kullanıcıya 601 gönderilebilir. Bu, Şekil 1'de gösterilir. Bilgi 603 tercihen orijinal kodun gönderildiği araçla kullanıcıya 601 gönderilir.

- 25 Şekil 5, buluşun ikinci bir uygulamasına uygun bir işaretleme yöntemini gösterir. Şekil 5'teki yöntemde, biri sistem gürültü değeri 225 temelinde ve diğeri fiziksel gürültü değeri 227 temelinde iki güvenli tanımlayıcı üretilir. Sistem gürültü değeri 225, adım 341'de UPI 221 ile birleştirilir. Sistem gürültü değeri ve fiziksel gürültü değerinin kombinasyonu ardından Şekil 3'teki birinci uygulamada olduğu gibi birinci tanımlayıcıyı 241 üretmek için adım 343'te CGOK 231 ile şifrelenir. Birinci tanımlayıcı 241 ardından adım 345'te CGID ile birleştirilir ve birinci bir güvenli tanımlayıcıyı 271 üretmek için adım 347'de genel anahtar 235 ile şifrelenir. Fiziksel gürültü değeri 227, ikinci bir tanımlayıcıyı 261 üretmek için adım 221'de UPI ile birleştirilir. İkinci tanımlayıcı, ikinci bir güvenli tanımlayıcıyı üretmek için adım 353'te genel anahtar 235 ile şifrelenir. Ürün, ardından adım 355'te birinci güvenli

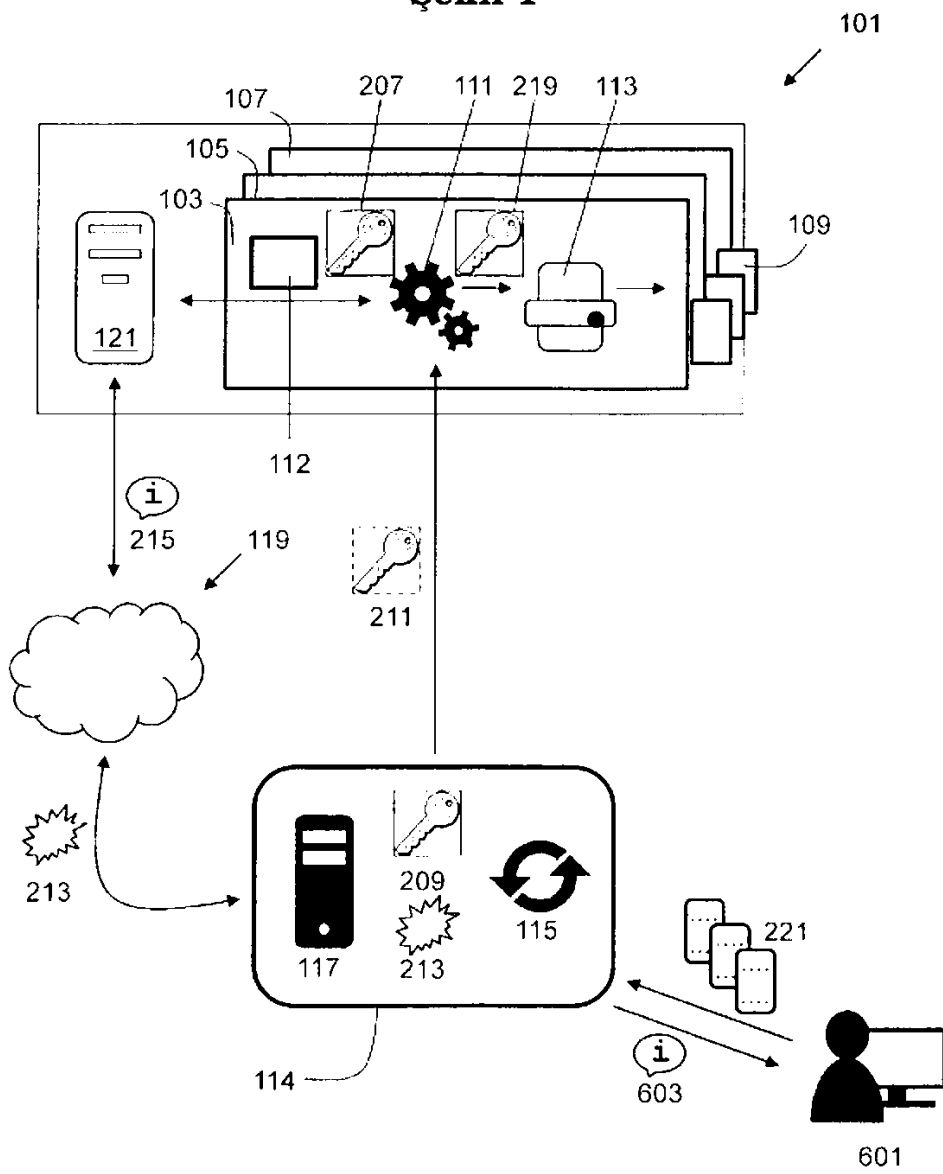
tanımlayıcı 271 ve ikinci güvenli tanımlayıcı 281 ile veya birinci güvenli tanımlayıcı 271 ve ikinci güvenli tanımlayıcının 281 kombinasyonundan elde edilen bir işaret veya işaretler ile işaretlenebilir.

5 Şekil 6, Şekil 5'te gösterilen yöntem kullanılarak işaretlenen bir ürünün kimliğini doğrulamak için gerçekleştirilen adımları gösterir. Adım 401'de, işaret veya işaretler kullanıcı tarafından okunur ve kullanıcı birinci güvenli tanımlayıcıyı 271 ve ikinci güvenli tanımlayıcıyı 281 üretir. Adım 403'te, genel anahtar 235, fiziksel gürültü değerini 227, UPI'nin 221 birinci kopyasını, birinci tanımlayıcıyı 241 ve CGID'yi 233 üretmek için kullanılır. Kullanıcının genel anahtarı 235 varsa, kullanıcı, ürünün kimliğini ikinci güvenli tanımlayıcı temelinde 10 çevrimdışı olarak, yani doğrulama merkezine bağlantıya gerek duyulmadan doğrulayabilir. Kullanıcı, adım 407'de yeni bir fiziksel anahtar üretir ve bu, adım 409'da yeni bir fiziksel gürültü değeri üretmek için UPI ile özetlenir. Kullanıcı, adım 411'de yeni fiziksel gürültü değerini adım 403'te çıkarılan fiziksel gürültü değeri ile karşılaştırabilir. Şekil 3'e atıfla 15 açıklandığı gibi, yeni fiziksel gürültü değerinin çıkarılan fiziksel gürültü değeriyle aynı ya da yeterince benzer olması durumunda, ürün adım 419'da özgün kabul edilebilir.

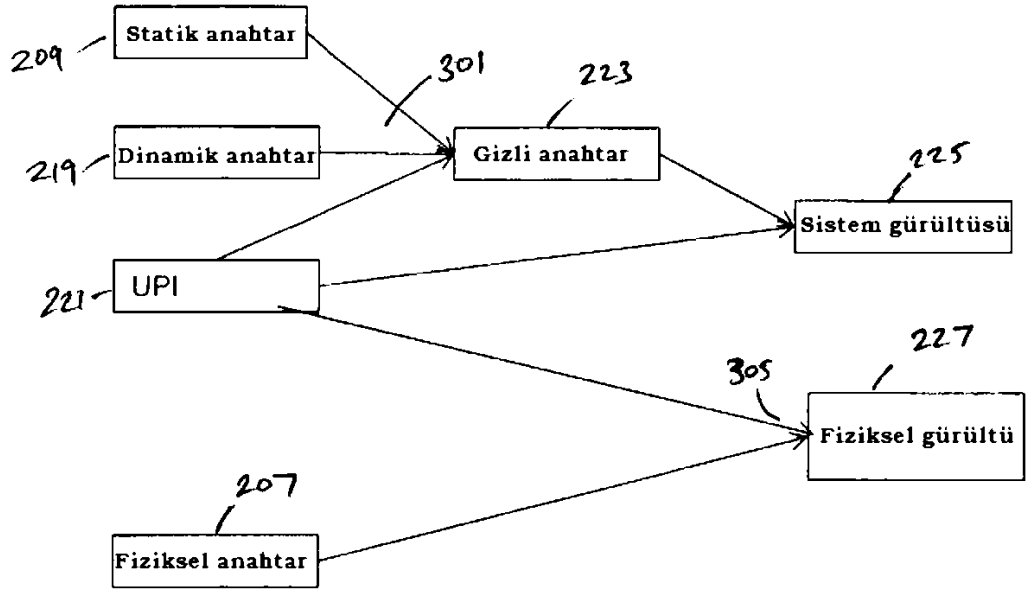
Adım 405'te, CGID, CGOK'yi 231 almak için doğrulama merkezi tarafından kullanılır ve CGOK, sistem gürültüsünü ve UPI'nin ikinci bir kopyasını ortaya çıkarmak üzere birinci tanımlayıcının 241 şifresini çözmek için kullanılır. Adım 408'de, UPI'nin ikinci kopyası ihtiyari olarak denetim amacıyla UPI'nin ikinci kopyası ile karşılaştırılabilir. Adım 423'te, 20 doğrulama merkezi 114, CGID ve UPI'yi kullanarak dinamik anahtarı 219 ve etkin statik anahtarı 209 alır. Adım 415'te, ilk olarak UPI, dinamik anahtar ve statik anahtardan bir gizli anahtarın yeniden üretilmesi ve ardından gizli anahtarın UPI ile özetlenmesi suretiyle yeni bir sistem gürültü değeri üretilir. Adım 417'de, yeni sistem gürültü değeri, adım 405'te çıkarılan sistem gürültü değeri ile karşılaştırılır. Aynı oldukları takdirde, ürünün kimliği adım 25 419'da doğrulanabilir. Şekil 3'teki uygulamada olduğu gibi, bir ürünün özgün kabul edilmesi için hem sistem gürültü değeri hem de fiziksel gürültü değeri temelinde kimlik doğrulaması gerekli olabilir.

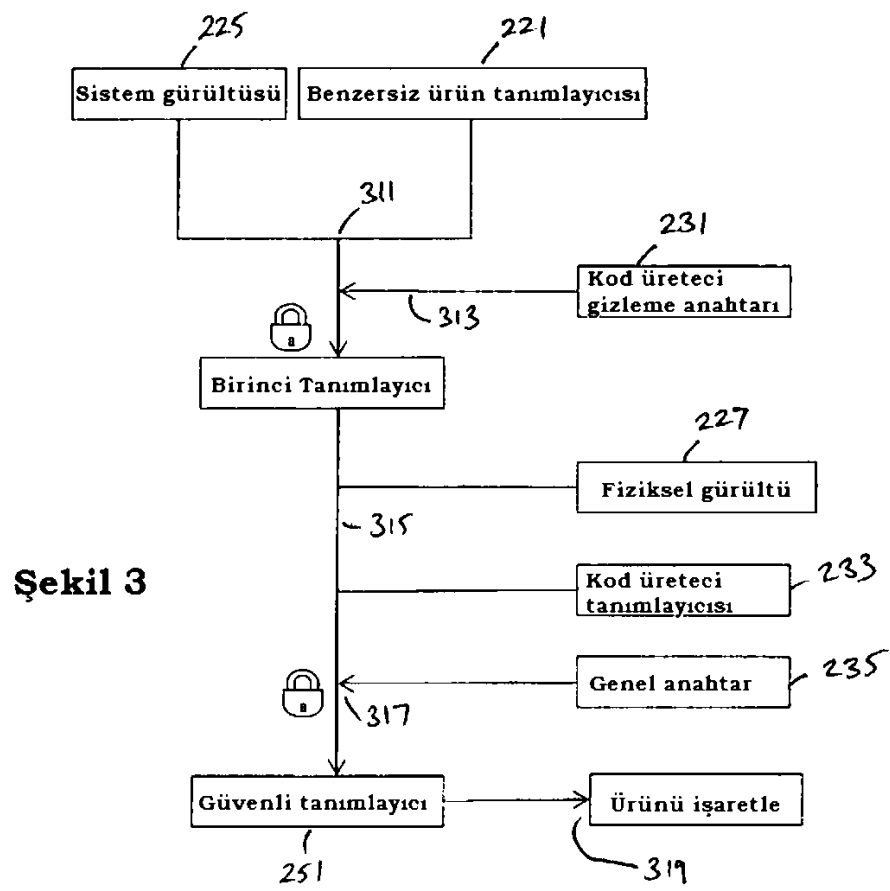
Buluş sigara üretimine atıfta bulunularak açıklanmış olmasına rağmen, buluşun ilaç, alkollü 30 içecekler ve lüks mallar gibi kimlik doğrulaması gerektiren her türlü ürüne uygulanabilir olduğu açık olmalıdır.

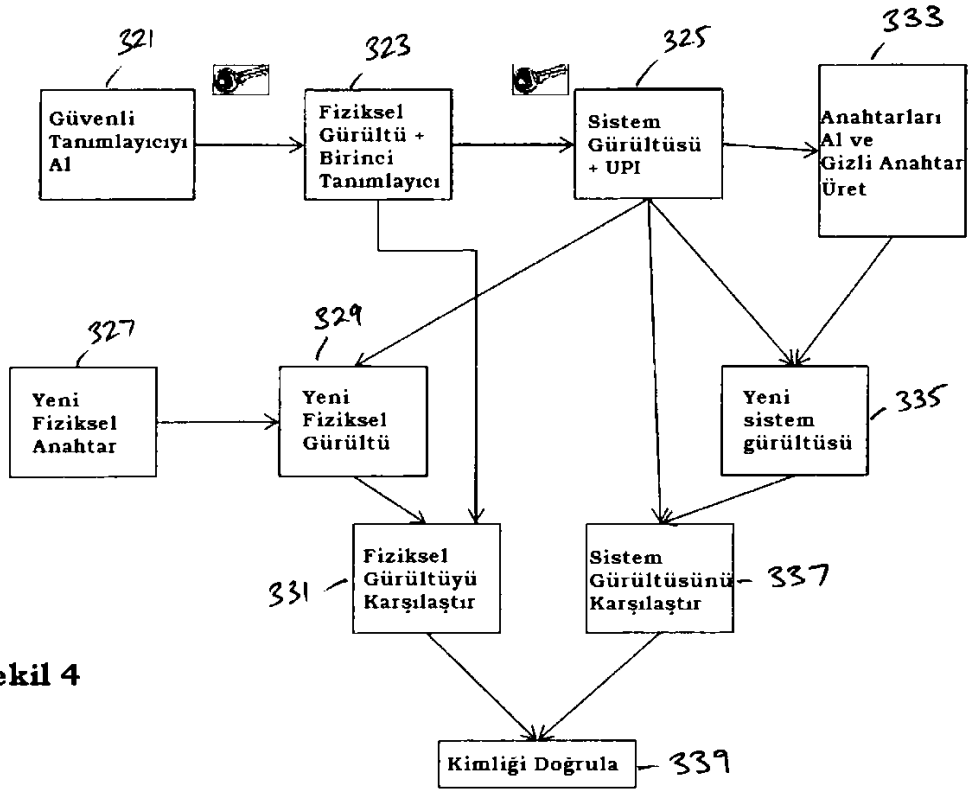
Şekil 1



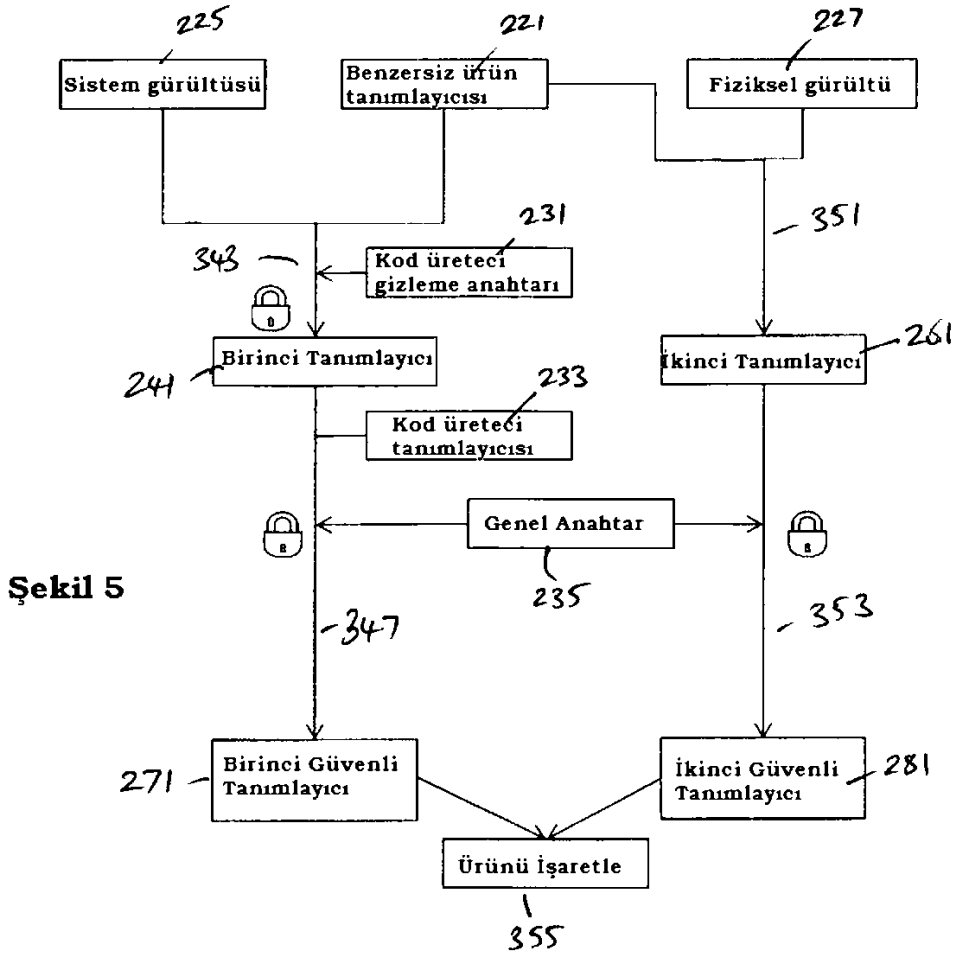
Şekil 2

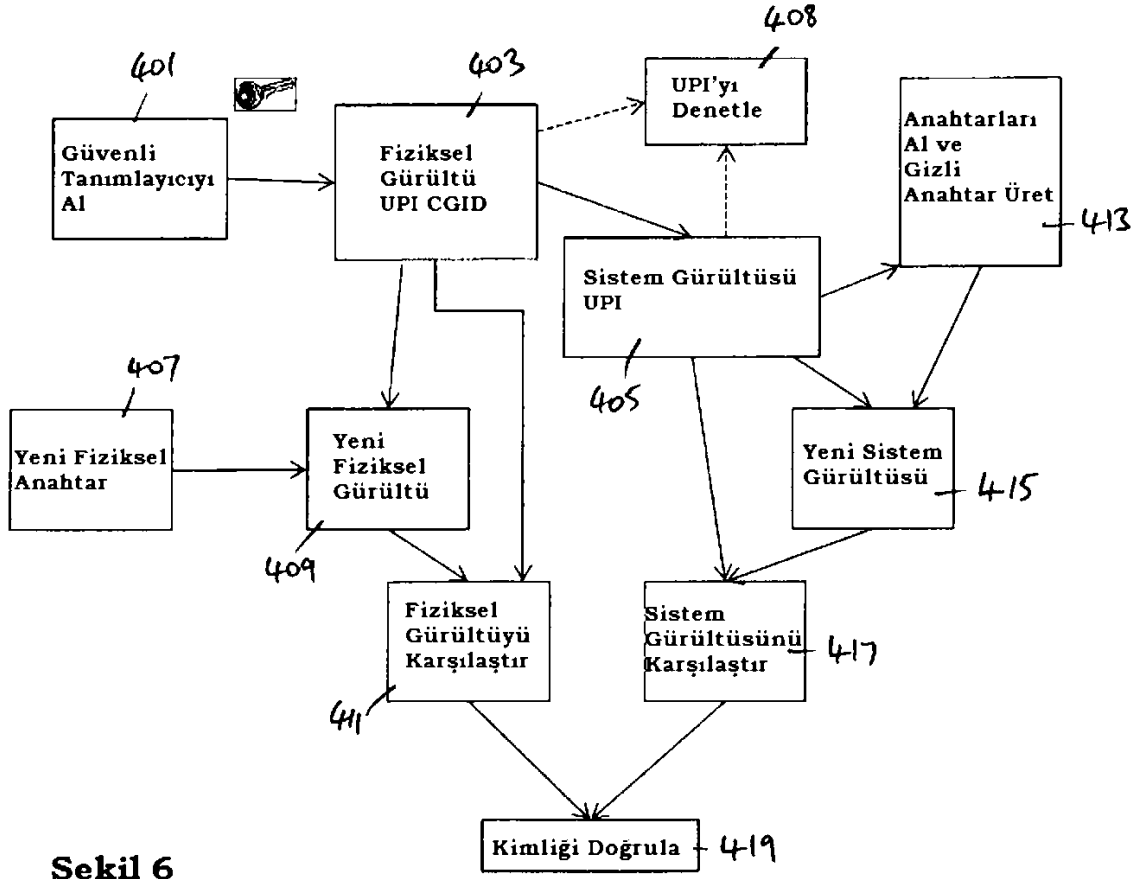






Şekil 4





Şekil 6