ÖZET

BİR MOBİL KİMLİK DOĞRULAMA UYGULAMASI KULLANARAK KULLANICIYA UYGUN KİMLİK DOĞRULAMA YÖNTEMİ VE APARATI

Uygulama etkileşimlerini sağlamak için yöntemler, aparatlar ve sistemler açıklanmaktadır. Uygulama etkileşimleri, bir kullanıcı kimlik doğrulama cihazında bir uygulama tanımlayıcıyı içeren bir kimlik doğrulama başlatma mesajı ile kodlanmış bir erişim cihazı tarafından yayılan bir sinyalin yakalanması, sinyal kodu çözme ve kimlik doğrulama başlatan mesajın alınması, uygulama tanımlayıcısının geri alınması, uygulama kimliğinin kullanıcıya yorumlanabilir bir şekilde sunulması, kimlik doğrulama sunucusunda kullanılabilen bir yanıt mesajı oluşturmak için kullanıcı onayının alınması, uygulama kimliğine kriptografik olarak bağlı bir kriptografik algoritma kullanarak dinamik bir güvenlik değeri oluşturulması ve oluşturulan dinamik güvenlik değerini içeren bir yanıt mesajının oluşturulması; yanıt mesajının bir doğrulama sunucusuna sunulması; ve doğrulama sunucusunda yanıt mesajının alınması, dinamik güvenlik değerinin geçerliliğinin doğrulanması ve yanıt mesajının doğrulamayı uygulamaya iletilmesi dahil olmak üzere yanıt mesajının doğrulanması ile güvence altına alınabilir.

İSTEMLER

1. Söz konusu uygulamayı barındıran bir uygulama sunucusuna (210) bağlanan bir erişim cihazı (230) aracılığıyla söz konusu uygulamaya uzaktan erişen bir kullanıcı (290) tarafından bir uygulama ile etkileşimin güvence altına alınması için bir yöntem (400) olup, aşağıdaki adımları içerir:

bir kullanıcı kimlik doğrulama cihazında (240) erişim cihazı tarafından yayılan bir sinyalin yakalanması (435), söz konusu sinyal bir kimlik doğrulama başlatma mesajı ile kodlanır, söz konusu kimlik doğrulama başlatma mesajı, uygulamanın bir kimliğine karşılık gelen en az bir uygulama tanımlayıcıyı içerir;

kullanıcı kimlik doğrulama cihazında (240) söz konusu sinyalin kodunun çözülmesi (435) ve kimlik doğrulama başlatma mesajının elde edilmesi;

kullanıcı kimlik doğrulama cihazında (240) kimlik doğrulama başlatma mesajından uygulama tanımlayıcısının geri alınması (440);

kullanıcı kimlik doğrulama cihazında (240) kriptografik dinamik güvenlik değeri oluşturma anahtarı ile parametrelenmiş bir birinci kriptografik algoritmayı kullanan ve belirli bir kullanıcı veya belirli bir kullanıcı kimlik doğrulaması ile ilişkili en az bir kişiselleştirilmiş veri elemanını kullanan bir dinamik güvenlik değeri oluşturulması (449);

kullanıcı kimlik doğrulama cihazında (240) en azından üretilen dinamik güvenlik değerini içeren bir yanıt mesajının oluşturulması (450);

yöntemin (400), **özelliği** ayrıca aşağıdaki adımları içermesi ile karakterize edilmesidir:

kullanıcı kimlik doğrulama cihazında (240), uygulama kimliğinin bir insan tarafından yorumlanabilir temsilini elde etmek için kimlik doğrulama başlatma mesajından geri alınan uygulama kimlik tanımlayıcısının kullanılması ve kullanıcı kimlik doğrulama cihazının (240) bir kullanıcı çıktı arayüzünü (340) kullanarak kullanıcıya (290) elde edilen uygulama kimlik temsilinin sunulması (442);

kullanıcı kimlik doğrulama cihazında (240), kullanıcıya sunulan uygulama kimliğine kriptografik olarak bağlı olduğu şekilde dinamik güvenlik değerinin oluşturulması;

kullanıcı kimlik doğrulama cihazında (240) kullanıcı kimlik doğrulama cihazının (240) bir kullanıcı giriş arayüzünün (350) kullanılmasıyla, bir yanıt mesajı

üretmek ve oluşturulan yanıt mesajını söz konusu doğrulama sunucusuna (220) temin etmek için bir onayın kullanıcıdan alınması (445);
söz konusu doğrulama sunucusuna (220) temin edilen oluşturulan yanıt mesajının üretilmesi (460);
doğrulama sunucusunda (220) yanıt mesajının alınması;
dinamik güvenlik değerinin geçerliliğini doğrulaması (475) dahil olmak üzere yanıt mesajının doğrulanması (470);
yanıt mesajının uygulamaya doğrulanması sonucunun iletilmesi (480).

2. İstem 1'e göre yöntem olup, özelliği yanıt mesajının ayrıca, kullanıcının bir kimliğinin veya kullanıcı kimlik doğrulama cihazının bir kimliğinin göstergesi olan bir veri elemanı içermesidir ve burada söz konusu veri elemanı, kullanıcı kimliğinin göstergesidir veya kullanıcı kimlik doğrulama cihazı kimliği bir kullanıcı kimliğini belirlemek için kullanılır ve burada söz konusu kullanıcı kimliği aynı zamanda uygulamaya iletilir.

3. İstem 2'ye göre yöntem olup, özelliği kullanıcı kimliğinin, ayrıca uygulama kimliğinin bir fonksiyonu olarak belirlenmesidir.

4. İstem 1'e göre yöntem olup, özelliği, uygulama kimliği temsilini elde etmek için kullanılan tüm uygulamaya bağımlı verilerin, kullanıcı kimlik doğrulama cihazı tarafından, kullanıcı kimlik doğrulama cihazına harici bir kaynaktan veya kimlik doğrulama başlatma mesajından elde edilmesidir.

5. Önceki istemlerden herhangi birine göre yöntem olup, özelliği ayrıca aşağıdaki adımları içermesidir:
kimlik doğrulama başlatan mesaja dahil edilecek bir sunucu kimlik bilgisinin üretilmesi (422), söz konusu üretme bir kriptografik sunucu kimlik bilgisi oluşturma anahtarı ile parametrelenmiş ikinci bir kriptografik algoritması kullanılarak yapılır;
kullanıcı kimlik doğrulama cihazında kimlik doğrulama başlatma mesajından alınan sunucu kimlik bilgisini alması;
kullanıcı kimlik doğrulama cihazında kriptografik sunucu kimlik doğrulama doğrulama anahtarı ile parametrelenmiş üçüncü bir kriptografik algoritma kullanarak sunucu kimlik doğrulamasını doğrulaması (441).

6. İstem 5'e göre yöntem olup, özelliği kimlik doğrulama başlatma mesajında yer alan uygulama tanımlayıcısının, kriptografik olarak sunucu bilgisine bağlanmasıdır.

7. Önceki istemlerden herhangi birine göre yöntem olup, özelliği bir yanıt mesajının üretilmesi adımının ayrıca aşağıdakileri içermesidir:
kullanıcı kimlik doğrulama cihazında kullanıcı kimlik doğrulama cihazının oluşturduğu yanıt mesajında kullanıcı için sunulan uygulama kimlik temsilini gösteren bir veri elemanını içermesi.

8. İstem 7'ye göre yöntem olup, özelliği ayrıca aşağıdakileri içermesidir:
doğrulama sunucusunda, kullanıcıya sunulan uygulama kimliği temsilinin göstergesi olan veri elemanının, doğrulama başlatma mesajında yer alan uygulama tanımlayıcısı tarafından belirtilen uygulama kimliği ile tutarlı olup olmadığının doğrulanması.

9. Önceki istemlerden herhangi birine göre yöntem olup, özelliği ayrıca aşağıdaki adımları içermesidir:
kullanıcı kimlik doğrulama cihazında kimlik doğrulama başlatma mesajında yer alan kimlik doğrulama başlatma mesaj işlemiyle ilgili verilerin geri alınması;
kullanıcı kimlik doğrulama cihazında, kullanıcı kimlik doğrulama cihazının bir kullanıcı çıkış arayüzü kullanılarak alınan işlemle ilgili verilerin sunulması (443); ve
burada üretilen dinamik güvenlik değeri, işlemle ilgili verilere kriptografik olarak bağlıdır.

10. İstem 9'a göre yöntem olup, özelliği, ayrıca aşağıdaki adımları içermesidir:
kimlik doğrulama başlatma mesajına dahil edilecek bir sunucu kimlik bilgisinin üretilmesi (422), söz konusu üretme bir kriptografik sunucu kimlik bilgisi oluşturma anahtarı ile parametrelenmiş ikinci bir kriptografik algoritması kullanılarak yapılır;
kullanıcı kimlik doğrulama cihazında kimlik doğrulama başlatma mesajından alınan sunucu kimlik bilgisini geri alınması;

kullanıcı kimlik doğrulama cihazında kriptografik sunucu kimlik doğrulama doğrulama anahtarı ile parametrelenmiş üçüncü bir kriptografik algoritması kullanılarak sunucu kimlik bilgisinin doğrulanması (441);
burada sunucu kimlik bilgisi, işlemle ilgili verilere kriptografik olarak bağlıdır.

11. İstem 9 veya 10'a göre yöntem olup, özelliği ayrıca aşağıdaki adımları içermesidir:
kullanıcı kimlik doğrulama cihazında kullanıcıya sunulan işlemle ilgili verilerin göstergesi olan kullanıcı kimlik doğrulama cihazı veri elemanları tarafından oluşturulan yanıt mesajını içermesi; ve
doğrulama sunucusunda, kullanıcıya sunulan işlemle ilgili verilerin göstergesi olan veri elemanlarının, doğrulama başlatma mesajında yer alan işlemle ilgili veriler ile tutarlı olup olmadığının doğrulanması.

12. Önceki istemlerden herhangi birine ait yöntem olup, özelliği
dinamik güvenlik değeri oluşturma anahtarının, bir gizli kişiselleştirilmiş anahtar içermesidir; ve burada
kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değeri oluşturma anahtarını en az bir dinamik giriş değeri ile kriptografik olarak birleştirerek dinamik güvenlik değerini hesaplar; ve burada
söz konusu dinamik girdi değeri, kullanıcı kimlik doğrulama cihazında bir zaman mekanizması tarafından sağlanan zamanla ilgili bir değerden en az birini, kullanıcı kimlik doğrulama cihazı tarafından depolanan ve muhafaza edilen sayaçla-ilişkili bir değeri veya kimlik doğrulama başlatma mesajında yer alan bir kimlik sormayı içerir.

13. İstem 12'ye göre yöntem olup, özelliği kullanıcı kimlik doğrulama cihazının, dinamik güvenlik değeri oluşturma anahtarını, kullanıcıya sunulan uygulama kimliği temsilini gösteren bir veri elemanı ile ayrıca kriptografik olarak birleştirerek dinamik güvenlik değerini hesaplamasıdır.

14. Kimlik doğrulama bilgilerinin üretilmesi için bir aparat (240) olup, aşağıdakileri içerir:
verilerin işlenmesi için uyarlanmış bir işlem bileşeni (310);
veri depolamak için bir depolama bileşeni (320);

bir kullanıcı için çıktıları ve kullanıcı tarafından girdi almak için bir girdi kullanıcı arayüzü (350) sunmak için bir birinci kullanıcı çıkış arayüzünü (340) içeren bir kullanıcı arayüzü (340, 350) bileşeni; ve

kullanıcının bir bilgisayar ağı üzerinden bir uygulamaya uzaktan erişim için kullandığı bir erişim cihazının (230) bir ikinci kullanıcı çıkış arayüzü tarafından yayılan bir sinyali yakalamak için uyarlanmış bir veri giriş arayüzü (360, 370), söz konusu sinyal bir kimlik doğrulama başlatma mesajı ile kodlanır, söz konusu uygulamanın bir kimliğine karşılık gelen en az bir uygulama tanımlayıcısını içeren kimlik doğrulama başlatma mesajı; burada aparat (240), söz konusu sinyalin kodunu çözmek ve kimlik doğrulama başlatan mesajı almak üzere uyarlanır;

kimlik doğrulama başlatma mesajından uygulama tanımlayıcısının geri alınması;

kriptografik dinamik güvenlik değeri oluşturma anahtarı ile parametrelenmiş bir birinci kriptografik algoritma kullanarak ve kullanıcı veya aparatın ilişkili en az bir kişiselleştirilmiş veri elemanını kullanarak bir dinamik güvenlik değerinin üretilmesi; ve

en azından üretilen dinamik güvenlik değerini içeren bir yanıt mesajının üretilmesi;

aparatın (240) **özelliği** ayrıca aşağıdakileri gerçekleştirmek üzere uyarlanması ile karakterize edilmesidir:

uygulama kimliğinin bir insan tarafından yorumlanabilir temsilini elde etmek için kimlik doğrulama başlatma mesajından alınan uygulama tanımlayıcısının kullanılması ve elde edilen uygulama kimlik temsilinin birinci kullanıcı çıkış arayüzünü kullanarak kullanıcıya sunulması;

dinamik güvenlik değerinin, kullanıcıya sunulan uygulama kimliğine kriptografik olarak bağlı olacak şekilde üretilmesi; ve

kullanıcı giriş arayüzünü kullanarak, bir yanıt mesajını oluşturmak ve bir doğrulama sunucusuna yanıt mesajını vermek için bir onay almak suretiyle kullanıcıdan elde edilmesi.

15. İstem 14'e göre aparat (240) olup, özelliği ayrıca üretilen yanıt mesajını, kullanıcıya birinci kullanıcı çıkış arayüzünü (340) kullanarak sunmak için uyarlanmasıdır.

16. İstem 14'e göre aparat (240) olup, özelliği ayrıca söz konusu yanıt mesajını bir doğrulama sunucusuna (220) iletmek için uyarlanmış bir veri iletişim arayüzü (330) içermesidir.

17. Söz konusu uygulamayı barındıran bir uygulama sunucusuna (210) bağlanan bir erişim cihazı (230) aracılığıyla söz konusu uygulamaya uzaktan erişim sağlayan bir kullanıcı tarafından bir uygulama ile etkileşimi sağlamak için bir sistem (200) olup, özelliği aşağıdakileri içermesidir:
istem 14'te talep edilen çok sayıda kullanıcı kimlik doğrulama cihazı (240); ve
çok sayıda kullanıcı kimlik doğrulama cihazının (240) herhangi biri tarafından üretilen bir yanıt mesajını almak üzere uyarlanmış ve yanıt mesajında yer alan dinamik güvenlik değerinin geçerliliğini doğrulamak üzere alınan yanıt mesajını doğrulamak için uyarlanmış ve yanıt mesajının doğrulanması sonucunu uygulamaya iletmek için uyarlanmış bir doğrulama sunucusu (220).

TARİFNAME
BİR MOBİL KİMLİK DOĞRULAMA UYGULAMASI KULLANARAK KULLANICIYA UYGUN KİMLİK DOĞRULAMA YÖNTEMİ VE APARATI

Buluşun Sahası

Buluş, bilgisayarlara ve uygulamalara uzaktan erişimin ve bilgisayar ağları üzerinden uzak işlemlerin güvenliğinin sağlanması ile ilgilidir. Daha spesifik olarak, buluş, kullanıcıları uzak uygulama sunucularına doğrulamak için yöntemler ve aparat ile ilgilidir.

Buluşun Alt Yapısı

Bilgisayar sistemlerine ve uygulamalarına uzaktan erişim yaygınlaştıkça, İnternet gibi ortak ağlar üzerinden uzaktan erişilen işlemlerin sayısı ve çeşitliliği önemli ölçüde artmıştır. Bu popülerlik, güvenlik ihtiyacını ortaya çıkarmıştır; özellikle: bir uygulamaya uzaktan erişen kişilerin iddia ettikleri kişi olduklarından emin olunması, uzaktan yapılan işlemlerin meşru şahıslar tarafından yapıldığıdan emin olunması ve bir uygulama sunucusu tarafından alınmadan önce işlem verilerinin değiştirilmediğinden emin olunması.

Geçmişte, uygulama sağlayıcıları uzak uygulamalar için güvenliği sağlamak üzere statik şifrelere güvenmişlerdir. Son yıllarda, statik şifrelerin yeterli olmadığı ve daha gelişmiş güvenlik teknolojisinin gerekli olduğu ortaya çıkmıştır.

Statik şifrelerden çok daha yüksek bir güvenlik seviyesi sunan bir kimlik doğrulama teknolojisi, 'güçlü kimlik doğrulama belirteç cihazları' tarafından sunulmaktadır. Güçlü kimlik doğrulama belirteçlerinin tipik örnekleri, Chicago, Illinois'den Vasco Data Security Inc. tarafından ticari olarak satılan DIGIPASS® hattının ürünleridir (http://www.vasco.com web sitesine bakınız). Güçlü bir kimlik doğrulama belirteci, kendi ekranı ve tuş takımı ile ve genellikle cep boyutunda kimlik doğrulama ve/veya işlem imza işlevleri sağlamaya adanmış, bağımsız bir akülü cihazdır. Bazı durumlarda tuş takımı tek bir düğmeye indirgenir veya tamamen iptal edilir, diğer durumlarda tuş takımı tam bir klavye olabilir. Tipik bir güçlü kimlik doğrulama belirtecinin ekranı ve tuş takımı, çıkarılamaz ve kullanıcı tarafından müdahale edilemez, tam olarak belirteç

tarafından kontrol edilebilir ve bir ana bilgisayardaki kötü amaçlı yazılım tarafından müdahaleye karşı duyarsızdır. Bu nedenle, güçlü kimlik doğrulama belirteçlerinin, örneğin her zaman virüs veya Truva gibi kötü amaçlı yazılımların kullanıcıya sahte mesajlar sunabilme veya kullanıcının girdiği her şeyi yakalama veya tuş takımı veya bir güvenlik uygulamasıyla ilişkili belleğe duyarlı veriyi okuduğu veya imzalanmadan önce verileri değiştirme olasılığın olduğu PC'lerin aksine güvenilir bir kullanıcı arayüzü olduğu kabul edilir. Güçlü bir kimlik doğrulama belirtecinin temel amacı, genellikle 'Tek Kullanımlık Şifreler' (OTP'ler) veya dinamik şifreler olarak adlandırılan dinamik güvenlik değerleri oluşturmaktır. Tipik olarak, bu OTP'ler, belirteç ile bir doğrulama veya kimlik doğrulama sunucusu arasında paylaşılan bir dinamik değer örneğin zaman değeri, bir sayaç değeri veya belirteç için sağlanan bir sunucu kimlik sorma veya bunların kombinasyonuna sahip bir parolayı kriptografik olarak birleştirerek oluşturulur. Bazı güçlü kimlik doğrulama belirteçleri, belirtece dinamik değer olarak sağlanan verileri (örneğin işlem verileri gibi) veya bir güvenlik değeri oluşturmak için yukarıda söz konusu dinamik değerlerden herhangi biriyle birlikte kullanabilir. Bu durumlarda ortaya çıkan güvenlik değeri, kullanıcının verileri onayladığını ve güvenlik değerinin genellikle elektronik imza veya Mesaj Kimlik Doğrulama Kodu (MAC) olarak adlandırıldığını gösterir. Bazı durumlarda, parolanın dinamik bir değerle kriptografik olarak birleştirilmesi, dinamik değere ilişkin veriler üzerinde bir simetrik şifreleme veya şifre çözme algoritmasının (örneğin, DES, 3DES veya AES) gerçekleştirilmesini ve parolanın bir simetrik şifreleme veya şifre çözme anahtarı olarak kullanılmasını içerir. Bazı durumlarda parolayı dinamik bir değerle kriptografik olarak birleştirmek (örneğin SHA-1 gibi), parola ile anahtarlı bir kriptografik sağlama işlevinin gerçekleştirilmesini ve sağlama işlevine girdi verisi olarak dinamik değer ile ilgili verilerin kullanılmasını içerir. Bazı güçlü kimlik doğrulama belirteçleri, ekranlı bir cihazdan ve ekli bir akıllı kart ile iletişim kurabilen bir tuş takımından oluşur; bu sayede OTP'ler veya MAC'lerin üretimi kısmen cihazın kendisi tarafından ve kısmen de ekli akıllı kart ile gerçekleştirilir.

Güçlü bir kimlik doğrulama belirtecine veri sağlamanın tipik bir yolu, kullanıcının verileri belirtecin tuş takımı üzerinden elle girmesine izin vermektir. Bu şekilde girilmesi gereken veri miktarı birkaç düzine karakteri aştığında, bu işlem kullanıcılar tarafından çok hantal olarak algılanabilir.

Oluşturulan OTP'leri veya MAC'leri, kimlik doğrulama belirtecinden, bunları doğrulaması gereken sisteme sunmanın tipik bir yolu, oluşturulan OTP'yi veya MAC'yi

ekranında gösteren belirteç ve kullanıcının görüntülenen OTP'yi veya MAC'yi kendi PC'sine (veya başka bir internet erişim cihazına) kopyalamasını içerir, burada bu OTP veya MAC, OTP veya MAC'nin geçerliliğinin doğrulanabileceği uygulama veya kimlik doğrulama sunucusuna iletilir. Ancak bu aynı zamanda, kullanıcı tarafından uygunsuz olarak algılanabilecek bazı eylemler gerektirir.

Güçlü kimlik doğrulama belirteçleri, genellikle güçlü bir kimlik doğrulama belirteci ve bir doğrulama sunucusu arasında paylaşılan simetrik gizli anahtarlarını kullanarak OTP'leri veya MAC'leri oluşturmak için simetrik kriptografik mekanizmalara dayanır. Bu, tüm uygulama sunucularının daha sonra güvenlik riskleri oluşturma potansiyeline sahip belirteç gizli anahtarını paylaşması gerektiğinden, bir kullanıcının çeşitli uygulamalarla birlikte kendi belirtecini kullanmak isterse sorunlu olabilir.

Özel donanım güçlü kimlik doğrulama belirteçlerinin bir başka yönü, kaçınılmaz olarak sıfır olmayan bir minimum maliyete sahip olmalarıdır. Bu bazen kullanıcı başına maliyet kritik bir faktör olabileceğinden birtakım uygulamalara yönelik özel donanım güçlü kimlik doğrulama belirteçlerinin daha az çekici kılabilir.
W02009/101549 A2, güçlü kimlik doğrulama belirtecinin, kullanıcının bir uzak terminali tarafından erişilen servisler için kullanıcı kimlik bilgisi üreten bir mobil cihaz olduğu bir sistemi açıklamaktadır.

İhtiyaç duyulan şey, bir yandan güçlü kimlik doğrulama belirteçleriyle aynı seviyede güvenlik sağlayan, ancak diğer yandan kullanıcı için oldukça uygun bir maliyete sahip olan ve çeşitli uygulamalar veya uygulama sağlayıcıları ile kolaylıkla kullanılabilen bir doğrulama mekanizmasıdır.

Buluşun Açıklaması

Buluş, sırasıyla 1, 14 ve 17 sayılı istemlerde tanımlanmıştır. Belirli uygulamalar, bağımlı istemlerde belirtilmiştir.

Bu buluşun yönleri, bu uygulamalar, uygulamalar tarafından güvenilen ve belirteç parolasına erişimi olan bir üçüncü taraf kimlik doğrulama sunucusunda bu belirteç tarafından oluşturulan OTP'lerin ve MAC'lerin doğrulanmasına güvenebiliyorsa, örneğin buluş sahiplerinin, bu farklı uygulamaların hepsinin parolaları paylaşmasına ihtiyaç

duyulmadan, aynı güçlü kimlik doğrulama belirteci ile birkaç farklı uygulamanın güvence altına alınabileceği şeklinde buluş sahiplerinin fikirlerin bir kombinasyonuna dayanmaktadır.

Buluşun hangi yönlerini temel aldığına dair diğer bir fikir kimlik doğrulama işlemi, kullanıcı için OTP'leri veya MAC'leri oluşturan cihazın, bilgi işlem cihazlarıyla veri alışverişi için iletişim arayüzleri içermesi durumunda, kullanıcı için çok uygun hale getirilebilmesidir; bu iletişim arayüzlerinin, hedeflenen uygulamalara (örneğin, web tabanlı uygulamalar) ve örneğin kullanıcıların bu uygulama arayüzlerine yönelik sürücüleri kurması gibi karmaşık ve hata eğilimli teknik adımlarla meşgul olmalarını gerektirmeden kullanıcıların bu uygulamalara erişmek için kullanabileceği Kişisel Bilgisayarlar (PC'ler) veya dizüstü bilgisayarlar gibi tipik erişim cihazlarına göre her yerde bulunabilir olduğu varsayılabilir.

Buluşun yönlerini temel alındığı başka bir fikir de çözüm, kullanıcının yeni bir donanım yerine zaten sahip olduğu, örneğin bir mobil telefon gibi bir cihazı tekrar kullanmanın mümkün olması halinde, çok uygun maliyetli olabilmesidir.

Kimlik doğrulama cihazları

Buluşun bazı uygulamalarında çok sayıda kullanıcıdan her bir kullanıcısı bir kimlik doğrulama cihazı ile donatılmıştır. Bazı uygulamalarda kimlik doğrulama cihazı, özel bir güçlü kimlik doğrulama belirteci gibi özel bir donanım cihazıdır. Diğer uygulamalarda, kimlik doğrulama cihazı, örneğin, bir akıllı telefon veya bir kişisel dijital yardımcı (PDA) gibi, elle tutulan bir mobil elektronik müşteri cihazı içermektedir. Bazı uygulamalarda, el tipi mobil elektronik müşteri cihazı bir kimlik doğrulama yazılımı uygulaması ile donatılmıştır. Bazı uygulamalarda, kimlik doğrulama cihazı, aşağıda açıklandığı gibi, kimlik doğrulama cihazı dinamik güvenlik değerlerin üretilmesinde, doğrudan veya dolaylı olarak kullanabilir en az bir gizli değer ile kişiye özel hale getirilmiştir.

Dinamik güvenlik değerlerinin üretilmesi.

Bazı uygulamalarda, kimlik doğrulama cihazı dinamik güvenlik değerleri üretecek şekilde uyarlanmıştır. Bazı uygulamalarda, üretilen dinamik güvenlik değerleri, işlem verilerine bir zaman veya daha fazla dinamik şifre ve/veya kimlik sorma ve/veya

elektronik imzalara yanıtlar içerebilir. Bazı uygulamalarda, kimlik doğrulama cihazı kullanıcıya üretilen dinamik güvenlik değerlerini sunmak üzere uyarlanmıştır. Bazı uygulamalarda, dinamik güvenlik değerleri, en az bir dinamik değişken (örneğin bir zaman değeri ve/veya bir sayaç değeri ve/veya bir kimlik sorma ve/veya işlemle ilgili veriler veya bunların herhangi bir kombinasyonu) ile en az bir gizli değerinin (bir şifreleme anahtarı gibi) kriptografik olarak birleştirilmesiyle üretilir. Bazı uygulamalarda, kriptografik olarak birleştirme, bir kriptografik algoritmanın gerçekleştirilmesini içerir. Bazı uygulamalarda, kriptografik algoritma DES, 3DES veya AES gibi bir simetrik şifreleme veya şifre çözme algoritması içerebilir. Bazı uygulamalarda, kriptografik algoritma, SHA-1 gibi bir sağlama veya anahtarlı sağlama algoritması içerebilir.

Bazı uygulamalarda, kimlik doğrulama cihazı, bir dinamik güvenlik değeri üretirken bir uygulama tanımlayıcı veri elemanını, örneğin bir Uygulama Tanımlayıcısını kullanabilir. Bazı uygulamalarda, kimlik doğrulama cihazı, Uygulama Tanımlayıcıyısı en az bir gizli değeri ve en az bir dinamik değişken gibi bir başka dinamik veri ile dinamik bir güvenlik değeri oluşturmak için kriptografik olarak birleştirir.

PIN kullanımı.

Bazı uygulamalarda, kimlik doğrulama cihazı kullanıcı tarafından sağlanan bir PIN veya gizli değerini alacak şekilde uyarlanmıştır. Bazı uygulamalarda doğrulama cihazı, doğrulama için kullanıcı tarafından sağlanan ikinci bir güvenlik cihazına (örneğin bir akıllı kart gibi) bir PIN veya gizli değerinden geçmek üzere uyarlanmıştır. Bazı uygulamalarda, kimlik doğrulama cihazı, PIN değeri doğrulandıktan sonra, bu PIN değerinin herhangi bir formatındaki herhangi bir kopyasını belleğinden çıkarmak üzere uyarlanmıştır. Bazı uygulamalarda, kimlik doğrulama cihazı, PIN değeri doğrulandıktan sonra böyle bir PIN değerinin geçici olarak saklandığı bellek konumlarını aktif olarak silmek veya üzerine yazmak üzere uyarlanmıştır. Bazı uygulamalarda, kimlik doğrulama cihazı, kullanıcı tarafından temin edilmesi beklenen PIN veya şifre için doğru bir değerle matematiksel olarak ilişkili bir referans değeri depolar ve doğrulama cihazı, bir kullanıcı tarafından bu referans değere sağlanan bir PIN veya gizli değerini karşılaştırmak üzere uyarlanır. Bazı uygulamalarda, kimlik doğrulama cihazı, kullanıcı tarafından sağlanan bir PIN veya gizli değerini kullanarak gizli değeri üretecek şekilde uyarlanmıştır. Bazı uygulamalarda, kimlik doğrulama cihazı, kullanıcı tarafından sağlanan bir PIN veya gizli değerden türetilen bir şifreleme anahtarı ile şifrelenen gizli

değeri içeren bir değer depolar ve kimlik doğrulama cihazı bir PIN veya kullanıcı tarafından sağlanan gizli değerini bir şifreleme anahtarı değeri elde edecek şekilde uyarlanır ve şifrelenmiş gizli değerin şifresini çözmek için, örneğin dinamik bir güvenlik değeri oluşturmak için şifreleme anahtarının değerini kullanır.

İletişim arayüzleri

Bazı uygulamalarda doğrulama cihazı ağa bağlanabilir. Bazı uygulamalarda, doğrulama cihazı bir bilgisayar ağı üzerinden veri iletişimi için bir veri iletişim arayüzü içerebilir. Bazı uygulamalarda iletişim arayüzü, örneğin bir cep telefonu şebekesiyle iletişim kurmak için bir kablosuz iletişim arayüzünü içerebilir. Bazı uygulamalarda, kimlik doğrulama cihazı, bir bilgisayar ağı üzerinden bir sunucuya kimlik doğrulama ile ilgili verileri göndermek ve/veya almak üzere uyarlanabilir. Bazı uygulamalarda, kimlik doğrulama cihazı, internet üzerinden veri iletmek üzere uyarlanmıştır. Bazı uygulamalarda kimlik doğrulama cihazı bir TCP/IP (İletim Kontrol Protokolü/İnternet Protokolü) yığını içerir. Bazı uygulamalarda, kimlik doğrulama cihazı bir SSL (Güvenli Yuva Katmanı) ve/veya TLS (Aktarım Katmanı Güvenliği) bağlantısı üzerinden veri alışverişi için uyarlanmıştır. Bazı uygulamalarda, kimlik doğrulama cihazı HTTP (Hiper-Metin Aktarım Protokolü) ve/veya HTTPS (Güvenli Bağlantılı Metin Aktarım Protokolü) mesajlarını göndermek ve/veya almak üzere uyarlanmıştır.

Kimlik Doğrulama Başlatma Mesajı

Bazı uygulamalarda, kimlik doğrulama cihazı bir Kimlik Doğrulama Başlatma Mesajını alacak şekilde uyarlanabilir. Buluşun bir uygulamasında Kimlik Doğrulama Başlatma Mesajı, bir zorluğu (örneğin, doğrulama/doğrulama amaçları için işlenebilecek bir rastgele sayı veya işlem verisi sağlaması) içerebilir. Buluşun bir başka uygulamasında, Kimlik Doğrulama Başlatma Mesajı, işlem değerleri veya işlem içeriği bilgileri dahil işlemle ilgili verileri içerir. Bazı uygulamalarda işlem içeriği bilgileri, işlemle ilgili verilerin anlamına ilişkin işlem verileri etiketlerini ve/veya bilgilerini içerebilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, uygulama akışı ile ilgili bilgileri içerir. Bazı uygulamalarda, uygulama akışı ile ilgili bilgiler, işlemin türüne ilişkin bilgileri içerebilir. Bazı uygulamalarda, uygulama akışı ile ilgili bilgiler, kimlik doğrulama cihazının alınan işlemle ilgili verileri nasıl ele alacağı ve/veya kimlik doğrulama cihazının kullanıcı etkileşim akışını nasıl ele alması gerektiği örneğin hangi verilerin

sunulması gerektiği, kullanıcıya gözden geçirme ve/veya onay için ve kullanıcıya veriyi sorma veya verme veya el ile ilave veri sağlama ve/veya kullanıcıya hangi mesajların sunulması gerektiği gibi sorular sorulup sorulmayacağı ile ilgili olarak yönlendirebilir.

Bazı uygulamalarda, kimlik doğrulama cihazı optik bilginin alınması için optik bileşenler içerebilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kullanıcının erişim cihazı tarafından yayılan bir optik sinyal olarak (örneğin erişim cihazının ekranında görselleştirilen dinamik veya statik bir model olarak) kodlanabilir ve kullanıcının kimlik doğrulama cihazı tarafından alınabilir ve kodu çözülebilir. Bazı uygulamalarda, kimlik doğrulama cihazı bir kamera içerebilir ve Kimlik Doğrulama Başlatma Mesajı erişim cihazının ekranında bir veya daha fazla resim veya görsel olarak kodlanabilir ve kimlik doğrulama cihazının kamerası tarafından yakalanabilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kimlik doğrulama cihazının kamera ile okuduğu ve fiili Doğrulama Başlatma Mesajını elde etmek için kod çözdüğü bir QR Kodu (Hızlı Yanıt Kodu) olarak kodlanabilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, birden fazla QR Kodu kullanılarak kodlanabilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı bir URL formunu içerebilir veya alabilir.

Sunucu Kimlik Bilgisi

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, bir sunucu tarafından kriptografik olarak oluşturulmuş bir sunucu kimlik bilgisi içerebilir (örneğin bir uygulama sunucusu veya kimlik doğrulama sunucusu olabilir). Bazı uygulamalarda sunucu, kimlik doğrulama cihazıyla veya kimlik doğrulama cihazının iletişim kurduğu ikinci bir güvenlik cihazı ile paylaşılan bir simetrik şifreleme ve bir gizli anahtar kullanarak sunucu bilgisini üretmiştir. Bazı uygulamalarda kimlik doğrulama cihazı, sunucu kimlik bilgisini doğrulamak için uyarlanmıştır. Bazı uygulamalarda, kimlik doğrulama cihazı, ikinci bir güvenlik cihazı ile işbirliği içinde sunucu kimlik bilgisini doğrulamak üzere uyarlanmıştır. Bazı uygulamalarda, sunucu kimlik bilgilerinin doğrulanması, sunucuyla paylaşılan bir gizli anahtar kullanan simetrik bir şifreleme algoritması kullanılarak yapılır. Bazı uygulamalarda sunucu kimlik bilgisi, bir sunucu bir kerelik şifre içerir. Bazı uygulamalarda sunucu kimlik bilgisi bir veri imzası içerir. Bazı uygulamalarda sunucu kimlik bilgisi bir Mesaj Kimlik Doğrulama Kodu (MAC) içerir. Bazı uygulamalarda sunucu kimlik bilgisi, şifreli girdi verilerini içerir. Bazı uygulamalarda, sunucu kimlik bilgisinin amacı bir sunucu veya sunucu uygulamasını doğrulamaktır. Bazı

uygulamalarda, sunucu kimlik bilgisinin amacı, kimlik doğrulama cihazı tarafından bir sunucudan alınan girdi verilerini (Kimlik Doğrulama Başlatma Mesajında içerilen) doğrulamaktır. Bazı uygulamalarda, sunucu kimlik bilgisinin amacı, kimlik doğrulama cihazı tarafından bir sunucudan alınan girdi verilerinin bütünlüğünü (Kimlik Doğrulama Başlatma Mesajında yer alabilir) korumaktır. Bazı uygulamalarda, sunucu kimlik bilgisinin amacı, kimlik doğrulama cihazı tarafından bir sunucudan alınan girdi verilerinin (Kimlik Doğrulama Başlatma Mesajında içerilen) gizliliğini korumaktır. Bazı uygulamalarda, sunucu kimlik bilgisinin amacı, kimlik doğrulama cihazı tarafından bir sunucudan alınan girdi verilerini (Kimlik Doğrulama Başlatma Mesajında içerilen) kriptografik olarak bir araya getirmektir. Bazı uygulamalarda, kimlik doğrulama cihazı tarafından dinamik güvenlik değerlerinin oluşturulması, sunucu kimlik bilgisinin başarılı bir şekilde doğrulanmasına bağlı olabilir.

Kimlik Doğrulama Oturum Tanımlayıcısı

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kimlik doğrulama oturumunun, örneğin bir Kimlik Doğrulama Oturum Tanımlayıcısının tanımlanması için bir veri elemanı içerebilir. Bazı uygulamalarda bu türlü bir Kimlik Doğrulama Oturumu Tanımlayıcısı veya kısaca Oturum ID, bir sıra numarası içerebilir. Bazı uygulamalarda, Oturum ID rastgele oluşturulmuş bir sayı içerebilir. Bazı uygulamalarda, Oturum ID bir uygulama sunucusu tarafından oluşturulabilir. Bazı uygulamalarda, Oturum ID bir kimlik doğrulama sunucusu tarafından oluşturulabilir. Bazı uygulamalarda Oturum ID, bir Dinamik Güvenlik Değerinin üretilmesinde Kimlik Doğrulama Başlatma Mesajını alan bir Kimlik Doğrulama Cihazı tarafından kullanılabilir.

Uygulama Tanımlayıcısı

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, bir uygulamayı veya uygulama sağlayıcısını tanımlamak için bir veri elemanı içerebilir, örneğin Bir Uygulama Tanımlayıcısı. Bazı uygulamalarda Uygulama Tanımlayıcısı, kullanıcının kimlik doğrulama cihazının bir dinamik güvenlik değeri üretmesi gereken uygulama veya uygulama sağlayıcısını belirleyebilir. Bazı uygulamalarda, kimlik doğrulama cihazı, bir dinamik güvenlik değeri hesaplamasında Kimlik Doğrulama Başlatma Mesajında yer alan bir Uygulama Tanımlayıcısı ile ilgili bir değer kullanacak şekilde uyarlanmıştır. Bazı uygulamalarda Uygulama Tanımlayıcısı, kullanıcının uygulamayı

veya uygulama sağlayıcısını tanımlayabileceği uygulama veya uygulama sağlayıcısının bir temsilini içerir ve kimlik doğrulama cihazı kullanıcıya bu temsili sunacak şekilde uyarlanır. Bazı uygulamalarda Uygulama Tanımlayıcı, bir dijital veri elemanını içerir ve kimlik doğrulama cihazı, bu dijital veri elemanının, kullanıcının uygulamayı veya uygulama sağlayıcısını tanımladığı şekilde tanıtabileceği uygulama sağlayıcısı uygulamasının bir temsilini almak üzere uyarlanır ve kimlik doğrulama cihazı kullanıcıya temsili sağlamak için uyarlanmıştır. Bazı uygulamalarda temsil, bir isim veya bir logo içerebilir. Bazı uygulamalarda temsil, sesler (örneğin, kullanıcının uygulamayı veya uygulama sağlayıcısını tanımlamak için kullanabileceği bir ismin konuşulması veya bir kullanıcı tarafından uygulama veya uygulama sağlayıcısı ile ilişkilendirilebileceği bir müzikal kimlik tanıma tonu) içerebilir. Bazı uygulamalarda, kimlik doğrulama cihazı bir görüntü üzerinde görsel verileri görselleştirerek temsili sunabilir. Bazı uygulamalarda, kimlik doğrulama cihazı örneğin konuşma veya müzik içerebilen sesleri göndererek kullanıcıya temsili sunabilir.

Bazı uygulamalarda, kimlik doğrulama cihazı bir Kimlik Doğrulama Başlatma Mesajını aldıktan sonra dinamik bir güvenlik değeri üretecek şekilde uyarlanmıştır. Kimlik doğrulama cihazı ayrıca, Kimlik Doğrulama Başlatma Mesajından bir Uygulama Tanımlayıcısı çıkartmak ve kullanıcıya karşılık gelen uygulama veya uygulama sağlayıcı temsilini sunmak ve bu uygulama veya uygulama sağlayıcısı için dinamik bir güvenlik değeri oluşturup oluşturmayacağı hakkında kullanıcının onayını almak üzere ve kullanıcının onaylaması koşuluyla dinamik güvenlik değerini oluşturmak için uyarlanabilir.

Hedef Adres

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı bir Hedef Adres içerebilir. Bazı uygulamalarda Hedef Adres, kimlik doğrulama cihazının veri veya bir veya daha fazla mesaj gönderebileceği bir sunucunun bir ağ adresini içerebilir. Bazı uygulamalarda bu bir uygulama sunucusunun ağ adresi olabilir. Bazı uygulamalarda bu bir kimlik doğrulama sunucusunun ağ adresi olabilir. Bazı uygulamalarda Hedef Adres bir IP adresi içerebilir. Bazı uygulamalarda, Hedef Adres bir alan adı içerebilir. Bazı uygulamalarda Hedef Adres bir URL (Tekdüzen Kaynak Konum Belirleyici) veya URI (Tekdüzen Kaynak Tanımlayıcı) içerebilir. Bazı uygulamalarda Hedef Adres, kimlik

doğrulama cihazının üretilen bir dinamik güvenlik değerini gönderebileceği bir sunucunun bir hedef adresini içerebilir.

Yanıt Mesajı

Bazı uygulamalarda, kimlik doğrulama cihazı, bir dinamik güvenlik değeri üretildikten sonra bir Yanıt Mesajı üretecek şekilde uyarlanmıştır. Bazı uygulamalarda Yanıt Mesajı, dinamik güvenlik değerini içerebilir. Bazı uygulamalarda Yanıt Mesajı, dinamik güvenlik değerinin üretildiği uygulamayı veya uygulama sağlayıcısını tanımlayan bir veri elemanı içerebilir. Uygulama veya uygulama sağlayıcısını tanımlayan bu veri elemanı, örneğin kimlik doğrulama cihazı tarafından alınan Kimlik Doğrulama Başlatma Mesajında yer alan Uygulama Tanımlayıcıyı içerebilir. Bazı uygulamalarda Yanıt Mesajı, kimlik doğrulama cihazını (örneğin bir seri numarası) belirten bir veri elemanı içerebilir. Bazı uygulamalarda, Yanıt Mesajı, kullanıcıyı tanımlayan bir veri elemanını, örneğin bir kullanıcı adı veya bir kullanıcı ID (kullanıcı tanımlayıcı) içerebilir. Bazı uygulamalarda Yanıt Mesajı, dinamik güvenlik değerinin üretildiği oturumu tanımlayan bir veri elemanı içerebilir. Bu, örneğin kimlik doğrulama cihazı tarafından alınan Kimlik Doğrulama Başlatma Mesajında yer alan bir Oturum Id içerebilir.

Bazı uygulamalarda, kimlik doğrulama cihazı, bir Yanıt Mesajını bir sunucuya bir bilgisayar ağı üzerinden göndermek üzere uyarlanabilir. Bazı uygulamalarda kimlik doğrulama cihazı, internet üzerinden bir sunucuya Yanıt Mesajını göndermek üzere uyarlanabilir. Bazı uygulamalarda, kimlik doğrulama cihazı bir IP mesajındaki bir sunucuya Yanıt Mesajı gönderecek şekilde uyarlanabilir. Bazı uygulamalarda kimlik doğrulama cihazı, bir HTTP mesajında, örneğin bir HTTP POST mesajı içinde bir Yanıt Mesajının bir sunucuya gönderilmesi için uyarlanabilir. Bazı uygulamalarda, kimlik doğrulama cihazı, Yanıt Mesajını uygulama sunucusuna gönderebilir. Bazı uygulamalarda kimlik doğrulama cihazı, Yanıt Mesajını bir doğrulama sunucusuna gönderebilir. Bazı uygulamalarda, kimlik doğrulama cihazının Yanıt Mesajını göndermesi gereken sunucunun hedef adresi, kimlik doğrulama cihazında saklanabilir. Bazı uygulamalarda, kimlik doğrulama cihazı, Yanıt Mesajının hedef adresini almak için bir veri elemanını (örneğin doğrulama cihazı tarafından alınan Kimlik Doğrulama Başlatma Mesajında yer alan bir Uygulama Tanımlayıcısı gibi) tanımlayan bir veri elemanı kullanır. Bazı uygulamalarda, kimlik doğrulama cihazı, Yanıt Mesajı için hedef adresi almak üzere kimlik doğrulama cihazı tarafından alınan Kimlik Doğrulama

Başlatma Mesajında yer alan bir Hedef Adres kullanır. Bazı uygulamalarda, kimlik doğrulama cihazı hedef adresi alınırken bir filtre uygular. Bazı uygulamalarda, kimlik doğrulama cihazı izin verilen hedef adreslerinin beyaz listesini muhafaza eder ve alınan hedef adresi bu beyaz listeyle karşılaştırır ve alınan hedef adres bu beyaz listeyle eşleşmezse Yanıt Mesajının gönderilmesini reddeder. Örneğin bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, Yanıt Mesajını gönderecek sunucunun alan adını içerir ve doğrulama cihazı, alan adını, izin verilen alan adları listesine göre karşılaştırır.

Kimlik doğrulama sunucusu.

Bazı uygulamalarda, kimlik doğrulama cihazlarının gizli anahtarları bir kimlik doğrulama sunucusu ile paylaşılmaktadır. Bazı uygulamalarda kimlik doğrulama sunucusu, bir veya daha fazla yazılım uygulamasını çalıştıran bir veya daha fazla sunucu bilgisayarı içerebilir. Bazı uygulamalarda, kimlik doğrulama sunucusu, kimlik doğrulama cihazlarının gizli anahtarlarının (veya eş değerlerinin) değerlerini depolayan bir veri tabanını içerir. Bazı uygulamalarda kimlik doğrulama sunucusu bir veya daha fazla parola saklar. Bazı uygulamalarda, veri tabanında saklanan bir gizli değer, ilgili kimlik doğrulama cihazının bir tanımlama değerine (bir seri numarası gibi) bağlanır veya kimlik doğrulama cihazı ile ilişkili bir kullanıcının bir kimlik değerine (kullanıcı adı gibi) bağlanır. Bazı uygulamalarda, kimlik doğrulama sunucusu bir ana parola saklar ve kimlik doğrulama cihazının ana parolasını ve kimlik doğrulama cihazının bir kimlik değerini veya kimlik doğrulama cihazıyla ilişkili bir kullanıcıyı kullanarak bir kimlik doğrulama cihazının gizli değerini yeniden oluşturmak veya türetmek üzere uyarlanır. Bazı uygulamalarda, kimlik doğrulama sunucusu, kimlik doğrulama cihazları tarafından üretilen dinamik güvenlik değerlerini doğrulamak üzere uyarlanmıştır. Bazı uygulamalarda, kimlik doğrulama sunucusu, kimlik doğrulama cihazı ile ilişkili olan ve bu kimlik doğrulama cihazı ile oluşturulduğu varsayılan bir dinamik güvenlik değerini doğrulamak için bir gizli değer (yukarıda açıklandığı gibi yeniden depolanabilir veya yeniden üretilebilir) kullanır.

Bazı uygulamalarda kimlik doğrulama sunucusu, verileri depolamak için bir veya daha fazla veri tabanını içerebilir. Bazı uygulamalarda kimlik doğrulama sunucusu kullanıcı ile ilgili verileri kullanabilir ve/veya depolayabilir. Bazı uygulamalarda, kimlik doğrulama sunucusu kimlik doğrulama cihazı ile ilgili verileri kullanabilir ve/veya saklayabilir. Bazı uygulamalarda, kullanıcı veya kimlik doğrulama cihazı ile ilgili veriler bir veya daha

fazla gizli anahtar içerir. Bazı uygulamalarda, bu gizli anahtarlardan bir veya daha fazlası kullanıcının kimlik doğrulama cihazı ile paylaşılabilir.

Buluşun yine bir başka yönü, bir kullanıcı tarafından erişilen, bir kullanıcının PC'sinde veya dizüstü bilgisayarında bir bilgi işlem cihazı üzerinden, bilgisayar ağı üzerinden, örneğin, internet bir uygulama sunucusu ile haberleşerek, bir erişim cihazı vasıtasıyla erişilen, uzak sunucu tabanlı bir uygulamayı güvenlik altına almak için bir yöntemden oluşmaktadır. Yöntem, aşağıdaki adımları içerebilir.

- Bir kullanıcı için yukarıda açıklandığı gibi bir kimlik doğrulama cihazını kullanılabilir hale getirmek. Bazı uygulamalarda, bu, özel bir donanım kimlik doğrulama belirtecini içeren kimlik doğrulama cihazlarını dağıtmayı içerir. Bazı uygulamalarda bu, örneğin bir akıllı telefon veya bir kişisel dijital yardımcı (PDA) gibi elde tutulan bir mobil elektronik müşteri cihazında indirme ve kurulum için bir kimlik doğrulama yazılımı uygulamasının sunulmasını içerir. Bazı uygulamalarda, bu ayrıca kimlik doğrulama cihazının kişiselleştirme verileriyle kişiselleştirilmesini içerir. Bazı uygulamalarda kişiselleştirme verileri bir gizli değer içerebilir. Bazı uygulamalarda kişiselleştirme verileri, örneğin bir seri numarası gibi bir kimlik doğrulama cihazı tanımlama değeri içerebilir. Bazı uygulamalarda kişiselleştirme, kişiselleştirici verilerinin, kullanıcıya bir kullanıcıya dağıtılmadan önce bir donanım güçlü kimlik doğrulama belirtecine yüklenmesini içerir. Bazı uygulamalarda kişiselleştirme, kişiselleştirme mesajlarını kişiselleştirme sunucusu ile değiştiren kimlik doğrulama cihazını içerir.
- Bir kimlik doğrulama cihazını ve/veya kullanıcıyı bir kimlik doğrulama sunucusu ile kaydetmek.
- Bir veya daha fazla kullanıcı için bir uygulamayı etkinleştirmek.
- Kimlik Doğrulama Başlatma Mesajını, söz konusu kimlik doğrulama cihazına birleştirmek.

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, doğrulama sunucusu tarafından toplanır. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı uygulama sunucusu tarafından toplanır. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kısmen kimlik doğrulama sunucusu ve kısmen de uygulama sunucusu tarafından birleştirilmektedir. Kimlik Doğrulama Başlatma Mesajı örneğin

bir oturum tanımlayıcı ve/veya bir kimlik sorma ve/veya işlemle ilgili veri ve/veya işlem bağlamıyla ilgili veriler ve/veya bir uygulama tanımlayıcı içerebilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı bir sunucu kimlik bilgisi içerebilir. Sunucu kimlik bilgilerini almak için bir sunucu isteğe bağlı olarak bir sunucu kimlik bilgisi üretebilir. Bazı uygulamalarda bu sunucu uygulama sunucusu olabilir. Bazı uygulamalarda bu sunucu kimlik doğrulama sunucusu olabilir. Sunucu, bir gizli anahtar ve bir kriptografik algoritma kullanarak sunucu kimlik bilgisi oluşturabilir. Kriptografik algoritma, simetrik bir kriptografik algoritma olabilir. Bazı uygulamalarda, sunucu kimlik bilgisinin üretilmesi için gizli anahtar, kullanıcının kimlik doğrulama belirteci ile paylaşılabilir.

- Kimlik Doğrulama Başlatma Mesajını kullanıcının kimlik doğrulama cihazına iletmek.

Bazı uygulamalarda, bu, önce Kimlik Doğrulama Başlatma Mesajının kullanıcının erişim cihazına gönderilmesini içerir. Kullanıcının erişim cihazı, bir web tarayıcısı gibi bir bilgisayar uygulaması kullanıyor olabilir. Kimlik Doğrulama Başlatma Mesajı, sunucu tabanlı uygulamanın bilgi işlem cihazının tarayıcısına sunduğu bir veya daha fazla web sayfasına gömülebilir. Daha sonra kimlik doğrulama cihazı, kullanıcının erişim cihazından Kimlik Doğrulama Başlatma Mesajını alabilir. Bazı uygulamalarda, kullanıcının erişim cihazının ekranı, kimlik doğrulama cihazı tarafından alınan ve kodu çözülen bir Kimlik Doğrulama Başlatma Mesajını kodlayan bir optik sinyal yayar.

Bazı uygulamalarda, kullanıcının erişim cihazı Kimlik Doğrulama Başlatma Mesajını (bir URL biçiminde olabilir) kodlayan bir QR Kodu görüntüler ve kullanıcının kimlik doğrulama cihazı bu QR Kodunu okur ve şifresini çözer. Örneğin, kullanıcının kimlik doğrulama cihazı, uygun bir kimlik doğrulama uygulamasına sahip bir akıllı telefon içerebilir. Kullanıcı, QR Kodunu okumak için akıllı telefonun kamerasını kullanan kimlik doğrulama uygulamasını başlatır ve ardından QR Kodunu çözer.

Bazı uygulamalarda kimlik doğrulama cihazı, çok adımlı bir işlemde Kimlik Doğrulama Başlatma Mesajını alır. Örneğin, kimlik doğrulama cihazı, kimlik doğrulama cihazının bir sunucu ile iletişim kurmasını ve fiili Doğrulama Başlatma Mesajını talep etmesini sağlayan bilgiyi içeren (örneğin bir URL) bir birinci mesaj

alabilir. Örneğin, kullanıcının erişim cihazında görüntülenen uygulama sunucusunun web sayfası, örneğin kimlik doğrulama sunucusunda bulunan fiili Kimlik Doğrulama Başlatma Mesajını işaret eden bir URL'yi kodlayan bir QR Kodu görüntüleyebilir.

- Kullanıcıdan onay almak.

Bazı uygulamalarda, kimlik doğrulama cihazı, bir dinamik güvenlik değeri üretmeden ve/veya üretilen bir dinamik güvenlik değerini içeren bir Yanıt Mesajı göndermeden önce kullanıcının onayını almaya uyarlanabilir. Bazı uygulamalarda, kullanıcının onayının istenmesi durumunda, kullanıcıya uygulama veya uygulama sağlayıcısının bir temsili sağlayan kimlik doğrulama cihazı bulunur. Bu temsil, yukarıda açıklandığı gibi elde edilebilir ve sunulabilir. Bazı uygulamalarda, kullanıcının onayının istenmesi, Kimlik Doğrulama Başlatma Mesajında yer alan kullanıcı verilerini sunan kimlik doğrulama cihazını içerir. Bazı uygulamalarda bu, kullanıcıya işlemle ilgili verilerin sunulmasını içerebilir. Bazı uygulamalarda kullanıcı bir OK butonu kullanarak onayını gösterebilir. Bazı uygulamalarda kullanıcı, geçerli bir PIN veya şifre girerek onayını gösterebilir. Bazı uygulamalarda, kullanıcı onayını belirtmemişse, kimlik doğrulama cihazı bir dinamik güvenlik değeri üretmez. Bazı uygulamalarda, kimlik doğrulama cihazı, kullanıcı onayını belirtmemişse, bir sunucuya dinamik güvenlik değeri içeren bir Yanıt Mesajı göndermez.

- Dinamik güvenlik değeri oluşturmak.

Kimlik doğrulama cihazı, önceki paragraflarda açıklandığı gibi dinamik güvenlik değerini üretebilir. Bazı uygulamalarda kimlik doğrulama belirteci, bir dinamik güvenlik değeri oluşturmak için Kimlik Doğrulama Başlatma Mesajını işler. Bazı uygulamalarda dinamik güvenlik değeri, bir dinamik değişkenin bir gizli anahtar ile kriptografik olarak birleştirilmesiyle üretilir. Bazı uygulamalarda, kriptografik olarak birleştirme, simetrik bir kriptografik algoritmanın kullanılmasını içerir. Bazı uygulamalarda dinamik değişken bir kimlik doğrulama içerir. Bazı uygulamalarda dinamik değişken, işlemle ilgili verileri içerir. Bazı uygulamalarda dinamik değişken, zamana bağlı bir değer içerir. Bazı uygulamalarda dinamik değişken bir sayaç içerir. Bazı uygulamalarda dinamik değişken, sunucu tabanlı uygulamadan alınan Kimlik Doğrulama Başlatma Mesajında yer alan bir veri elemanını içerir. Bazı

uygulamalarda dinamik güvenlik değeri, sunucu tabanlı uygulama ile paylaşılan bir anahtar kullanılarak üretilir. Bazı uygulamalarda, girdi verileri bir sunucu kimlik bilgisi içerir ve kimlik doğrulama cihazı, dinamik güvenlik değerini üretmeden önce sunucu bilgisini doğrular. Bazı uygulamalarda, kimlik doğrulama cihazı, sunucu bilgisini doğrulamak için uygulama sunucusuyla paylaşılan bir gizli anahtar ile simetrik bir kriptografik algoritma kullanır. Bazı uygulamalarda, kimlik doğrulama cihazı, sunucu kimlik bilgilerinin doğrulanmasının başarılı olması koşuluyla dinamik güvenlik değerini üretir.

Bazı uygulamalarda, kimlik doğrulama cihazı, uygulamayı veya uygulama sağlayıcısını tanımlayan bir veri elemanını girdi olarak kullanılan bir kriptografik algoritma kullanarak dinamik güvenlik değerini üretebilir. Bazı uygulamalarda bu veri elemanı, Kimlik Doğrulama Başlatma Mesajında yer alan Uygulama Tanımlayıcıyı içerebilir.

– oluşturulan dinamik güvenlik değerini kimlik doğrulama sunucusuna iletmek.

Bazı uygulamalarda, kimlik doğrulama belirteci güvenli bir kullanıcı çıkış arayüzü içerir ve kullanıcıya dinamik güvenlik değerini vermek için bu güvenli kullanıcı çıkış arayüzünü kullanır. Bazı uygulamalarda, kullanıcı dinamik güvenlik değerini alır ve sunucu tabanlı uygulamaya ilişkin bir web sayfasında dinamik güvenlik değerine girer.

Bazı uygulamalarda kimlik doğrulama cihazı, dinamik güvenlik değerini içeren bir Yanıt Mesajı oluşturur ve bunu kimlik doğrulama sunucusuna gönderir. Bazı uygulamalarda, kimlik doğrulama cihazı, dinamik güvenlik değerini içeren bir Yanıt Mesajı oluşturur ve bunu uygulama sunucusuna gönderir ve uygulama sunucusu, Yanıt Mesajını veya bunun bir kısmını kimlik doğrulama sunucusuna iletir. Bazı uygulamalarda, Yanıt Mesajı, bir oturum tanımlayıcısı, bir uygulama tanımlayıcısı, bir kimlik doğrulama cihazı tanımlayıcısı, bir kullanıcı belirleyici veri elemanı ve/veya kullanıcı tarafından onaylanmış ve/veya dinamik güvenlik değerinin üretilmesinde, bir işlem veya işlem verileri veya zaman veya sayaç senkronizasyon verileri gibi kullanılabilecek diğer verileri içerebilir.

- Alınan dinamik güvenlik değerini doğrulamak. Bazı uygulamalarda kimlik doğrulama sunucusu, alınan dinamik güvenlik değerinin geçerliliğini doğrulayabilir. Kimlik doğrulama sunucusu, alınan dinamik güvenlik değerini bir kriptografik algoritma kullanarak doğrulayabilir. Bazı uygulamalarda, kimlik doğrulama sunucusu, alınan dinamik güvenlik değerini doğrulamak için bir referans dinamik değişkenini bir referans gizli anahtar ile kriptografik olarak birleştirir. Bazı uygulamalarda, kimlik doğrulama sunucusu bir referans güvenlik değeri üretir ve referans güvenlik değerini alınan dinamik güvenlik değeriyle karşılaştırır. Bazı uygulamalarda, kimlik doğrulama sunucusu bir referans dinamik değişkenini bir referans gizli anahtar ile kriptografik olarak birleştirerek referans güvenlik değerini hesaplar. Bazı uygulamalarda, kriptografik olarak birleştirme, simetrik bir kriptografik algoritmanın gerçekleştirilmesini içerir. Bazı uygulamalarda, gizli anahtar, kimlik doğrulama sunucusunun kimlik doğrulama cihazı ile paylaştığı bir gizli anahtar veya kullanıcının kimlik doğrulama cihazının, dinamik güvenlik değerini oluşturmak üzere işbirliği yaptığı çıkarılabilir bir ikinci güvenlik cihazı içerir.

- uygulama sağlayıcısını doğrulamak

Bazı uygulamalarda kimlik doğrulama cihazı kullanıcıya bir uygulama tanımlayıcısı sunar. Bazı uygulamalarda, kimlik doğrulama sunucusu, dinamik güvenlik değerinin doğrulanmasını talep eden uygulama sunucusunun, kullanıcıya sunulan uygulama tanımlayıcısı ile eşleşip eşleşmediğini doğrular. Bazı uygulamalarda, kimlik doğrulama cihazı, Yanıt Mesajında kullanıcıya sunulan uygulama tanımlayıcısını içerir ve kimlik doğrulama sunucusu, aldığı Yanıt Mesajındaki uygulama tanımlayıcısının, dinamik güvenlik değerinin doğrulanmasını talep eden uygulama sunucusuyla eşleşip eşleşmediğini doğrular.

Bazı uygulamalarda kimlik doğrulama cihazı kullanıcıya bir uygulama tanımlayıcısı sunar ve bu uygulama tanımlayıcısını dinamik güvenlik değerinin üretilmesinde kullanır. Bazı uygulamalarda, sunucu, dinamik güvenlik değerinin doğrulanmasında bir referans uygulama sağlayıcısı tanımlayıcısı kullanır, şöyle ki dinamik güvenlik değerinin üretilmesinde kimlik doğrulama cihazı tarafından kullanılan uygulama tanımlayıcısı, kimlik doğrulama sunucusu tarafından kullanılan tanımlayıcı referans uygulama sağlayıcısı ile eşleşmezse, bu doğrulama başarısız olur. Bazı

uygulamalarda, kimlik doğrulama sunucusu, referans uygulama sağlayıcısı tanımlayıcısını, doğrulanacak dinamik güvenlik değerini de içeren Yanıt Mesajından çıkarır. Bazı uygulamalarda, kimlik doğrulama sunucusu, sunucu tarafından dinamik güvenlik değerini doğruladığı uygulama sunucusu kimliğinin referans uygulama sağlayıcısı tanımlayıcı değerini çıkarır.

- Uygulama sunucusunu doğrulama sonucu hakkında bilgilendirmek.

Bazı uygulamalarda, dinamik güvenlik değerinin geçerliliğinin doğrulanması üzerine, kimlik doğrulama sunucusu, uygulama sunucusunu doğrulama sonucu hakkında bilgilendirebilir. Bu bilgilendirme, doğrulamanın başarılı olup olmadığını bildirmeyi içerebilir. Bu bilgilendirme, doğrulama işleminin başarısız olması durumunda, bir hata kodu (örneğin "kriptografik doğrulama başarısız", "bilinmeyen kimlik doğrulama cihazı", "bilinmeyen oturum id", "kullanıcı hesabı süresi doldu", "uygulama sağlayıcısı hesabı kullanım süresi doldu",...) içerir.

- Uygulama sunucusunu kullanıcı kimliği hakkında bilgilendirmek.

Bazı uygulamalarda kimlik doğrulama sunucusu, uygulama sunucusunu, kullanıcının kimliğinin bir gösterimini de geçirebilir. Bazı uygulamalarda, kimlik doğrulama sunucusu uygulama sunucusunu, uygulamadan veya uygulama sağlayıcısından bağımsız olan genel bir kullanıcı adından geçirebilir. Bazı uygulamalarda, kimlik doğrulama sunucusu uygulama sunucusunu, kullanıcının ve uygulama veya uygulama sağlayıcısının bir işlevi olan belirli bir kullanıcı adını geçirebilir. Bazı uygulamalarda, kimlik doğrulama sunucusu, her bir kayıtlı kullanıcı çifti ve etkinleştirilmiş uygulamaların bir kullanıcı kimliğinin her bir doğrulama oturumunda uygulama sunucusuna geçmesini sağlayan bir veritabanını muhafaza etmektedir.

- Doğrulama sonucu hakkında kullanıcıyı bilgilendirmek.

Bazı uygulamalarda, Yanıt Mesajını alan sunucu, dinamik güvenlik değerinin doğrulanması sonucunu içeren kimlik doğrulama cihazına bir alındı mesajı gönderir. Bu mesaj, hata durumunda, bir hata kodu (örneğin "kriptografik doğrulama başarısız", "bilinmeyen kimlik doğrulama cihazı", "bilinmeyen oturum id",

"kullanıcı hesabı süresi doldu", "uygulama sağlayıcısı hesabı süresi doldu",...) içerebilir.

- Dinamik güvenlik değerinin doğrulanmasının sonucuna bağlı olarak uygun eylemde bulunmak. Bazı uygulamalarda, doğrulama işleminin başarılı olması durumunda, kullanıcıya uygulama sunucusunun uygulamasına erişim hakkı verilmesi ve doğrulamanın başarılı olmaması durumunda erişimin reddedilmesi olabilir. Bazı uygulamalarda, doğrulama başarılı olduğunda ve doğrulama başarılı olmazsa gerçekleştirilmediğinde, kullanıcı tarafından sunulan bir işlem isteğinin gerçekleştirilebilmesini içerebilir.

Bazı uygulamalarda uygulama sunucusu, bir veya daha fazla yazılım uygulamasını çalıştıran bir veya daha fazla sunucu bilgisayarı içerebilir. Bazı uygulamalarda uygulama sunucusu, bir veya daha fazla kullanıcı tarafından uzaktan erişilmek üzere bir veya daha fazla uygulamayı barındırabilir. Bazı uygulamalarda uygulama sunucusu bir veya daha fazla web sunucusu içerebilir. Bazı uygulamalarda, uygulama sunucusu tarafından barındırılan bir veya daha fazla uygulama, web tabanlı olabilir.

Bazı uygulamalarda, kullanıcının erişim cihazı, uygulama sunucusu tarafından barındırılan uygulamaya erişmek için bir bilgi işlem cihazını içerebilir. Bazı uygulamalarda, bu bilgi işlem cihazı bir PC veya bir dizüstü bilgisayar içerebilir. Bazı uygulamalarda, bu bilgi işlem cihazı, örneğin bir ortak internet erişim noktasında bir internet erişim cihazı içerebilir. Bazı uygulamalarda erişim cihazı ağa bağlanabilir. Bazı uygulamalarda erişim cihazı, bir bilgisayar ağı üzerinden bir uygulama sunucusu ile iletişim kurmak üzere uyarlanabilir. Bazı uygulamalarda bu bilgisayar ağı, bir ortak telekomünikasyon ağı içerebilir. Bazı uygulamalarda bu bilgisayar ağı interneti içerebilir.

Şekillerin Kısa Açıklaması

Buluşun yukarıdaki ve diğer özellikleri ve avantajları, ekteki çizimlerde gösterildiği gibi, buluşun uygulamalarının daha özel bir tarifnamesi olan aşağıdaki açıklamalardan anlaşılacaktır.

Şekil 1, buluşun örnek bir uygulamasını şematik olarak göstermektedir.

Şekil 2, buluşun bir yönüne göre bir sistemin bir örneğini şematik olarak göstermektedir.

Şekil 3a ve 3b, buluşun bir yönüne göre bir kullanıcı kimlik doğrulama cihazının örneklerini şematik olarak göstermektedir.

Şekil 4a ve 4b, buluşun bir yönüne göre uzaktan erişilebilir bir uygulamayı güvence altına almak için bir yöntemi şematik olarak göstermektedir.

Detaylı Açıklama

Mevcut buluşun bazı uygulamaları aşağıda tartışılmaktadır. Özel uygulamalar tartışılırken, bunun sadece örnekleme amacıyla yapıldığı anlaşılmalıdır. İlgili teknikte uzman bir kişi, diğer bileşenlerin ve yapılandırmaların, buluşun özünden ve alanından ayrılmadan kullanılabileceğini kabul edecektir.

Şekil 1, buluşun örnek bir uygulamasını göstermektedir.

Bir kullanıcı, bir erişim cihazını (şekil üzerinde 'PC Web Tarayıcısı' olarak belirtilen) kullanarak bir uzak uygulamaya (şekilde 'MDP' olarak belirtilir) erişir. Erişim cihazı, örneğin bir PC veya bir dizüstü bilgisayar olabilir. Uzak uygulama bir uygulama sunucusu tarafından barındırılabilir. Kullanıcının erişim cihazı, uygulama sunucusu ile örneğin internet gibi bir bilgisayar ağı üzerinden iletişim kurabilir. Uygulama, web tabanlı olabilir ve kullanıcı, kullanıcının erişim cihazında çalışan bir web tarayıcısı kullanarak web tabanlı uygulamaya erişebilir.

Bir noktada, kullanıcı açık veya dolaylı olarak, uygulamanın erişim-korumalı bir bölümüne (şekil üzerinde 'https://mydigipass.com' olarak etiketlenen ok ile belirtilen) erişim talebinde bulunabilir.

Uygulama bir Kimlik Doğrulama Başlatma Mesajı alabilir. Uygulama, bir Kimlik Doğrulama Sunucusuna (şekilde 'DPS' olarak belirtilir) bir istek göndererek (şekilde 'İstenilen QR Kodu' olarak etiketlenen okla gösterilir) bir Doğrulama Sunucusu göndererek Kimlik Doğrulama Başlatma Mesajı alabilir. Kimlik Doğrulama Sunucusu, bu talebe uygulama bölümüne veya Kimlik Doğrulama Başlatma Mesajının tüm

içeriğine geri dönerek yanıt verebilir. Örneğin, Kimlik Doğrulama Sunucusu, uygulamaya bir alan adı içeren bir mesaj gönderebilir. Mesaj ayrıca bir oturum ID içerebilir. Mesaj ayrıca bir kimlik sorma içerebilir. Uygulama, Kimlik Doğrulama Başlatma Mesajının bir temsilini içeren erişim cihazındaki web tarayıcısına bir web sayfası gönderebilir. Örneğin, web sayfası bir QR Kodu içerebilir. QR Kodu bir URL veya URI'yi kodlayabilir. Bu URL/URI, bir alan adı ve/veya bir oturum ID ve/veya bir kimlik sorma gibi Kimlik Doğrulama Başlatma Mesajında bulunan verileri içerebilir. Web sayfası, kullanıcının kimlik doğrulama cihazı ile QR Kodunu okumasını önerebilir.

Kullanıcının kimlik doğrulama cihazı (şekilde 'Mobil App' ile gösterilir) örneğin bir fotoğraf makinesi içeren ve bir kimlik doğrulama uygulaması ile donatılmış bir akıllı telefon olabilir. Diğer uygulamalarda, özel bir donanım belirteci içerebilir. Kullanıcı kimlik doğrulama cihazında kimlik doğrulama küçük uygulamasını veya uygulamayı başlatabilir ve erişim cihazı tarafından sunulan Kimlik Doğrulama Başlatma Mesajının temsilini elde etmek için kimlik doğrulama küçük uygulamasına veya uygulamasına talimat verebilir. Örneğin, kullanıcı kimlik doğrulama cihazının, kullanıcının erişim cihazının ekranında QR Kodunu okumasını sağlayabilir. Erişim cihazı tarafından sunulan Kimlik Doğrulama Başlatma Mesajının temsilinin elde edilmesi üzerine, örneğin QR Kodunu okuyarak ('QR Kodunu Tara' ve 'QR Kodu (Oturum)' etiketli oklarla gösterilen), kimlik doğrulama uygulaması, Kimlik Doğrulama Başlatma Mesajının içeriğini elde etmek için QR Kodunu çözer. Bu içerikler örneğin bir alan adı ve/veya bir oturum ID ve/veya bir kimlik sorma içerebilir.

Bazı uygulamalarda, kimlik doğrulama uygulaması daha sonra kullanıcı etkileşimi olmadan dinamik bir güvenlik değeri üretebilir. Diğer uygulamalarda, kimlik doğrulama uygulaması, ilerlemeden önce kullanıcının açık onay vermesini isteyebilir, Kimlik doğrulama uygulaması, zamanla depoladığı bir veya daha fazla dinamik değişkeni kriptografik olarak birleştirerek bir kerelik bir şifre oluşturabilir (Şekilde "Oturumu Kimlik Sorma Olarak Kullan' olarak belirtilir). Bir veya daha fazla dinamik değişken, Kimlik Doğrulama Başlatma Mesajından çıkarılan kimlik sorma değerini ve/veya kimlik doğrulama cihazı üzerindeki bir saat tarafından tutulan sürenin değerini ve/veya kimlik doğrulama uygulaması tarafından tutulan bir sayacın değerini içerebilir. (burada kimlik doğrulama uygulaması örneğin her bir OTP'yi ürettiği zaman sayacı arttırabilir). Kimlik doğrulama uygulaması örneğin bir veya daha fazla dinamik değişkenin bir kombinasyonunun bir kriptografik sağlamasını ve SHA-1 gibi bir şifreleme sağlama

algoritması kullanarak şifre üretebilir. Kimlik doğrulama uygulaması örneğin, şifre tarafından parametrelenmiş bir şifreleme algoritması kullanılarak dinamik değişkenlerin bir kombinasyonunu şifreleyebilir.

Kimlik doğrulama cihazı bir Yanıt Mesajı oluşturabilir. Bu Yanıt Mesajı oluşturulan OTP'yi içerebilir. Kimlik Doğrulama Başlatma Mesajından alınan oturum ID'sini de içerebilir. Kimlik doğrulama cihazının örneğin kimlik doğrulama uygulaması tarafından saklanan özgün bir seri numarası gibi bir kimlik tanımlayıcısını da içerebilir. Kimlik doğrulama cihazı, bu Yanıt Mesajını Kimlik Doğrulama Başlatma Mesajından alınan alan adıyla belirtilen bir sunucuya gönderebilir. Alan adı örneğin kimlik doğrulama sunucusunu gösterebilir. Yanıt Mesajını göndermeden önce kimlik doğrulama uygulaması, alan adının Yanıt Mesajı için izin verilen bir hedef noktasını gösterip göstermediğini doğrulayabilir. Kimlik doğrulama cihazı, örneğin alan adını, izin verilen alan adları listesi veya izin verilen alan adı listesi ile karşılaştırabilir.

Kimlik doğrulama cihazı, Yanıt Mesajını örneğin kimlik doğrulama sunucusuna ('Kimlik Doğrulama Talebi (SN, OTP)' olarak etiketlenen ok ile gösterilir) gönderebilir. Yanıt Mesajı örneğin bir HTTP POST mesajını içerebilir. Bu HTTP POST mesajı, QR Kodu tarafından kodlanmış olan URL'de belirtilen sunucuya gönderilebilir.

Yanıt Mesajı alındıktan sonra, kimlik doğrulama sunucusu Yanıt Mesajında bulunan OTP'yi doğrulayabilir. OTP'yi doğrulamak için kimlik doğrulama sunucusu bir doğrulama şifresi kullanabilir. Kimlik doğrulama sunucusu, doğrulama mesajını, Yanıt Mesajında yer alan bir kimlik doğrulama cihazı tanımlayıcısı (örneğin bir seri numarası) kullanarak elde edebilir. Örneğin, doğrulama sunucusu bir veritabanında doğrulama şifresini aramak için kimlik doğrulama cihazı tanımlayıcısını kullanabilir veya doğrulama sunucusu kimlik doğrulama cihazı tanımlayıcısından doğrulama şifresini ve bir ana şifreyi türetebilir.

OTP'yi onayladıktan sonra, kimlik doğrulama sunucusu sonucu kimlik doğrulama cihazına bildirebilir (şekilde 'ACK' olarak etiketlenen ok ile gösterilir).

OTP'yi onayladıktan sonra, kimlik doğrulama sunucusu, doğrulama sonucunu uygulama sunucusuna bildirebilir. Örneğin, uygulama sunucusu Kimlik Doğrulama Başlatma Mesajında yer alan oturum ID'siyle ilişkili OTP'nin geçerliliği için kimlik doğrulama sunucusunu sorgulayabilir.

Kimlik doğrulama sunucusu, uygulama sunucusuna bir kullanıcı tanımlayıcısı (kullanıcı adı gibi) da iletebilir. Kullanıcı tanımlayıcısını elde etmek için, kimlik doğrulama sunucusu, Yanıt Mesajında bulunabilecek kimlik doğrulama cihazı tanımlayıcısını kullanarak bir veritabanında arama yapabilir. Bazı uygulamalarda, veritabanı belirli bir kimlik doğrulama cihazı ile ilişkili aynı kullanıcı için birden fazla kullanıcı tanımlayıcısı içerebilir. Örneğin kimlik doğrulama hizmeti, farklı uygulama sunucuları için farklı bir kullanıcı tanımlayıcısını depolayabilir ve ilgili kullanıcı tanımlayıcısını uygulama sunucusuna iletebilir. Bazı uygulamalarda, kimlik doğrulama hizmeti aynı kullanıcı ve aynı uygulama için birden fazla kullanıcı tanımlayıcısını depolayabilir ve kimlik doğrulama sunucusu, kullanıcının uygulama sunucusuna geçmesi için doğru kullanıcı tanımlayıcısını seçmesine izin vermek üzere kimlik doğrulama cihazı ile bir diyaloga girebilir.

Uzaktan uygulamaları güvenli hale getirmek için bir sistem.

Şekil 2, buluşun bir yönüne göre bir sistemin bir örneğini şematik olarak göstermektedir.

Sistem (200) aşağıdaki bileşenleri içerir: bir uygulama sunucusu (210), bir kimlik doğrulama sunucusu (220), bir çok erişim cihazı (230) ve bir çok kullanıcı kimlik doğrulama cihazı (240). Bazı uygulamalarda, birden fazla uygulama sunucusu olabilir.

Uygulama sunucusu (210), bir veya daha fazla uzaktan erişilebilir uygulamayı barındırmak üzere uyarlanabilir. Örneğin bir web sunucusunu barındırabilir. Uygulama sunucusu bir sunucu bilgisayarı içerebilir. Uygulama sunucusu, örneğin bir veya daha fazla mikroişlemci gibi bir veri işleme bileşenini içerebilir. Veri ve/veya yazılım depolamak için depolama bileşenlerini içerebilir. Bu depolama bileşenleri, RAM ve/veya sabit diskler gibi uçucu ve/veya uçucu olmayan bellek içerebilir. Uygulama sunucusu, uygulama sunucusunun veri ve mesajları örneğin kimlik doğrulama sunucusu ve/veya bir erişim cihazı ve/veya bir kullanıcı kimlik doğrulama cihazı ile iletişim ve veri alışverişi yapabilmesi için uygulama sunucusunu bir bilgisayar ağına (250) (örneğin internet) bağlamak için bir veri iletişim arayüzü (örneğin bir Ethernet kartı gibi) içerebilir.

Bir uygulama sunucusu tarafından barındırılabilecek uzaktan erişilebilir uygulamalara örnek olarak şunlar verilebilir: İnternet bankacılığı uygulamaları, e-ticaret siteleri, web posta uygulamaları (Gmail gibi), sosyal ağ siteleri (Facebook gibi) ve diğer web tabanlı, internet tabanlı veya bulut tabanlı uygulamalar.

Kimlik doğrulama sunucusu (220), bir kullanıcı kimlik doğrulama cihazı tarafından oluşturulabilen örnek bir kerelik şifreler veya işlem imzaları gibi dinamik güvenlik değerlerini doğrulamak üzere uyarlanabilen bir kimlik doğrulama sunucusu uygulamasını barındırabilir. Bazı uygulamalarda, kimlik doğrulama sunucusu, farklı, ilgisiz uygulama sağlayıcılarının kontrolü altında olabilen birden fazla uygulama sunucusu adına dinamik güvenlik değerlerini doğrulayan güvenilir bir taraf olarak hareket edebilir. Kimlik doğrulama sunucusu, bazı uygulamalarda simetrik ve/veya asimetrik kriptografik algoritmaları içerebilen kriptografik hesaplamaları gerçekleştirecek şekilde uyarlanabilir. Kimlik doğrulama sunucusu, belirli güvenlik hassasiyetli işlemleri veya gizli anahtarları içerebilen hesaplamaları güvenli bir şekilde gerçekleştirmek için örneğin bir HSM (donanım güvenlik modülü) gibi güvenli donanımı içerebilir. Kimlik doğrulama sunucusu bir sunucu bilgisayarını içerebilir. Kimlik doğrulama sunucusu, örneğin bir veya daha fazla mikroişlemci gibi bir veri işleme bileşenini içerebilir. Veri ve/veya yazılım depolamak için depolama bileşenlerini içerebilir. Bu depolama bileşenleri, RAM (Rastgele Erişim Belleği) ve/veya sabit diskler gibi uçucu ve/veya uçucu olmayan bellek içerebilir.

Bazı uygulamalarda, depolama bileşenleri bir veri tabanını içerebilir. Bazı uygulamalarda, depolama bileşenleri, birden çok kullanıcının her biri için kullanıcı ile ilgili verileri depolamak için kullanılabilir. Bazı uygulamalarda, bu kullanıcı ile ilgili veriler, örneğin, bazı uygulamalarda uygulamaya özgü olabilecek bir veya daha fazla kullanıcı ile ilişkili gizli anahtar veya kullanıcı profili verisi içerebilir. Bazı uygulamalarda, kullanıcı ile ilgili bu veriler, örneğin kullanıcıyla ilişkilendirilebilen bir veya daha fazla Kullanıcı kimlik doğrulama cihazının kullanıcı kimlik doğrulama cihazı tanımlama verilerini (seri numarası gibi) içerebilir.

Bazı uygulamalarda, depolama bileşenleri, çok sayıda kullanıcı kimlik doğrulama cihazının her biri için kullanıcı kimlik doğrulama cihazı ile ilgili verileri depolamak için kullanılabilir. Bazı uygulamalarda, bu kullanıcı kimlik doğrulama cihazı ile ilgili veriler, örneğin, bazı uygulamalarda uygulama ve/veya kullanıcıya özel olabilecek bir veya daha fazla kullanıcı kimlik doğrulama cihazı ile ilgili gizli anahtar veya kullanıcı kimlik

doğrulama cihazı yapılandırma verilerini içerebilir. Bazı uygulamalarda, bu kullanıcı kimlik doğrulama cihazı ile ilgili veriler, örneğin kullanıcı kimlik doğrulama cihazıyla ilişkili olabilen bir veya daha fazla kullanıcının kullanıcı tanımlama verilerini (bir kullanıcı adı veya kullanıcı ID gibi) içerebilir.

Kimlik doğrulama sunucusu, kimlik doğrulama sunucusunun bir bilgisayar ağına (örneğin, internet gibi) bağlanması için bir iletişim arayüzü (örneğin bir Ethernet kartı) içerebilir, böylece kimlik doğrulama sunucusu örneğin bir uygulama sunucusu ve/veya bir kullanıcı kimlik doğrulama cihazı ve/veya bir erişim cihazı ile iletişim kurabilir.

Bazı uygulamalarda, tek bir sunucu hem bir uygulama sunucusu hem de bir kimlik doğrulama sunucusu olarak görev yapabilir. Diğer uygulamalarda, uygulama sunucuları ve kimlik doğrulama sunucusu, bir bilgisayar ağı (örneğin internet gibi) üzerinden mesajlar göndererek uzaktan etkileşimde bulunan ayrı sunuculardır.

Erişim cihazı (230), bir uygulama sunucusuna bağlanmak ve bir kullanıcının bir uygulama sunucusu ile bir bilgisayar ağı üzerinden uzaktan etkileşime girmesine izin vermek için uyarlanmış bir elektronik cihaz olabilir. Erişim cihazı, örneğin bir veya daha fazla mikroişlemci gibi bir veri işleme bileşenini içerebilir. Veri ve/veya yazılım depolamak için depolama bileşenlerini içerebilir. Bu depolama bileşenleri, RAM ve/veya sabit diskler ve/veya katı hal sürücüleri (SSD) gibi uçucu ve/veya uçucu olmayan bellek içerebilir. Erişim cihazı, erişim cihazının bir bilgisayar ağına (örneğin, internet gibi) bağlanması için bir iletişim arayüzü (örneğin bir Ethernet kartı gibi) içerebilir, böylece erişim cihazı örneğin bir uygulama sunucusu ve/veya bir kimlik doğrulama sunucusu ile iletişim kurabilir. Erişim cihazı, bir kullanıcı giriş arayüzü ve bir kullanıcı (290) ile etkileşime girmek için bir kullanıcı çıkış arayüzüne sahip bir kullanıcı arayüzü içerebilir. Erişim cihazı, örneğin kullanıcıya çıkışı sunmak için bir ekran ve/veya hoparlör içerebilir ve örneğin bir kullanıcıdan giriş almak için bir klavye ve/veya bir dokunmatik ekran ve/veya bir fare içerebilir.

Erişim cihazı örneğin bir Kişisel Bilgisayar (PC) veya bir dizüstü bilgisayar veya bir tablet bilgisayar gibi bir bilgi işlem cihazını içerebilir. Erişim cihazının, kullanıcının internet gibi bir bilgisayar ağı üzerinden uzak bir uygulama ile etkileşime girmesine izin veren bir bilgisayar programı sağlanabilir. Bu bilgisayar programı örneğin bir web tarayıcısını (örneğin, Internet Explorer veya Mozilla Firefox gibi) içerebilir ve uzak

uygulama örneğin bir web-tabanlı sunucu uygulamasını içerebilir. Erişim cihazı, veri ve mesaj alışverişi yaparak bir uygulama sunucusu tarafından barındırılan bir uygulama ile etkileşime girebilir. Erişim cihazı, bir uygulama sunucusu tarafından barındırılan bir uygulama ile, örneğin IP (İnternet Protokolü) ve/veya SSL/TLS (Güvenli Yuva Katmanı/Aktarım Katmanı Güvenliği) gibi bir iletişim protokolü kullanılarak HTTP (Hypertext Transfer protokolü) gibi mesajlar alışverişi için etkileşim kurabilir.

Bazı uygulamalarda erişim cihazı, erişim cihazının bir uygulama sunucusundan Kimlik Doğrulama Başlatma Mesajının bir temsilini elde etmesini veya üretmesini sağlayan bir Kimlik Doğrulama Başlatma Mesajıyla ilgili verileri almak üzere uyarlanabilir. Örneğin, bazı uygulamalarda erişim cihazı, bir uygulama sunucusundan Kimlik Doğrulama Başlatma Mesajının bir temsilini alacak şekilde uyarlanmıştır. Örneğin, erişim cihazı bir görüntü içeren bir web sayfası (örneğin QR kodu gibi iki boyutlu bir barkod) veya Kimlik Doğrulama Başlatma Mesajını kodlayan bir ses dosyasını alacak şekilde uyarlanabilir. Bazı uygulamalarda, erişim cihazı, bir uygulama sunucusundan Kimlik Doğrulama Başlatma Mesajında yer alan bir veya daha fazla veri elemanını (örneğin bir kimlik sorma ve/veya işlem verisi ve/veya bir uygulama tanımlayıcısı) almak üzere ve bu erişim cihazı, Kimlik Doğrulama Başlatma Mesajının bir temsilini oluşturmak için kullanmak üzere uyarlanmıştır. Örneğin, erişim cihazı Kimlik Doğrulama Başlatma Mesajında içerilecek olan veri elemanlarını içeren bir web sayfasını almak üzere uyarlanabilir ve erişim cihazı, örneğin Kimlik Doğrulama Başlatma Mesajının bir görüntüsünü (örneğin iki boyutlu barkod) üretmek üzere bir tarayıcı eklentisi veya küçük bir uygulama (bu ayrıca alınan bir web sayfasında bulunabilir) gibi bir uygulamayı gerçekleştirebilir. Bazı uygulamalarda erişim cihazı, uygulama sunucusundan, erişim cihazının başka bir sunucudan (örneğin bir kimlik doğrulama sunucusu gibi) Kimlik Doğrulama Başlatma Mesajında yer alan bir veya daha fazla veri elemanını almak için kullandığı bir veri elemanını alacak şekilde uyarlanır ve erişim cihazı Kimlik Doğrulama Başlatma Mesajının bir temsilini oluşturmak için kullanılır. Örneğin, erişim cihazı, bazı sunucularda (örneğin bir kimlik doğrulama sunucusu gibi) bir veri elemanını işaret eden bir URL (Tekdüzen Kaynak Konum Belirleyici) veya URI (Tekdüzen Kaynak Tanımlayıcı) içeren bir web sayfası alacak şekilde uyarlanabilir, burada erişim cihazı Kimlik Doğrulama Başlatma Mesajının bir temsilini oluşturmak için kullanılır. Bu veri elemanı, örneğin Kimlik Doğrulama Başlatma Mesajının içeriğinde yer alan bir veya daha fazla veri elemanını (örneğin bir kimlik sorma) içerebilir veya Kimlik Doğrulama Başlatma Mesajının tamamının bir temsilini içerebilir veya Kimlik

Doğrulama Başlatma Mesajının içeriği veya Kimlik Doğrulama Başlatma Mesajının şifrelenmiş bir temsili üzerinde bir imza veya MAC (Mesaj Kimlik Doğrulama Kodu) gibi Kimlik Doğrulama Başlatma Mesajının kaynağını doğrulayan bir sunucu kimlik bilgisi içerebilir.

Erişim cihazı, Kimlik Doğrulama Başlatma Mesajının bir temsilini kodlayan bir sinyalin çıkışı için uyarlanabilir. Bazı uygulamalarda, erişim cihazı, kullanıcı çıkış arayüzünü (örneğin, ses hoparlörlerini veya ekranını), Kimlik Doğrulama Başlatma Mesajının bir temsilini kodlayan sinyali çıkarmak için kullanacak şekilde uyarlanmıştır. Örneğin bazı uygulamalarda erişim cihazı, hoparlörleri üzerinde, Kimlik Doğrulama Başlatma Mesajının bir temsilini kodlayan bir ses sinyali içeren bir ses dosyasını çalmak üzere uyarlanabilir. Bazı uygulamalarda erişim cihazı, Kimlik Doğrulama Başlatma Mesajının bir temsilini kodlayan zamana bağlı bir optik model göstererek bir optik sinyal yaymaya uyarlanabilir. Bazı uygulamalarda erişim cihazı, Kimlik Doğrulama Başlatma Mesajının bir temsilini kodlayan bir veya daha fazla görüntüyü (iki boyutlu barkodlar gibi) gösterecek şekilde uyarlanabilir.

Kullanıcı kimlik doğrulama cihazı (240), şekiller 3a ve 3b ile ilgili olarak daha ayrıntılı olarak ele alınacaktır.

Bazı uygulamalarda, erişim cihazı ve kullanıcı kimlik doğrulama cihazı, fiziksel olarak farklı cihazlardır. Bazı uygulamalarda, erişim cihazı güvenilir bir varlık olmasa da, kullanıcı kimlik doğrulama cihazı güvenilir bir varlıktır.

Sistem, uygulama sunucularından biri tarafından barındırılan bir uygulamaya erişen kullanıcıların kimliklerini doğrulamak ve/veya uygulama sunucuları tarafından barındırılan bir uygulamaya kullanıcı tarafından gönderilen işlemleri doğrulamak için uyarlanmıştır ve örneğin Şekil 4 ile ilgili tartışılan yöntemle kullanılabilir.

Şekiller 3a ve 3b, buluşun bir yönüne göre bir aparatın uygulama örneğini ve bir varyantını şematik olarak göstermektedir. Aparat, şekil 2'ye göre ele alınan sistemin bir Kullanıcı kimlik doğrulama cihazı (240) örneğini içerir.

Kullanıcı kimlik doğrulama cihazı (240), örneğin bir kullanıcının veya bir işlemin doğrulanması için bir Kimlik Doğrulama Başlatma Mesajına yanıt olarak bir dinamik

güvenlik değeri içeren bir Yanıt Mesajı oluşturmak üzere uyarlanmış bir elektronik cihaz içerir. Kullanıcı kimlik doğrulama cihazı, bir veri işleme bileşenini (310), veri ve/veya yazılımı depolamak için depolama bileşenlerini (320), kullanıcı kimlik doğrulama cihazını bir bilgisayar ağına bağlamak için bir veri iletişim arayüzününe (330), bir kullanıcı ile etkileşim kurmak için bir kullanıcı arayüzüne (340, 350), bir erişim cihazı tarafından (örneğin erişim cihazının kullanıcı çıkış arayüzü vasıtasıyla) çıkarılan bir Kimlik Doğrulama Başlatma Mesajını temsil eden bir sinyali yakalamak için bir giriş arayüzüne (360, 370) ve zamanla ilgili değerler sağlamak için gerçek zamanlı bir saate (380) sahip olabilir.

Veri işleme bileşeni (310), örneğin bir veya daha fazla mikroişlemciyi içerebilir. Veri işleme bileşeni, dinamik güvenlik değerleri üretmek için bir algoritma gerçekleştirecek şekilde uyarlanabilir. Veri işleme bileşeni, simetrik veya asimetrik kriptografik algoritmaların gerçekleştirilmesini içeren kriptografik işlemleri gerçekleştirecek şekilde uyarlanabilir. Bazı uygulamalarda, veri işleme bileşeni bir mikroişlemci ve/veya bir denetleyici ve/veya bir ASIC (Uygulamaya Özgü Entegre Devre) içerebilir.

Kullanıcı kimlik doğrulama cihazı, veri ve/veya yazılım depolamak için depolama bileşenleri (320) içerebilir. Bu depolama bileşenleri, RAM ve/veya ROM (Salt Okunur Bellek) ve/veya Flash ve/veya sabit diskler ve/veya katı hal sürücüleri (SSD) gibi uçucu ve/veya uçucu olmayan bellek içerebilir.

Kullanıcı kimlik doğrulama cihazı, kullanıcı kimlik doğrulama cihazının bir bilgisayar ağına (örneğin, internet) bağlanması için bir veri iletişim arayüzü (330) içerebilir, böylece kullanıcı kimlik doğrulama cihazı ve/veya bir kimlik doğrulama sunucusu örneğin bir uygulama sunucusu ile iletişim kurabilir. Veri iletişim arayüzü, örneğin bir GSM (Mobil İletişim için Global Sistem) veya UMTS (Evrensel Mobil Telekomünikasyon Sistemleri) ağı gibi bir mobil telefon ağı gibi bir kablosuz iletişim ağına bağlanmak için örneğin bir kablosuz veri iletişim arayüzü (330) içerebilir. Bazı uygulamalarda, veri iletişim arayüzü bir mobil telsiz arayüzü ve/veya bir GSM ağ arayüzü içerebilir. Bazı uygulamalarda, veri iletişim arayüzü bir anten içerebilir. Bazı uygulamalarda kablosuz veri iletişim arayüzü, kullanıcı kimlik doğrulama cihazından bir ortak kablosuz veri iletişim ağı kullanılarak bir hedef sunucuya veri göndermek üzere uyarlanabilir. Bazı uygulamalarda, kablosuz veri iletişim arayüzü, ortak bir kablosuz veri iletişim ağı

kullanılarak uzak bir sunucudan (uygulama sunucusu veya kimlik doğrulama sunucusu gibi) veri almak için uyarlanabilir.

Kullanıcı kimlik doğrulama cihazı, bir kullanıcı giriş arayüzü (350) ve bir kullanıcı ile etkileşime girmek için bir kullanıcı çıkış arayüzüne (340) sahip bir kullanıcı arayüzü (340, 350) içerebilir. Kullanıcı kimlik doğrulama cihazı, bir kullanıcıya çıkış sağlamak için bir kullanıcı çıkış arayüzü içerebilir. Kullanıcı çıkış arayüzü, örneğin kullanıcıya çıkışı sunmak için bir ekran (340) ve/veya hoparlör içerebilir. Kullanıcı kimlik doğrulama cihazı, bir kullanıcıdan girdi almak için bir kullanıcı giriş arayüzü içerebilir. Kullanıcı giriş arayüzü, örneğin bir kullanıcıdan girdi almak için bir klavye (350) ve/veya bir dokunmatik ekran ve/veya bir mikrofon içerebilir. Ekran bir grafik ekran içerebilir. Ekran bir renkli ekran içerebilir. Ekran, örneğin bir LCD (Sıvı Kristal Ekran) ekranı veya bir TFT (İnce Film Transistör) ekranı veya bir OLED (Organik Işık Yayan Diyot) ekranı içerebilir.

Kullanıcı kimlik doğrulama cihazı, bir erişim cihazı tarafından (örneğin erişim cihazının kullanıcı çıkış arayüzü tarafından) çıkan bir Kimlik Doğrulama Başlatma Mesajını temsil eden bir sinyali yakalamak için bir giriş arayüzü (360, 370) içerebilir. Örneğin, bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, örneğin bir erişim cihazının hoparlörleri tarafından yayılan ve bir Kimlik Doğrulama Başlatma Mesajıyla kodlanan bir ses sinyalini yakalamak için bir mikrofon (370) içerebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, örneğin bir erişim cihazının gösterilmesiyle ve bir Kimlik Doğrulama Başlatma Mesajıyla kodlanmış olarak ortaya çıkan optik sinyalleri yakalamak için optik sensörler içerebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, bir erişim cihazının ekranında görüntülenen bir veya daha fazla görüntüyü yakalamak ve bir Kimlik Doğrulama Başlatma Mesajını kodlamak için bir kamera (360) içerebilir. Bazı uygulamalarda, bu görüntüler bir QR kodu gibi iki boyutlu bir kod içerebilir.

Kullanıcı kimlik doğrulama cihazı, kullanıcı kimlik doğrulama cihazının dinamik bir güvenlik değeri oluşturmak için bir kriptografik algoritma için girdi olarak kullanabileceği zamana bağlı değerler sağlamak için gerçek zamanlı saat (380) gibi bir zamanlama mekanizması içerebilir.

Kullanıcı kimlik doğrulama cihazı, yakalanan sinyalin kodunu çözerek Kimlik Doğrulama Başlatma Mesajını elde etmek üzere uyarlanabilir. Örneğin, bir Kimlik Doğrulama Başlatma Mesajını şifreleyen modüle edilmiş bir ses sinyalinin kodunu çözmek için uyarlanabilir veya bir Kimlik Doğrulama Başlatma Mesajını kodlayan bir veya daha fazla görüntüyü (QR kodları gibi) çözmek üzere uyarlanabilir.

Sunucu kimlik doğrulaması.

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, bir sunucu kimlik bilgisini içerir ve kullanıcı kimlik doğrulama cihazı, bu kimlik bilgisini doğrulamak için uyarlanabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcı kimlik doğrulama cihazında depolanabilen veya kullanıcı kimlik doğrulama cihazının, kullanıcı kimlik doğrulama cihazı içinde depolanan bir anahtar kullanılarak elde edilebilen bir sunucu kimlik doğrulama anahtarı ile parametrelenmiş bir kriptografik algoritma kullanılarak sunucu bilgisini doğrulamak üzere uyarlanmıştır.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, sunucu bilgisini doğrulamak için asimetrik bir kriptografik algoritma kullanabilir. Bazı uygulamalarda, sunucu kimlik bilgisi, Kimlik Doğrulama Başlatma Mesajının en azından bazı veri elemanları üzerinde bir dijital imzadan oluşur ve sunucu kimlik bilgilerinin doğrulanması, bu imzanın doğrulanmasını içerebilir. Bazı uygulamalarda, sunucu kimlik bilgisinin imzası, kimlik doğrulama sunucusu gibi bir güvenilir sunucu ile ilişkilendirilmiş bir ortak-özel anahtar çiftinin özel anahtarı tarafından oluşturulmuştur ve kullanıcı kimlik doğrulama cihazı, kullanıcı kimlik doğrulama cihazında depolanabilen ilgili ortak anahtarı kullanarak imzayı doğrulamaktadır.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, sunucu bilgisini doğrulamak için bir simetrik kriptografik algoritma kullanabilir. Bazı uygulamalarda simetrik kriptografik algoritma, simetrik bir gizli sunucu kimlik anahtarı ile parametrelenir. Bazı uygulamalarda, sunucu kimlik bilgisi Kimlik Doğrulama Başlatma Mesajının şifrelenmiş bir bölümünü içerir ve kullanıcı kimlik doğrulama cihazı, bu şifrelenmiş bölümün şifresini çözerek sunucu bilgisini doğrular ve örneğin, şifrelenmiş kısımdaki belirli veri elemanları (örneğin etiketler) için belirli sabit değerler veya örneğin bir CRC kodunun değeri veya belirli verilerin uzunlukları gibi belirli veri elemanlarının değerleri arasındaki belirli zorunlu değerler gibi belirli veri alanları (uzunluk alanları ile belirtildiği gibi) veya

belirli veri alanlarının değerlerinin izin verilen aralığı üzerindeki kısıtlamalar gibi şifrelenmiş kısımda belirli beklenen yapısal elemanların mevcut olduğunu doğrular. Bazı uygulamalarda, sunucu kimlik bilgisi bir MAC (mesaj doğrulama kodu) veya Kimlik Doğrulama Başlatma Mesajının bir kısmı üzerinden anahtarlanmış bir sağlama içerir ve kullanıcı kimlik doğrulama cihazı MAC veya anahtarlı sağlama için bir referans değeri hesaplayabilir ve referans değerini alınan sunucu kimlik bilgisi ile karşılaştırır.

Bazı uygulamalarsa, kullanıcı kimlik doğrulama cihazı, sunucu kimlik doğrulamasının doğrulanması başarısız olursa Kimlik Doğrulama Başlatma Mesajını reddedebilir.

Bazı uygulamalarda kodu çözülmüş Kimlik Doğrulama Başlatma Mesajı şifrelenebilir ve kullanıcı kimlik doğrulama cihazı, şifreli Kimlik Doğrulama Başlatma Mesajının şifresini çözmek için uyarlanabilir.

Kimlik Doğrulama Başlatma Mesajından veri çıkarma.

Kullanıcı kimlik doğrulama cihazı, Kimlik Doğrulama Başlatma Mesajında bulunan bazı veri elemanlarını çıkarmak için uyarlanabilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajında yer alan ve kullanıcı kimlik doğrulama cihazı tarafından çıkarılabilen veri elemanları aşağıdakilerden birini veya daha fazlasını içerebilir: bir kimlik sorma, işlemle ilgili tarih, uygulama kimliği ile ilgili veri elemanı, bir oturum id, bir tek seferlik anahtar, sunucu tarafından oluşturulan dinamik güvenlik değeri.

Başvuru kimliğinin gösterilmesi ve onaylanması.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı Kimlik Doğrulama Başlatma Mesajından bir uygulama kimliği ile ilgili veri elemanını çıkarmak üzere uyarlanabilir. Kullanıcı kimlik doğrulama cihazı, uygulama kimliğinin bir temsilini elde etmek veya üretmek için bu uygulama kimliği ile ilgili veri elemanını kullanacak şekilde uyarlanabilir. Uygulama kimliğinin bu temsili, kullanıcı tarafından yorumlanabilir ve tanınabilir. Bazı uygulamalarda, uygulama kimliği ile ilgili veri elemanı, uygulama kimliğinin temsilidir. Örneğin, uygulama kimliği ile ilgili veri elemanı (ve uygulama kimliğinin temsili) sadece bir alfanümerik uygulama adı olabilir. Bazı uygulamalarda, uygulama kimliği ile ilgili veri elemanı, kullanıcı kimlik doğrulama cihazının, uygulama kimliğinin temsilini bir dahili veri tabanından almak için kullanabileceği bir endekse sahip olabilir. Bazı

uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcı kimlik doğrulama cihazında depolanan herhangi bir uygulamaya özel veri elemanı (kalıcı olarak) kullanılmadan Kimlik Doğrulama Başlatma Mesajındaki uygulama kimliği ile ilgili veri elemanından uygulama kimliğinin temsilini belirlemek için uyarlanabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcı kimlik doğrulama cihazının bir harici kaynaktan aldığı Kimlik Doğrulama Başlatma Mesajındaki uygulama kimliği ile ilgili veri elemanından uygulama kimliğinin temsilini ve veriyi saptamak üzere uyarlanabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, uygulamaya özgü verileri harici bir kaynaktan almak için uygulama kimliği ile ilgili veri elemanını kullanabilir ve uygulama kimliğinin temsilini elde etmek için alınan verileri kullanabilir. Bazı uygulamlarda, uygulama kimliği ile ilgili veri elemanı, örneğin bir URL veya URI gibi bir referans içerebilir, şöyle ki kullanıcı kimlik doğrulama cihazı bu referansları uygulama kimliğinin temsilini, örneğin kimlik doğrulama sunucusu veya bir uygulama sunucusu gibi bir uzak sunucu gibi bir harici kaynaktan almak için kullanabilir. Bazı uygulamalarda, uygulama kimliğinin temsili, bir uygulama ismi içerebilir. Bazı uygulamalarda, uygulama kimliğinin temsili bir uygulama logosu gibi bir grafik görüntüsü içerebilir. Bazı uygulamalarda uygulama kimliğinin temsili, karakteristik bir ses dizisi içerebilir. Bazı uygulamalarda, uygulama kimliğinin temsili bir uygulama isminin bir sentetik konuşma oluşturulmasını içerebilir.

Bazı uygulamalarda, uygulama kimliğinin temsili, kullanıcı tarafından yorumlanabilir ve tanınabilir ve kullanıcı kimlik doğrulama cihazı, Kimlik Doğrulama Başlatma Mesajına yanıt olarak bir Yanıt Mesajı oluşturmak üzere işlemin bir parçası olarak kullanıcı kimlik doğrulama cihazının kullanıcısına uygulama kimliğinin temsilini sunacak şekilde uyarlanabilir. Örneğin bazı uygulamalarda kullanıcı kimlik doğrulama cihazı kendi ekranında bir uygulama ismi gösterebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı kendi ekranında, uygulama logosu gibi uygulamanın bir temsilcisini görüntüleyebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, hoparlörleri üzerinde, karakteristik bir ses dizisi veya uygulama isminin bir sentetik konuşma görüntüsü gibi uygulamayı temsil eden bir ses dizisi üzerinden çıktı verebilmektedir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcının kimlik doğrulama cihazının kullanıcıya sunduğu uygulama kimliğinin temsilinin açık veya net bir şekilde teyit edilmesini sağlamak üzere uyarlanmıştır. Bazı uygulamalarda, kullanıcı uygulama kimliğinin temsilini örneğin bir OK düğmesine tıklayarak teyit eder. Bazı uygulamalarda,

uygulama kimliğinin temsilinin teyidi, genel bir teyide entegre edilir, burada kullanıcı örneğin Yanıt Mesajının üretilmesini onaylar ve böylece tüm veri veya mesajların onayını veya teyidini sinyaller (uygulama kimliğinin gösterilmesinden ayrı olarak, kullanıcı tarafından onaylanması gereken Kimlik Doğrulama Başlatma Mesajında yer alan belirli verileri içerebilir), şöyle ki kullanıcı kimlik doğrulama cihazı, bir Yanıt Mesajı oluşturma sürecini kullanıcıya sunar. Bazı uygulamalarda, kullanıcı bir PIN veya şifre girerek, kullanıcı kimlik doğrulama cihazı tarafından dahili bir onay veya teyit olarak kabul edilir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcı uygulama kimliğinin temsilini doğrulamazsa, Yanıt Mesajının üretimini iptal etmek üzere uyarlanmıştır. Bazı uygulamalarda, kullanıcı onaylamazsa, kullanıcı kimlik doğrulama cihazı yine de Yanıt Mesajının oluşturulmasına devam edebilir, ancak bunun yerine kullanıcıya veya bir hedef sunucuya Yanıt Mesajını sunmaz.

İşlemle ilgili verilerin onaylanması.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, Kimlik Doğrulama Başlatma Mesajından işlemle ilgili verileri çıkarmak için uyarlanabilir. Bazı uygulamalarda, işleme ilişkin veriler, Kimlik Doğrulama Başlatma Mesajının şifrelenmiş bir bölümünde oluşturulabilir veya sunucu tarafından oluşturulan dinamik güvenlik değeri gibi Kimlik Doğrulama Başlatma Mesajındaki diğer verilere kriptografik olarak (örneğin bir sunucu kimlik bilgisi ile) bağlanabilir. Bu işlemle ilgili veriler, kullanıcının uzak uygulamaya gönderdiği bir işlemin elemanları için değerler içerebilir. Örneğin, para transferi işlemi söz konusu olduğunda, bu işlemle ilgili veriler transfer edilecek para miktarını, para kodunu ve hedef hesap numarasını içerebilir. Hisse senedi alım satım işlemi söz konusu olduğunda, işlemle ilgili veriler örneğin, işlem görecek olan hisse senedinin sembolü, alım veya satım, hisse başına fiyat ve işlem yapılacak payların miktarını içerebilir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, bu işlemle ilgili verileri kullanıcıya sunacak ve kullanıcı kimlik doğrulama cihazının kullanıcıya sunduğu işlemle ilgili verilerin gizli veya açık bir şekilde onaylanmasını sağlayacak şekilde uyarlanır. Bazı uygulamalarda, kullanıcı, işlemle ilgili verileri örneğin, bir OK düğmesine tıklayarak teyit eder. Bazı uygulamalarda uygulama kimliğinin gösterilmesinin doğrulanması,

genel onayda entegre şekildedir, burada kullanıcı, örneğin Yanıt Mesajının oluşturulmasını onaylar ve böylelikle bir Yanıt Mesajı oluşturmak üzere süreç sırasında kullanıcı doğrulama cihazının kullanıcıya sunduğu tüm (uygulama kimliğinin gösterilmesinden ayrı olarak, kullanıcı tarafından doğrulanması gereken Doğrulama Başlatma Mesajında yer alan bazı verileri de içerebilen) veri veya mesajların kendisi tarafından onaylandığını veya kabul edildiğini bildirir. Bazı uygulamalarda, kullanıcının bir PIN veya şifre girmesi, kullanıcı kimlik doğrulama cihazı tarafından dahili bir onay veya teyit olarak kabul edilir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcı işlemle ilgili verileri doğrulamazsa, Yanıt Mesajının üretimini iptal etmek üzere uyarlanmıştır. Bazı uygulamalarda, kullanıcı onaylamazsa, kullanıcı kimlik doğrulama cihazı yine de Yanıt Mesajının oluşturulmasına devam edebilir, ancak bunun yerine Kullanıcıya veya bir hedef sunucuya Yanıt Mesajını sunmaz.

Kullanıcı tarafından sağlanan verilerin girişi.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcının belirli veri elemanları için değerleri girmesini istemek üzere uyarlanabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı bu değerleri dinamik güvenlik değerinin üretilmesinde ve/veya Yanıt Mesajının üretilmesinde kullanabilir.

PIN girişi ve PIN kullanımı.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcıdan bir PIN veya şifre değeri elde edecek şekilde uyarlanmıştır. Bazı uygulamalarda kullanıcı, kullanıcı kimlik doğrulama cihazının klavyesi veya dokunmatik ekranını kullanarak PIN veya şifre değerini sağlayabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı bir PIN veya şifre referans değerini saklamak ve saklanan referans değeri ile karşılaştırarak kullanıcı tarafından sağlanan PIN veya şifre değerini doğrulamak üzere uyarlanmıştır. Kullanıcı kimlik doğrulama cihazı, kullanıcı tarafından sağlanan PIN veya şifre değeri, kayıtlı referans değeriyle eşleştiğinde PIN veya şifre doğrulamasını başarılı olarak kabul edebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, PIN veya şifre doğrulaması başarısız olursa, Yanıt Mesajının üretilmesini iptal edecek şekilde uyarlanmıştır. Bazı uygulamalarda, PIN veya şifre doğrulaması başarısız olursa,

kullanıcı kimlik doğrulama cihazı yine de Yanıt Mesajının oluşturulmasına devam edebilir, ancak bunun yerine kullanıcıya veya bir hedef sunucuya Yanıt Mesajını sunmaz.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, bir gizli anahtarın değerini elde etmek veya üretmek için girilen PIN veya şifre değerini kullanabilir. Örneğin, kullanıcı kimlik doğrulama cihazı, başka bir anahtar elde etmek için PIN veya şifre değeri ana anahtarla kriptografik olarak birleştirebilir veya şifreli bir anahtar değerinin şifresini çözmek için PIN veya şifre değeri bir anahtar olarak kullanabilir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, Yanıt Mesajına girilen PIN veya şifre değerinin bir temsilcisini eklemek üzere uyarlanmıştır. Bazı uygulamalarda, Kullanıcı kimlik doğrulama cihazı, girilen PIN'in veya şifre değerinin değer temsilcisini içeren Yanıt Mesajının bir bölümünü şifrelemek üzere uyarlanmıştır.

Kriptografik olarak dinamik bir güvenlik değeri üretme veya elde etme.

Kullanıcı kimlik doğrulama cihazı, en az bir gizli anahtar ile parametrelenmiş bir kriptografik algoritma kullanarak dinamik bir güvenlik değeri üretmek veya elde etmek üzere uyarlanabilir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazının dinamik güvenlik değerini (veya dinamik güvenlik değeri oluşturma anahtarını) oluşturmak için kullandığı en az bir gizli anahtar, kullanıcı kimlik doğrulama cihazının bir depolama bileşeninde saklanan bir temel şifre ile matematiksel olarak ilişkilidir. Bazı uygulamalarda temel şifre, kişiselleştirilmiş bir veri elemanı içerebilir. Bu uygulama bağlamında bir kullanıcı kimlik doğrulama cihazının terminoloji 'kişiselleştirilmiş veri elemanı', çok sayıda kullanıcı kimlik doğrulama cihazının her bir cihazında aynı fonksiyona sahip olan çok sayıda kullanıcı doğrulama cihazında bulunan, ancak çok sayıda kullanıcı doğrulama cihazının her bir özel cihazında belirli bir bireysel değere sahip olan bir veri elemanına atıfta bulunmaktadır. Başka uygulamalarda temel şifre, çoklu kullanıcı doğrulama cihazları arasında paylaşılan bir ana şifre içerebilir. Bazı uygulamalarda, Kullanıcı kimlik doğrulama cihazı, kullanıcı kimlik doğrulama cihazının bir depolama bileşeninde saklanan temel şifreden en az bir dinamik güvenlik değeri oluşturma anahtarını türetmek üzere uyarlanmıştır. Bazı uygulamalarda, Kullanıcı kimlik doğrulama cihazı,

kullanıcı tarafından sağlanan bir PIN veya şifre veya başka bir gizli değer kullanarak en az bir dinamik güvenlik değeri üretme anahtarını türetmek üzere uyarlanmıştır. Bazı uygulamalarda, en az bir dinamik güvenlik değeri oluşturma anahtarı temel şifredir. Bazı uygulamalarda, en az bir dinamik güvenlik değeri oluşturma anahtarının ve/veya kişiselleştirilmiş temel şifre değerleri, belirli bir kullanıcıyla veya belirli bir kullanıcı kimlik doğrulama cihazı ile ilişkilendirilir. Bazı uygulamalarda, dinamik güvenlik değeri oluşturma anahtarı, örneğin bir kimlik doğrulama sunucusuyla paylaşıldığı veya bir kimlik doğrulama sunucusu için mevcut olduğu bir simetrik şifreleme veya şifre çözme anahtarı gibi bir simetrik anahtar içerebilir. Bazı uygulamalarda, dinamik güvenlik değeri oluşturma anahtarı, asimetrik bir şifreleme algoritması ile kullanılacak bir ortak/özel anahtar çiftinin özel anahtarını içerebilir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama aracı, giriş değerlerini en az bir dinamik güvenlik değeri oluşturma anahtarı ile parametrelenen bir kriptografik algoritmaya göndererek bir dizi girdi değerini ve en az bir dinamik güvenlik değeri oluşturma anahtarını kriptografik olarak birleştirerek dinamik güvenlik değerini üretecek şekilde uyarlanabilir. Bu girdi değerleri örneğin aşağıdakileri içerebilir: bir dinamik değişken (kullanıcı kimlik doğrulama cihazı tarafından sağlanan zamana bağlı bir değer ve/veya kullanıcı kimlik doğrulama cihazı tarafından sağlanan sayaç-ilişkili bir değer ve/veya Kimlik Doğrulama Başlatma Mesajından çıkarılan kullanıcı kimlik doğrulama cihazı ile ilgili bir kimlik sorma) ve/veya kullanıcı kimlik doğrulama cihazının Kimlik Doğrulama Başlatma Mesajından çıkardığı ve kullanıcı tarafından onaylanabilen işlemle ilgili veriler ve/veya kullanıcı kimlik doğrulama cihazının Kimlik Doğrulama Başlatma Mesajından çıkardığı bir oturum tanımlayıcısı ve/veya kullanıcı kimlik doğrulama cihazının Kimlik Doğrulama Başlatma Mesajından çıkardığı veya kullanıcıya sunulan ve kullanıcı tarafından onaylanabilen uygulama tanımlayıcısı bir temsili ile ilgili olduğu bir uygulama tanımlayıcısına ilişkin bir veri elemanı. Bazı uygulamalarda, girdi değerleri kullanıcı tarafından kullanıcı kimlik doğrulama cihazına sağlanan verileri de içerebilir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kişiselleştirilmiş bir veri elemanı kullanılarak dinamik güvenlik değerini üretecek şekilde uyarlanabilir. Bazı uygulamalarda bu kişiselleştirilmiş veri elemanı kişiselleştirilmiş bir şifreleme anahtarını içerebilir. Bazı uygulamalarda bu kişiselleştirilmiş veri elemanı, bir kullanıcı kimlik doğrulama cihazı tanımlayıcısı ile ilgili veri elemanını (bir seri numarası gibi) içerebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, bir ana şifreden ve bazı

uygulamalarda bir kullanıcı kimlik doğrulama cihazı tanımlayıcısı ile ilgili veri elemanını (bir seri numarası gibi) içerebilen kişiselleştirilmiş bir veri elemanından dinamik güvenlik değeri oluşturma anahtarını türetir.

Bazı uygulamalarda, dinamik güvenlik değerini üretmek veya elde etmek için kullanıcı kimlik doğrulama cihazı tarafından kullanılan şifreleme algoritması, bir simetrik kriptografik algoritma içerebilir. Simetrik kriptografik algoritmaların örnekleri arasında, DES (Veri Şifreleme Standardı) veya AES (Gelişmiş Şifreleme Standardı), simetrik MAC (Mesaj Doğrulama Kodu) algoritmaları, HMAC (anahtarlı sağlama mesaj kimlik doğrulama kodu) gibi anahtarlı karma algoritmalar gibi simetrik şifreleme/şifre çözme algoritmaları veya SHA-1 veya MD5 (en az bir dinamik güvenlik değeri oluşturma anahtarı karma algoritması) bulunabilir. Örneğin, bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, CBC (Şifre Blok Zincirlemesi) modunda DES veya AES gibi simetrik bir blok şifreleyici kullanarak giriş değerlerinin bir birleşimini şifreleyebilir ve sonuçta elde edilen kriptogramın bir kısmını (tercihen kriptogramın son bloğunun bir parçasını) kullanabilir.

Bazı uygulamalarda, dinamik güvenlik değerini oluşturmak veya elde etmek için kullanıcı kimlik doğrulama cihazı tarafından kullanılan kriptografik algoritma, asimetrik bir şifreleme algoritması içerebilir. Simetrik kriptografik algoritma örnekleri, örneğin RSA (Rivest-Shamir-Adleman) veya DSA (Dijital İmza Algoritması) içerebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı örneğin bir ortak-özel anahtar çiftinin özel anahtarı ile parametrelenmiş bir asimetrik kriptografik algoritma kullanılarak giriş değerleri üzerinde bir dijital imza üretebilir.

Bazı uygulamalarda, bir sunucu tarafından üretilen dinamik güvenlik değeri, Kimlik Doğrulama Başlatma Mesajının şifrelenmiş bir bölümünde oluşturulabilir ve kullanıcı kimlik doğrulama cihazı, şifrelenmiş bölümün şifresini çözerek ve şifresi çözülmüş bölümden sunucu tarafından oluşturulan dinamik güvenlik değerini çıkararak bu dinamik güvenlik değerini elde edecek şekilde uyarlanabilir.

Çıkarılabilir güvenlik cihazı

Bazı uygulamalarda, **şekil 3b**'de gösterildiği gibi, kullanıcı kimlik doğrulama cihazı (240), bir çıkarılabilir güvenlik cihazı (395) ve bu çıkarılabilir güvenlik cihazı ile veri

ve/veya mesajlar ve/veya komutlar ve yanıtlar ile veri alışverişi için ve bir iletişim arayüzü (390) içerebilir. Bazı uygulamalarda çıkarılabilir güvenlik cihazı, gizli anahtarları güvenli bir şekilde depolamak ve/veya işlemek üzere uyarlanabilir ve/veya belirli kriptografik hesaplamaları gerçekleştirmek üzere uyarlanabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, bazı şifreleri (kriptografik anahtarlar ve/veya kullanıcı PIN veya şifre değerleri gibi) güvenli bir şekilde depolamak ve/veya yönetmek için çıkarılabilir güvenlik cihazına güvenebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, bazı kriptografik hesaplarını çıkarılabilir güvenlik cihazına devredebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değeri oluşturma anahtarının değerini elde etmek için çıkarılabilir güvenlik cihazı tarafından sağlanan veri elemanlarını kullanır. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değeri oluşturma anahtarının değerinin çıkarılabilir güvenlik cihazına türetilmesi için kriptografik hesapların bir kısmını temsil eder. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değerini çıkarılabilir güvenlik cihazına üretmek için kriptografik hesaplamaların bir kısmını temsil eder. Bazı uygulamalarda, çıkarılabilir güvenlik cihazı kullanıcı kimlik doğrulama ile ilgili referans verilerini (örneğin bir kullanıcı PIN veya şifre için referans değerleri veya bir kullanıcı biyometrik için referans şablonu) içerir ve kullanıcı kimlik doğrulama cihazı kullanıcıyı doğrulamak için çıkarılabilir güvenlik cihazını kullanır (örneğin çıkarılabilir güvenlik cihazının bir kullanıcı PIN kodunu veya şifresini veya kullanıcı ile ilişkili bir biyometrik olduğunu doğrulayarak).

Örneğin bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı (240) bir akıllı kart okuyucusu (391) içeren bir iletişim arayüzü (390) içerebilir ve çıkarılabilir güvenlik cihazı bir akıllı kart veya SIM (Abone Kimlik Modülü) kartı (395) içerebilir. Bazı uygulamalarda, akıllı kart ve kullanıcı kimlik doğrulama cihazı arasındaki iletişimin bazı yönleri, ISO/IEC 7816 standardı ile belirlenebilir. Bazı uygulamalarda, akıllı kart bir finans kurumu tarafından verilen bir kartı içerebilir. Bazı uygulamalarda, akıllı kart bir EMV (Europay-Mastercard-Visa) kartı içerebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kısmen veya tamamen CAP (Çip Doğrulama Programı) standardıyla uyumlu olabilir.

Bir Yanıt Mesajı Üretilmesi.

Kullanıcı kimlik doğrulama cihazı, en azından üretilen veya elde edilen dinamik güvenlik değerini içeren bir Yanıt Mesajı oluşturmak üzere uyarlanabilir. Bazı uygulamalarda Yanıt Mesajı ayrıca ek veri elemanlarını içerebilir; örneğin, kullanıcı kimlik doğrulama cihazının Kimlik Doğrulama Başlatma Mesajından çıkarıldığı bir oturum tanımlayıcısı ve/veya bir kullanıcı kimlik doğrulama cihazı tanımlayıcısı (kullanıcı kimlik doğrulama cihazının seri numarası gibi) ve/veya bir kullanıcı tanımlayıcısı (örneğin, bir kullanıcı ID veya kullanıcı adı) ve/veya bir uygulama tanımlayıcısı ve/veya bir tek seferlik anahtar. Bazı uygulamalarda kullanıcı kimlik doğrulama cihazı, Yanıt Mesajını tamamen veya kısmen şifrelemek üzere uyarlanabilir.

Yanıt mesajını kullanıcı veya kimlik doğrulama sunucusu için kullanılabilir hale getirmek.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, Yanıt Mesajını kullanıcıya sunmak için uyarlanabilir, böylece kullanıcı, Yanıt Mesajını kimlik doğrulama sunucusuna iletebilir (örneğin, Yanıt Mesajını erişim cihazına kopyalayarak bu cihaz Yanıt Mesajını doğrudan kimlik doğrulama sunucusuna veya kimlik doğrulama sunucusuna dönüşte iletebilecek uygulama sunucusuna iletebilir). Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, örneğin Yanıt Mesajını, kullanıcının erişim cihazına, okuyabileceği ve kopyalayabileceği sayısal veya onaltılık veya alfanümerik rakam veya karakter dizisi olarak gösterilecek şekilde uyarlanabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, örneğin, kullanıcının duyabileceği ve erişim cihazına kopyalayabileceği bir dizi sayısal veya onaltılık veya alfanümerik rakamları veya karakterleri temsil eden sentezlenmiş konuşma parçacıklarının bir dizisini yaymak üzere uyarlanabilir.

Bazı uygulamalarda kullanıcı kimlik doğrulama cihazı, Yanıt Mesajını bir hedef sunucuya göndermek üzere uyarlanabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kablosuz veri iletişim arayüzünü kullanarak bir kablosuz iletişim ağı (örneğin bir mobil telefon şebekesi gibi) üzerinden bir hedef sunucuya bir Yanıt Mesaj ıgönderecek şekilde uyarlanabilir. Bazı uygulamalarda kimlik doğrulama cihazı örneğin bir SMS (Kısa Mesaj Servisi) vasıtasıyla Yanıt Mesajını göndermek üzere uyarlanabilir veya örneğin bir kablosuz IP bağlantısı üzerinden örneğin HTTP İletim mesajı formunda Yanıt Mesajının gönderilmesi için uyarlanabilir.

Kullanıcı kimlik doğrulama cihazlarının türleri.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı özel bir donanım güvenlik cihazı olabilir. Bu bağlamda özel bir donanım güvenlik cihazının birincil işlevi bir Kimlik Doğrulama Başlatma Mesajı alıp işlemesi ve yanıt olarak dinamik bir güvenlik değeri oluşturmasıdır. Bu ayrıca, cihazın, kriptografik anahtarlar ve/veya PIN değerleri gibi şifrelerin güvenli bir şekilde depolanması için uyarlanmış bir depolama bileşeni ve uygulama sabit bellenimin değiştirilemediği veya güncellenemediği veya sadece cihaz bellenimi güncellemesinin doğruluğunu cihaza kanıtlamak için kriptografik mekanizmalar kullanan bellenim güncelleme protokolleri kullanılarak değiştirilebileceği veya güncellenebileceği anlamına gelir.

Diğer uygulamalarda, kullanıcı kimlik doğrulama cihazı, birincil fonksiyonu bir Kimlik Doğrulama Başlatma Mesajını almak ve işlemek ve yanıt olarak dinamik bir güvenlik değeri üretmek olmayan, kullanıcı tarafından yazılım uygulamalarının ücretsiz eklenmesine veya güncellenmesine olanak tanıyan bir cihaz içerebilir. Örneğin, kullanıcı kimlik doğrulama cihazı bir akıllı telefon içerebilir.

Bir uygulamayı güvenli hale getirme yöntemi.

Şekil 4a ve 4b, bir kullanıcı tarafından erişilen, örneğin şekil 2 ile ilgili olarak tartışılan sistem gibi bir sistemi kullanan uzaktan erişilebilen bir uygulamayı emniyete almak için bir yöntemi (400) göstermektedir.

Yöntem, aşağıdaki adımları içermektedir.

Kullanıcının uygulama ile başlangıç etkileşimi

Bir ilk adımda, bir uygulama sunucusu tarafından barındırılan uzaktan erişilebilen bir uygulama, kullanıcı tarafından uygulamaya veri ve mesajlar, uygulamaya erişmek ve bunlarla etkileşime girmek için kullandığı bir erişim cihazı ile değiştirilerek (410) bir kullanıcı ile etkileşime girer. Örneğin, uygulama erişim cihazından bir erişim talebi alabilir veya uygulama, kullanıcı tarafından sunulan işlem verilerini (örneğin bir işlem talep mesajında) erişim cihazından alabilir. Bazı uygulamalarda uygulama, bir web-tabanlı uygulamadır ve uygulama, örneğin HTTP mesajlarını değiştirerek erişim

cihazındaki bir web-tarayıcısı ile etkileşir. Bir noktada uygulama, kullanıcının veya kullanıcının gönderdiği verilerin doğrulanmasını gerektirebilir. Bazı uygulamalarda, kullanıcı, (talep edilen veya varsayılan) kimliğini, kimlik doğrulama işleminin başlamasından önce uygulamaya iletmiş olabilir. Diğer uygulamalarda uygulama, kullanıcı tanımlanmadan önce kimlik doğrulama işlemini başlatır. Örneğin, bazı uygulamalarda kullanıcı, kullanıcının kullanıcı adını veya giriş adını veya hesap numarasını içeren bir erişim isteği gönderebilir. Diğer uygulamalarda, kullanıcı, kullanıcı kimliğinin bir belirtisini içermeyen bir anonim erişim isteği gönderebilir.

Kimlik Doğrulama Başlatma İletisi (420) elde etme ve üretme.

Takip eden bir adımda, uygulama bir dizi veri elemanını (421) toplayabilir ve bu veri elemanlarını bir Kimlik Doğrulama Başlatma Mesajında birleştirebilir. Uygulama, örneğin doğrulanması gereken bir kimlik sorma ve/veya işlem verisi (ve kullanıcı doğrulama cihazı tarafından onay için kullanıcıya sunulması gerekebilir) ve/veya bir oturum tanımlayıcısı ve/veya bir uygulama tanımlayıcısı (kullanıcı tarafından uygulamayı tanımlamak için kullanılabilir ve kullanıcı doğrulama cihazı tarafından onay için kullanıcıya sunulabilir) ve/veya bir sunucu kimlik bilgisi (Kimlik Doğrulama Başlatma Mesajının kaynağını ve/veya içeriğini doğrulamak için kullanıcı doğrulama cihazı tarafından doğrulanabilir) ve/veya bir yanıt veya hedef adresi (bir Yanıt Mesajı gönderirken kullanıcı doğrulama cihazı tarafından kullanılabilecek) ve/veya bir tek seferlik anahtar (örneğin bir sunucu kimlik doğrulama doğrulama anahtarı veya bir dinamik güvenlik değeri oluşturma anahtarı gibi gizli kriptografik anahtarlarının türetilmesi için kullanıcı doğrulama cihazı tarafından kullanılabilecek) ve/veya bir kullanıcı tanımlayıcısı (örneğin, kullanıcının bir erişim veya giriş isteğinde sağlandığı bir kullanıcı adı) toplayabilir. Bu veri elemanlarının bir kısmı veya tamamı uygulama tarafından oluşturulmuş olabilir. Bu veri elemanlarının bir kısmı veya tamamı başka bir varlık tarafından oluşturulmuş olabilir ve bu varlıktan başvuruyla elde edilmiş olabilir. Bu varlık, örneğin, başvuru tarafından güvenilen bir kimlik doğrulama sunucusu olabilir. Güvenilir bir kimlik doğrulama sunucusu gibi başka bir varlık tarafından uygulama için oluşturulmuş ve sağlanmış olabilen veri elemanlarının örnekleri aşağıdakileri içerebilir: bir kimlik sorma ve/veya bir oturum tanımlayıcısı ve/veya bir sunucu kimlik bilgisi ve/veya tek seferlik bir anahtar. Bazı uygulamalarda aynı veri elemanı birden fazla işleve sahip olabilir. Örneğin, bazı uygulamalarda, tek bir veri elemanı, kimlik sorma, oturum tanımlayıcısı ve tek seferlik bir anahtar fonksiyonunu birleştirebilir.

Bazı uygulamalarda veri elemanlarının toplanması ve/veya bunların bir Kimlik Doğrulama Başlatma Mesajının üretilmesi için kullanılması, tamamen uygulama sunucusu üzerindeki uygulama tarafından yapılabilir. Bazı uygulamalarda veri elemanlarının toplanması ve/veya bir Kimlik Doğrulama Başlatma Mesajının üretilmesi için kullanılması, kısmen uygulama sunucusu üzerindeki uygulama tarafından yapılabilir ve kısmen erişim cihazındaki uygulamanın kontrolü altında yapılabilir (örneğin bir java uygulaması veya uygulama ile ilişkili bir tarayıcı eklentisi). Bazı uygulamalarda veri elemanlarının toplanması ve/veya bir Kimlik Doğrulama Başlatma Mesajının üretilmesi için bunların kullanılması, erişim cihazındaki uygulamanın kontrolü altında tamamlanabilir (örneğin, bir java uygulaması veya uygulama ile bağlantılı bir tarayıcı eklentisi gibi bir uygulama tarafından). Bazı uygulamalarda, Kimlik Doğrulama Başlatma Mesajının tamamı, güvenilir bir kimlik doğrulama sunucusu gibi başka bir varlık tarafından oluşturulabilir ve uygulamaya sunulur (örneğin, oluşturulan Kimlik Doğrulama İletisi Gönderme uygulamasını uygulamayı barındıran uygulama sunucusuna göndererek veya uygulama sunucusu ile etkileşim kuran erişim cihazına göndererek). Örneğin bazı uygulamalarda, uygulama sunucusu tüm veri elemanlarını toplayabilir ve bir Kimlik Doğrulama Başlatma Mesajı oluşturabilir ve erişim cihazına gönderebilir. Bazı uygulamalarda, uygulama sunucusu tüm veri elemanlarını toplayabilir ve bunları, bu veri elemanları (örneğin, bir java uygulaması veya uygulama ile bağlantılı bir tarayıcı eklentisi gibi bir uygulama tarafından) kullanılarak Kimlik Doğrulama Başlatma Mesajının üretildiği erişim cihazına gönderebilir. Bazı uygulamalarda, uygulama sunucusu bazı veri elemanlarını toplayabilir ve bunları erişim cihazına gönderebilir ve erişim cihazı bazı diğer veri elemanlarını toplayabilir ve bu veri elemanlarını (örneğin bir java uygulaması veya uygulama ile ilişkili bir tarayıcı eklentisi) kullanan erişim cihazında Kimlik Doğrulama Başlatma Mesajı oluşturulur. Bazı uygulamalarda, bir kimlik doğrulama sunucusu gibi başka bir varlık tüm veri elemanlarını toplayabilir ve Kimlik Doğrulama Başlatma Mesajını oluşturabilir ve bunu uygulama sunucusuna (erişim cihazına iletebilir) gönderebilir veya doğrudan erişim cihazına gönderebilir.

Sunucu kimlik bilgisi üretme (422)

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı bir sunucu kimlik bilgisini içerir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, bir gizli anahtar ile

parametrelenmiş bir kriptografik algoritma kullanılarak oluşturulabilir. Bazı uygulamalarda, sunucu kimlik doğrulaması kimlik doğrulama sunucusu tarafından oluşturulur. Sunucu kimlik bilgisi, Kimlik Doğrulama Başlatma Mesajında yer alan veri elemanlarının en azından bir kısmının kriptografik olarak bağlanması ve/veya doğrulanması için kullanılabilir. Örneğin, bazı uygulamalarda sunucu kimlik bilgisi, Kimlik Doğrulama Başlatma Mesajında yer alan bir uygulama tanımlayıcısının ve/veya işlemle ilgili verilerin doğrulanması için kullanılabilir. Bazı uygulamalarda, sunucu kimlik bilgisi, örneğin Kimlik Doğrulama Başlatma Mesajında yer alan bir sunucu tarafından üretilen dinamik güvenlik değerinin kriptografik olarak bir uygulama tanımlayıcısına ve/veya Kimlik Doğrulama Başlatma Mesajında da yer alan işlemle ilgili verilere bağlanması için kullanılabilir. Bazı uygulamalarda sunucu kimlik doğrulaması Kimlik Doğrulama Başlatma Mesajının şifreli bir bölümünü içerir. Uygulamalarda sunucu kimlik bilgisi, şifrelenmiş Kimlik Doğrulama Başlatma Mesajının tamamını içerir. Bazı uygulamalarda sunucu kimlik bilgisi, en az bir sunucu tarafından oluşturulan dinamik güvenlik değeri içeren Kimlik Doğrulama Başlatma Mesajının şifrelenmiş bir bölümünü içerir.

Erişim cihazında bir Kimlik Doğrulama Başlatma Mesajının temsilini kodlayan bir sinyalin yayılması (430).

Erişim cihazı, Kimlik Doğrulama Başlatma Mesajını veya yukarıda daha ayrıntılı olarak açıklandığı gibi bir temsilini elde edebilir. Kimlik Doğrulama Başlatma Mesajını veya bir temsilini aldıktan sonra, erişim cihazı Kimlik Doğrulama Başlatma Mesajını kodlayan bir sinyal yayar. Erişim cihazı, yukarıda daha ayrıntılı olarak tarif edildiği gibi kullanıcı çıkış arayüzünü kullanarak bu sinyal verebilir.

Kimlik Doğrulama Başlatma Mesajını (435) elde etmek için Kullanıcı kimlik doğrulama cihazında yayılan sinyali yakalama ve şifresini çözme.

Kimlik Doğrulama Başlatma Mesajını kodlayan sinyal, erişim cihazı tarafından yayıldığında, yukarıda daha ayrıntılı olarak tarif edildiği gibi kullanıcı kimlik doğrulama cihazı tarafından yakalanabilir. Kimlik Doğrulama Başlatma Mesajının daha sonra yukarıda daha detaylı olarak tarif edildiği gibi yakalanan sinyalden kullanıcı kimlik doğrulama cihazı tarafından şifresi çözülebilir.

Kimlik Doğrulama Başlatma Mesajının İşlenmesi ve Yanıt İletisi Üretimi (440)

Kimlik Doğrulama Başlatma Mesajı, kullanıcı kimlik doğrulama cihazı tarafından alındıktan sonra, işlenebilir ve kullanıcı kimlik doğrulama cihazı tarafından bir dinamik güvenlik değeri içeren bir Yanıt Mesajı üretilebilir.

Kimlik Doğrulama Başlatma Mesajı, içeriğinin elde edilmesi için işlenebilir ve eğer uygulanabilirse (örneğin, Kimlik Doğrulama Başlatma Mesajının bir sunucu kimlik bilgisi içermesi durumunda), yukarıda daha ayrıntılı olarak açıklandığı gibi içeriğini veya kimliğini doğrular.

Sunucu kimlik doğrulaması (441)

Uygulanabilirse (örneğin, Kimlik Doğrulama Başlatma Mesajı bir sunucu kimlik bilgisi içeriyorsa), yukarıda daha ayrıntılı olarak açıklandığı şekilde kimliği veya içeriğini doğrulamak için işlenebilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, bir sunucu kimlik bilgisi içerebilir ve bu sunucu kimlik bilgisi, yukarıda daha ayrıntılı olarak açıklanan, örneğin Kimlik Doğrulama Başlatma Mesajının veya içeriğinin bir kısmının kimliğini doğrulamak için kullanıcı kimlik doğrulama cihazı tarafından doğrulanabilir. Sunucu kimlik doğrulaması başarısız olursa, kullanıcı kimlik doğrulama cihazı kimlik doğrulama işleminin diğer adımlarını iptal edebilir. Böyle bir durumda kullanıcı kimlik doğrulama cihazı kullanıcıyı hatadan haberdar edebilir.

Uygulama kimlik sunumu (442)

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kullanıcı kimlik doğrulama cihazının, uygulama kimliğinin bir temsilini elde etmek için kullandığı bir uygulama tanımlayıcısını içerir. Uygulama kimliğinin temsili, kullanıcı çıkış arayüzü vasıtasıyla kullanıcıya sunulabilir ve kullanıcının, kullanıcı kimlik doğrulama cihazı tarafından, uygulama kimliğinin sunulmuş temsilinin onayı alınabilir. Onay, kimlik doğrulama sürecinin daha ileri adımlarında kullanılabilir.

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kimlik doğrulama sunucusu tarafından sunucu kimlik bilgisinin üretildiği ve kimlik doğrulama işleminin yapıldığı Kimlik Doğrulama Başlatma Mesajında yer alan en az uygulama tanımlayıcısının

kimliğini doğrulayan bir sunucu kimlik bilgisinin yanı sıra bir uygulama tanımlayıcısı da içerebilir, sunucu, uygulama tanımlayıcısının, sunucu kimlik bilgisini oluşturduğu uygulamanın kimliğiyle eşleştiğini doğrulamış olabilir, böylece kullanıcı, Kimlik Doğrulama Başlatma Mesajının gerçekten, uygulama tanıtıcısıyla ilişkili uygulamadan kaynaklandığından emin olabilir.

İşlem Verilerinin Sunulması (443)

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kullanıcı tarafından kullanıcı kimlik doğrulama cihazı tarafından kullanıcı tarafından incelenecek ve/veya onaylanacak kullanıcı çıkış arayüzü vasıtasıyla sunulabilecek bir veya daha fazla işleme ilişkin veri elemanını içerebilir. Kullanıcının sunulan işlemle ilgili verileri onayı, kullanıcı kimlik doğrulama cihazı tarafından yakalanabilir. Onay, kimlik doğrulama işleminin daha ileri adımlarında kullanılabilir.

PIN girişi (444)

Bazı uygulamalarda kullanıcıdan, kullanıcı kimlik doğrulama cihazı tarafından bir PIN veya şifre sağlaması istenebilir ve kullanıcı kimlik doğrulama cihazı, kullanıcının yukarıda açıklandığı gibi sağladığı ve kullanacağı PIN veya şifreyi yakalayabilir. Bazı uygulamalarda, kullanıcının bir PIN veya şifre girişi, dahili bir onay görevi görür. Örneğin, kullanıcı kimlik doğrulama cihazı tarafından, kullanıcı kimlik doğrulama cihazının kullanıcı tarafından kimlik doğrulama işleminde bu noktaya kadar sunulmuş olan veri elemanlarının veya mesajlarının (örneğin uygulama kimliğini veya işlemle ilgili verileri temsil eden) onayı olarak kabul edilebilir veya kullanıcı kimlik doğrulama cihazının bir dinamik güvenlik değerinin üretilmesi ve/veya Yanıt Mesajının üretilmesi ve/veya bir Yanıt Mesajının bir hedef sunucuya gönderilmesi için kullanıcının onayı olarak kabul edilebilir.

Kullanıcı onayının alınması (445).

Bir veya daha fazla dahili veya açık kullanıcı onayı, kullanıcı kimlik doğrulama cihazı tarafından istenebilir (örneğin, kimlik doğrulama sürecine devam etmek için bir onay veya uygulama kimliğinin onaylanması veya işlemle ilgili tarihin onaylanması). Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı açık bir şekilde kullanıcının bir onay

vermesini ister (örneğin "aşağıdaki işlem verilerini onaylıyor musunuz?" veya "aşağıdaki uygulamaya şimdi erişmek ister misiniz?" gibi bir mesajı görüntülemek) ve açıkça kullanıcıya onaylama veya raporlama (örneğin: "evet/hayır" veya "devam et/iptal et") seçimini sunar ve kullanıcı açıkça bir seçim yaparak ve kullanıcı kimlik doğrulama cihazına uygun seçimi açıkça belirterek onay verebilir. Bazı uygulamalarda kullanıcı, onayını dahili bir şekilde gösterir. Örneğin, normal kullanıcı etkileşimi, incelenecek belirli veri veya mesajlarla sunulduğunda veya örneğin belirli veri veya mesajlar kullanıcıya sunulduğunda bir PIN veya şifre girerek (iptal etmek yerine) devam ettirmek suretiyle.

Kimlik doğrulama işleminde kullanıcı onaylarının kullanımı ve doğrulanması.

Kimlik doğrulama işleminin devam etmesi, bu kullanıcı onaylarının bir veya daha fazlasına bağlı olabilir ve kullanıcı tarafından onayların bir veya daha fazlası sağlanmıyorsa veya kullanıcı onaylamazsa, kimlik doğrulama işlemi bir noktada iptal edilebilir. Örneğin bazı uygulamalarda, dinamik güvenlik değerinin oluşturulması ve/veya dinamik güvenlik değerini içeren Yanıt Mesajının üretilmesi, kullanıcı onayı başarısız olduğunda iptal edilebilir. Bazı uygulamalarda, gerekli kullanıcı onayları elde edilmemişse, kullanıcı kimlik doğrulama cihazı üretilen Yanıt Mesajını bir hedef sunucuya göndermeyebilir veya Yanıt Mesajını kullanıcıya göstermeyebilir.

Bazı uygulamalarda kullanıcı onayları, Yanıt Mesajında dahili olabilir, çünkü bunlar kullanıcı kimlik doğrulama cihazının dinamik güvenlik değerini ve / veya Yanıt Mesajını oluşturması için veya Yanıt Mesajını sunmak için kullanıcı kimlik doğrulama cihazı için veya Yanıt Mesajını bir hedef sunucuya göndermek için gerekli bir koşuldur. Bu tür uygulamalarda, dinamik güvenlik değerini doğrulayan kimlik doğrulama sunucusu, kullanıcı, gerekli onayları sağlamazsa, kimlik doğrulama sunucusunun geçerli bir dinamik güvenlik değerine sahip bir Yanıt Mesajı almadığı için dinamik güvenlik değerini doğrulayarak kullanıcı onaylarını dolaylı olarak doğrulayabilir.

Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değerinin kriptografik hesaplanmasında kullanıcı onaylarını (veya bunların eksikliğini) belirten veri elemanlarını içerir ve bu Yanıt Mesajında bu veri elemanlarını içerebilir veya içermeyebilir. Örneğin, kullanıcı kimlik doğrulama cihazı, kullanıcının belirli bir onay vermesi istenip istenmediğini ve/veya kullanıcının gerçekten bu onayı sağlayıp

sağlamadığını belirten bit işaretlerini içeren bir veri elemanı kullanabilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değerini üretmek için kriptografik algoritma için girdi olarak kullanıcı onaylarının göstergesi olan ve bu veri elemanlarını da Yanıt Mesajının içeriğinde de içerebilen bu veri elemanlarını içerebilir. Yanıt Mesajını alan bir doğrulama hizmeti, bu veri elemanlarının kullanıcının onayları açısından tatmin edici bir durumu gösterip göstermediğini doğrulayabilir ve aynı Yanıt Mesajında yer alan dinamik güvenlik değerinin bu veri elemanlarıyla tutarlı olup olmadığını kriptografik olarak doğrulayabilir. Diğer uygulamalarda, kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değerini oluşturmak için kriptografik algoritma için girdi olarak kullanıcı onaylarının göstergesi olan veri elemanlarını içerebilir, ancak bu veri elemanlarını da Yanıt Mesajının içeriğine dahil etmeyebilir. Yanıt Mesajını alan bir doğrulama hizmeti, Yanıt mesajı olarak kabul edilmek için zorunlu olan bu veri elemanları için belirli değerler alabilir (örneğin kullanıcının gerekli tüm onayları sağladığını belirten değerler) ve aynı Yanıt Mesajında bulunan dinamik güvenlik değerinin., bu veri elermanları için bu varsayılan değerler ile tutarlı olup olmadığını kriptografik olarak doğrulayabilir.

Dinamik güvenlik değeri üretme (449)

Kullanıcı kimlik doğrulama cihazı bir dinamik güvenlik değeri üretmek için gerekli olan tüm veri elemanlarını elde ettikten sonra, dinamik güvenlik değeri yukarıda tarif edildiği gibi üretilebilir.

Kullanıcı kimlik doğrulama cihazı tarafından dinamik güvenlik değerinin üretilmesi, belirli doğrulamalar ve/veya olaylara koşullu olabilir. Örneğin, Kimlik Doğrulama Başlatma Mesajında yer alan bir sunucu kimlik bilgisinin başarılı bir şekilde doğrulanmasına bağlı olabilir veya kullanıcının belirli onayları sağlaması koşuluyla koşula bağlı olabilir veya kullanıcı tarafından girilen bir PIN veya şifrenin başarılı bir şekilde doğrulanmasına bağlı olabilir.

Bir yanıt mesajı oluşturma (450)

Yukarıda tarif edildiği gibi, dinamik güvenlik değerini içeren kullanıcı kimlik doğrulama cihazı tarafından bir Yanıt Mesajı oluşturulabilir. Yanıt Mesajı ayrıca, örneğin uygulama kimliği ile ilgili bir veri elemanı ve/veya bir oturum tanımlayıcısı ve/veya bir kullanıcı

tanımlayıcısı (kullanıcı kimlik doğrulama cihazında depolanabilir veya Kimlik Doğrulama Başlatma Mesajından çıkartılmış veya kullanıcı tarafından kullanıcı kimlik doğrulama cihazına sağlanmış olabilir) ve/veya bir kullanıcı kimlik doğrulama cihazı tanımlayıcısı (bir seri numarası gibi kullanıcı kimlik doğrulama cihazında depolanabilir) ve/veya kullanıcı onaylarını gösteren işaretler gibi diğer veri elemanlarını da içerebilir.

Yanıt Mesajının kullanıcı kimlik doğrulama cihazı tarafından oluşturulması, belirli doğrulamalar ve/veya olaylara bağlı olabilir. Örneğin, Kimlik Doğrulama Başlatma Mesajında yer alan bir sunucu kimlik bilgisinin başarılı bir şekilde doğrulanmasına bağlı olabilir veya kullanıcının belirli onayları sağlaması koşuluyla koşula bağlı olabilir veya kullanıcı tarafından girilen bir PIN veya şifrenin başarılı bir şekilde doğrulanmasına bağlı olabilir.

Yanıt mesajının bir doğrulama sunucusuna sağlanması (460).

Oluşturulan Yanıt Mesajı daha sonra kimlik doğrulama sunucusu gibi bir doğrulama sunucusuna iletilebilir.

Yanıt Mesajının kullanıcıya sunulması (461).

Bazı uygulamalarda, Yanıt Mesajı, kullanıcı çıktı arayüzü vasıtasıyla kullanıcıya kullanıcı kimlik doğrulama cihazı tarafından sunulur, ardından kullanıcı, Yanıt Mesajını doğrudan doğrulama sunucusuna Yanıt Mesajı'nı gönderebilecek olan erişim cihazın kopyalayabilir, örneğin kimlik doğrulama sunucusu gibi doğrulama sunucusu veya doğrulama sunucusuna iletebilen uygulama sunucusuna gönderebilir.

Yanıt Mesajının kullanıcı kimlik doğrulama cihazı tarafından sunulması, belirli doğrulamalar ve/veya olaylara bağlı olabilir. Örneğin, Kimlik Doğrulama Başlatma Mesajında yer alan bir sunucu kimlik bilgisinin başarılı bir şekilde doğrulanmasına bağlı olabilir veya kullanıcının belirli onayları sağlaması koşuluyla koşula bağlı olabilir veya kullanıcı tarafından girilen bir PIN veya şifrenin başarılı bir şekilde doğrulanmasına bağlı olabilir.

Yanıt Mesajının bir hedef sunucuya gönderilmesi (465).

Bazı uygulamalarda, Yanıt Mesajı bir veri iletişim arayüzü kullanılarak kullanıcı kimlik doğrulama cihazı tarafından bir hedef sunucuya (örneğin uygulama sunucusu veya kimlik doğrulama sunucusu olabilir) gönderilir. Bazı uygulamalarda bu veri iletişim arayüzü, bir kablosuz veri iletişim arayüzü içerir. Bazı uygulamalarda, bu kablosuz veri iletişim arayüzü, bir GSM veya UMTS ağı gibi bir ortak mobil iletişim ağı üzerinden veri mesajlarını göndermek için bir arayüz içerir.

Bazı uygulamalarda, hedef sunucunun hedef adresi kullanıcı kimlik doğrulama cihazında saklanır. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, Kimlik Doğrulama Başlatma Mesajından çıkarılan hedef adrese bağlı bir veri elemanı kullanılarak hedef adresi belirleyebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı belirlenen hedef adrese izin verilip verilmediğini doğrular. Örneğin, belirlenen hedef adresi yasak adreslerin kara listesi veya izin verilen adreslerin beyaz listesi ile karşılaştırılabilir veya birtakım kurallara uyup uymadığını doğrulayabilir.

Yanıt Mesajının, kullanıcı kimlik doğrulama cihazı tarafından belirlenen hedef adres tarafından belirtilen bir hedef sunucuya gönderilmesi, belirli doğrulamalar ve/veya olaylara bağlı olabilir. Örneğin, Kimlik Doğrulama Başlatma Mesajında yer alan bir sunucu kimlik bilgisinin başarılı bir şekilde doğrulanmasına bağlı olabilir veya kullanıcının belirli onayları sağlaması koşuluyla koşula bağlı olabilir veya kullanıcı tarafından girilen bir PIN veya şifrenin başarılı bir şekilde doğrulanmasına bağlı olabilir.

Yanıt mesajının doğrulanması (470).

Doğrulama sunucusunda Yanıt Mesajı alındıktan sonra, doğrulanabilir. Yanıt Mesajının doğrulanması çeşitli adımlar içerebilir ve doğrulama bölümleri uygulama sunucusu tarafından yapılabilir ve doğrulama bölümleri kimlik doğrulama sunucusu tarafından yapılabilir.

Bazı uygulamalarda, Yanıt Mesajının doğrulanmasının bir bölümü, Yanıt Mesajındaki belirli veri elemanlarının değerlerinin kabul edilebilir değerlere sahip olup olmadığını içerir. Bazı uygulamalarda bu, bu değerlerin bazılarının belirli bir aralık içinde olduğunun doğrulanmasını içerebilir. Bazı uygulamalarda bu, bu değerlerden bazılarının sınırlı sayıda izin verilebilir değerden birine sahip olduğunu doğrulamayı içerebilir. Örneğin bazı uygulamalarda Yanıt Mesajı, kullanıcının belirli veri elemanlarını

onayladığını veya onaylamadığını gösteren işaretler içerebilir ve doğrulama işleminin bir bölümü bu işaretlerin kullanıcının gerçekten onay verdiğine işaret ettiğini doğrulamayı içerebilir. Bazı uygulamalarda Yanıt Mesajı, kullanıcıya sunulan bir uygulama tanımlayıcısının temsiliyle ilgili bir veri elemanı içerebilir ve Yanıt Mesajının doğrulanması, kullanıcının gözden geçirmesi gereken uygulama tanımlayıcısının temsiline karşılık gelen bu veri elemanının değerinin doğrulanmasını içerir. Örneğin, bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kullanıcı kimlik doğrulama cihazı tarafından geri alınan ve kullanıcıya sunulan bir uygulama logosunu sunan bir URL içerebilir. Bu uygulamaların bazılarında Kimlik Doğrulama Başlatma Mesajı ve/veya logoyu geri alma işlemi kriptografik olarak güvence altına alınmamakta, böylece kullanıcıya yanlış bir logo sunumunun dışlanması mümkün olmamaktadır. Kullanıcıya yanlış bir logonun sunulup sunulmadığını saptamak için, bu tür uygulamalardaki kullanıcı kimlik doğrulama cihazı, Yanıt Mesajında (ve ayrıca dinamik güvenlik değerinin hesaplanmasında), örneğin kullanıcıya etkili bir şekilde sunulan logonun bir sağlamasını içerebilir. Yanıt mesajının doğrulanması, bu sağlama değerinin kullanıcıya sunulması gereken logoya karşılık gelebilmesini içerebilir. Bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcıdan bazı girişler yakalayabilir ve Yanıt Mesajında (ve muhtemelen dinamik güvenlik değerinin hesaplanmasında). Örneğin, bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, kullanıcıdan uygulama veya kimlik doğrulama sunucusu tarafından bilinebilecek bir PIN veya şifre girmesini isteyebilir ve Yanıt Mesajında (muhtemelen Yanıt Mesajının şifrelenmiş bir bölümünde) PIN veya şifreyi temsil eden bir veri elemanını içerebilir. Yanıt Mesajının doğrulanmasının bir bölümü, uygun sunucu tarafından bu PIN veya şifre ile ilgili veri elemanının değerini doğrulamayı içerebilir.

Yanıt Mesajının Doğrulanması, dinamik güvenlik değerinin doğrulanmasını da içerebilir (475).

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, sunucu tarafından oluşturulan bir dinamik güvenlik değeri içerebilir ve Yanıt Mesajındaki dinamik güvenlik değerinin doğrulanması, Yanıt Mesajında alınan dinamik güvenlik değerinin sunucu tarafından oluşturulan dinamik güvenlik değeriyle karşılaştırılmasını içerebilir.

Bazı uygulamalarda, dinamik güvenlik değerinin doğrulanması, dinamik güvenlik değerinin kriptografik geçerliliğinin doğrulanmasını içerir.

Bazı uygulamalarda, bu, kullanıcı kimlik doğrulama cihazı tarafından dinamik güvenlik değerinin hesaplanmasında kullanıldığı varsayılan veri elemanları için referans değerlerinin belirlenmesini içerir. Bazı uygulamalarda: bu veri elemanlarından bazılarının referans değerlerinin kaynağı, Yanıt Mesajı (örneğin kullanıcı onay işaretleri ve/veya uygulama kimliği ile ilgili veriler) olabilir. Bazı uygulamalarda, bu veri elemanlarından bazılarının referans değerlerinin kaynağı, uygulama sunucusu olabilir (örneğin, uygulamanın Kimlik Doğrulama Başlatma Mesajında yer alan ve Yanıt Mesajında yer almayan, ancak dinamik güvenlik değerinin hesaplanmasında girdi olarak kullanılan bir kimlik sorma veya örneğin işlemle ilgili veriler). Bazı uygulamalarda, bu veri elemanlarından bazılarının referans değerlerinin kaynağı kimlik doğrulama sunucusu (örneğin, kimlik doğrulama sunucusu tarafından orijinal olarak sağlanan bir kimlik sorma değeri) olabilir. Bazı uygulamalarda, belirli veri elemanlarının referans değerlerinin belirlenmesi varsayımlara dayanabilir. Örneğin, bazı uygulamalarda, kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değerinin hesaplanmasında sayaç ile ilgili bir değer kullanabilir ve doğrulama sunucusu bu sayacın ilgili değerinin bir kopyasını tutabilir ve kullanıcı kimlik doğrulama cihazının kullanılacağı varsayılan değerini belirlemek için bir senkronizasyon algoritması kullanabilir veya kullanıcı kimlik doğrulama cihazı dinamik güvenlik değerinin hesaplanmasında zamana bağlı bir değer kullanır ve doğrulama sunucusu, yanıt mesajının alınma zamanına bağlı olarak bu zamana bağlı değeri tahmin edebilir.

Bazı uygulamalarda, dinamik güvenlik değerinin kriptografik doğrulaması, bir kriptografik doğrulama anahtarının geri alınmasını içerir. Bazı uygulamalarda bu doğrulama anahtarı, kullanıcı kimlik doğrulama cihazı ile ilişkilendirilir ve Yanıt Mesajında yer alan bir kullanıcı kimlik doğrulama cihazı tanımlayıcısı kullanılarak geri alınabilir. Bazı uygulamalarda, bu doğrulama anahtarı kullanıcıyla ilişkilendirilir ve Yanıt Mesajında yer alan bir kullanıcı tanımlayıcısı kullanılarak geri alınabilir. Bazı uygulamalarda doğrulama anahtarının geri alınması, bir kullanıcı tanımlayıcısı veya bir kullanıcı kimlik doğrulama cihazı tanımlayıcısı ile ilgili veri elemanını arama endeksi olarak kullanarak bir veritabanında bir arama yapılmasını içerebilir. Bazı uygulamalarda doğrulama anahtarının geri alınması, bir kullanıcı tanımlayıcısı veya bir kullanıcı kimlik doğrulama cihazı tanımlayıcısı ile ilgili veri elemanını türetme veya çeşitlendirme çekirdeği olarak kullanan bir ana anahtardan bir anahtar türetme veya çeşitlendirme yapmayı içerebilir.

Bazı uygulamalarda, dinamik güvenlik değerinin kriptografik doğrulamasında kullanılan bir doğrulama anahtarı, dinamik güvenlik değerinin hesaplanmasında kullanıcı kimlik doğrulama cihazı tarafından da kullanılan bir gizli simetrik anahtar içerir. Bazı uygulamalarda, dinamik güvenlik değerinin kriptografik olarak doğrulanmasında kullanılan bir doğrulama anahtarı, özel anahtarın, kullanıcı kimlik doğrulama cihazı tarafından dinamik güvenlik değerinin hesaplanmasında kullanıldığı bir ortak-özel anahtar çiftinin ortak anahtarını içermektedir. Bazı uygulamalarda, alınan dinamik güvenlik değerinin kriptografik doğrulaması, yukarıda belirtilen kriptografik doğrulama anahtarını kullanarak yukarıda söz konusu referans değerlerine bir kriptografik algoritmanın uygulanmasını ve bu kriptografik işlemin sonucunun alınan dinamik güvenlik değeriyle karşılaştırılmasını içerir. Örneğin, bazı uygulamalarda, alınan dinamik güvenlik değerinin kriptografik doğrulaması, yukarıda belirtilen referans değerleri üzerinde bir anahtarlı sağlama veya bir MAC'nin hesaplanmasını içerebilir (burada anahtarlı sağlama veya MAC algoritması, aşağıdaki gibi yukarıda tarif edilen geri alınabilen bir gizli simetrik doğrulama anahtarı ile parametrelendirilmiştir). Bazı uygulamalarda, alınan dinamik güvenlik değerinin kriptografik doğrulaması, yukarıda söz konusu kriptografik doğrulama anahtarını kullanarak alınan dinamik güvenlik değeri üzerinde bir kriptografik algoritmanın yürütülmesini ve bu kriptografik işlemin sonucunun yukarıda belirtilen referans değerlerle karşılaştırılmasını içerir. Örneğin, bazı uygulamalarda, alınan dinamik güvenlik değerinin kriptografik doğrulaması, dinamik güvenlik değerini oluşturmak için kullanıcı kimlik doğrulama cihazı tarafından kullanılan özel anahtara karşılık gelen ortak anahtar kullanılarak bir asimetrik şifre çözme algoritması ile dinamik güvenlik değerinin deşifre edilmesini içerir ve daha sonra şifresi çözülmüş değeri yukarıda belirtilen referans değerlerinin bir sağlaması ile karşılaştırır.

Bir doğrulama sonucunun uygulama sunucusuna iletilmesi (480).

Bazı uygulamalarda, Yanıt Mesajının doğrulanmasının en az bir kısmı güvenilir bir doğrulama sunucusu tarafından yapılır ve güvenilir kimlik doğrulama sunucusu tarafından yapılan doğrulama sonucu uygulama sunucusuna iletilir. Bazı uygulamalarda doğrulama sonucundan ayrı olarak, diğer veri elemanları uygulama sunucusuna iletilebilir. Örneğin, bazı uygulamalarda, kimlik doğrulama sunucusu, Yanıt Mesajında yer alan veri elemanlarını uygulama sunucusuna, örneğin bir oturum

tanımlayıcısı veya kullanıcı tanımlayıcısı veya kullanıcıya sunulan uygulama kimliğinin temsiliyle ilgili bir veri elemanı veya kullanıcı kimlik doğrulama cihazı (işlemle ilgili veriler gibi) tarafından kullanıcıya sunulmuş olabilecek veya kullanıcı tarafından kullanıcı kimlik doğrulama cihazına sağlanmış olabilecek diğer veri elemanları ile iletişim kuarbilir. Bir oturum tanımlayıcısı almak, uygulama sunucusunun, iletilen sonuçların hangi uygulama oturumunun geçerli olduğunu belirlemesine izin verebilir. Bir kullanıcı tanımlayıcısının alınması, uygulama sunucusunun, kullanıcı kimliğini uygulamaya manuel olarak vermek zorunda kalmadan kullanıcı genel kimliğini belirleyebilmesine ve böylece genel kullanıcı rahatlığını arttırmasına olanak sağlayabilir. Kullanıcı kimlik doğrulama cihazı tarafından kullanıcıya sunulan verilerin alınması, uygulama sunucusunun doğru verilerin kullanıcıya sunulduğunun doğrulamasına olanak tanır.

Bazı uygulamalarda, uygulama sunucusu ve kimlik doğrulama sunucusu arasındaki iletişim güvenli hale getirilebilir. Örneğin, bazı uygulamalarda, kimlik doğrulama sunucusundan uygulama sunucusuna gönderilen mesajlar, bunların yasal kimlik doğrulama sunucusundan kaynaklandığını uygulama sunucusuna göstermek için kriptografik olarak doğrulanabilir. Bazı uygulamalarda, bir uygulama sunucusundan kimlik doğrulama sunucusuna gönderilen mesajların, yasal bir uygulama sunucusundan kaynaklandığını göstermek için kriptografik olarak doğrulanabilir. Bazı uygulamalarda, mesajların içeriğinin gizliliğini garanti altına almak için bazı mesajlar şifrelenebilir. Bazı uygulamalarda, mesajların içeriklerinin bütünlüğünü garanti altına almak için bazı mesajlar kriptografik olarak (örneğin kriptografik kontroller veya imzalar ile) korunabilir.

Bazı uygulamalarda, kimlik doğrulama sunucusu uygulama sunucusunu belirleyebilir ve doğrulama sonucunu muhtemelen uygulama sunucusuna ek verilerle birlikte gönderebilir. Bazı uygulamalarda, ilave veriler, uygulama sunucusunun, doğrulama sunucusu tarafından sağlanan doğrulama sonuçlarını bir uygulama oturumuna bağlamasına olanak sağlayan verileri (bir oturum tanımlayıcısı veya bir kullanıcı tanımlayıcısı gibi) içerebilir.

Diğer uygulamalarda, uygulama sunucusu doğrulama sonucu için kimlik doğrulama sunucusunu oylayabilir. Uygulama sunucusunun kimlik doğrulama sunucusuna gönderdiği oylama isteği mesajlarında, uygulama sunucusu kimlik doğrulama

sunucusunun oylama isteğini, aldıkları Yanıt Mesajlarının doğru olanıyla eşleştirmek için kullanabileceği verileri içerebilir. Bu veriler, örneğin, Yanıt Mesajındaki karşılık gelen veri öğelerini eşleştirebilen bir oturum tanımlayıcısı veya bir kullanıcı tanımlayıcısı gibi verileri içerebilir. Bazı uygulamalarda, uygulama sunucusu, dinamik güvenlik değerinin hesaplanmasında kullanılan işlemle ilgili verilerin değerleri gibi dinamik güvenlik değerinin doğrulanması için gerekli olabilecek kimlik doğrulama sunucusu verilerine de sahiptir.

Ek kullanıcı ile ilgili verileri uygulama sunucusuna iletme (499).

Bazı uygulamalarda, güvenilir kimlik doğrulama sunucusu, Yanıt Mesajının doğrulanması için gerekli olmayan, ancak uygulamaya değer olabilecek kullanıcı ile ilgili verileri depolayabilir ve yönetebilir. Bu veriler, örneğin, kullanıcının başvuruya ilişkin kullanıcı adını, kişisel bilgileri (kullanıcının gerçek adı, fiziksel adresi ve/veya telefon numarası gibi), finansal bilgileri (kredi kartı numarası gibi) ve/veya kullanıcı profili bilgilerini içerebilir. Bazı uygulamalarda, kimlik doğrulama hizmeti, bu bilginin bir bölümünü, doğrulama sonucunun iletişimi ile birlikte uygulamaya aktarmaktadır. Bu, dinamik güvenlik değerinin başarılı bir şekilde doğrulanmasına bağlı olabilir. Bazı uygulamalarda bu, politika kurallarına ve bir kullanıcı profili konfigürasyonuna tabi olabilir. Örneğin, bazı uygulamalarda, bir kullanıcı, kullanıcı ile ilgili birçok veriyi içeren bir kimlik doğrulama sunucusuna sahip bir profile sahip olabilir ve kullanıcı, hangi verilerin hangi koşullar altında hangi uygulamaya iletilebileceğini belirtmek üzere bu profili yapılandırabilir. Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kullanıcı kimlik doğrulama cihazı tarafından kimlik doğrulama sunucusunun belirli verileri uygulama sunucusuna (örneğin kullanıcının telefon numarası veya adresi veya kredi kartı numarası gibi) ilettiğini onaylaması için kullanıcıya sunulması için bir talep içerebilir. Kullanıcı kimlik doğrulama cihazı bu talebi kullanıcıya sunabilir ve kullanıcının Yanıt Mesajında ve dinamik güvenlik değerinin hesaplanmasında kullanıcının yanıtını içerebilir. Yanıt Mesajının olumlu bir şekilde doğrulanması üzerine, kimlik doğrulama sunucusu, kullanıcının istenen verilerin serbest bırakılmasını onayladığı ve istenen verileri uygulama sunucusuna ilettiği sonucuna varabilir.

Bazı uygulamalarda, uygulama, kullanıcının belirli verileri (uygulamaya özel bir şifre gibi) sağlaması için Kimlik Doğrulama Başlatma Mesajı taleplerine veya kimlik doğrulama sunucusu tarafından saklanan belirli verilere uygulamaya yönelik talepleri

içerebilir, böylece kimlik doğrulama sunucusu, Yanıt Mesajının başarılı bir şekilde doğrulanması üzerine talep edilen verileri (diğer bir deyişle girilen veya yayınlanan bilgiler) uygulama sunucusuna iletebilir. Bu uygulamaların bazılarında, istenen tarihin, kimlik doğrulama sunucusu tarafından uygulama sunucusuna iletilmesi, kimlik doğrulama sunucusunun, kullanıcı kimlik doğrulama cihazının, kullanıcı tarafından onaylanan kullanıcıya uygulama kimliğinin bir temsilini sunduğu başarılı onayına bağlı olabilir ve kullanıcı tarafından sunulmuş ve onaylanmış olan uygulama kimliğinin temsili, gerçekten de, verileri talep eden uygulamanın kimliğiyle eşleşmektedir. Bu uygulamaların bazılarında, Kimlik Doğrulama Başlatma Mesajındaki uygulama tanımlayıcısı, Kimlik Doğrulama Başlatma Mesajında de yer alan bir sunucu kimlik bilgisi tarafından doğrulanır; böylece kullanıcı, gerçekte talep edilen verilerin talep edilen uygulamadan geldiğinden emin olabilir.

Uygulama sunucusunda doğrulama sonucunun bir fonksiyonu olarak tepki (490).

Yanıt Mesajının doğrulanmasının sonucuna bağlı olarak, uygulama uygun eylemi gerçekleştirebilir. Örneğin, başarılı bir doğrulama söz konusu olduğunda, başvuru kullanıcıya erişim izni verebilir veya verilen işlemi gerçekleştirebilir (491) ve başarısız bir doğrulama durumunda, başvuru kullanıcıya erişim izni vermeyi reddedebilir veya verilen işlemi gerçekleştirmeyebilir (492).

Uygulama kimliğinin dinamik güvenlik değerine kriptografik olarak bağlanması.

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, kullanıcıya sunduğu uygulama kimliğinin bir temsilini elde etmek için kimlik doğrulama kullanıcı cihazı tarafından kullanılan bir uygulama tanımlayıcısı içermektedir. Bazı uygulamalarda, bu uygulama tanımlayıcısı veya uygulama kimliğinin karşılık gelen temsili, kullanıcı kimlik doğrulama cihazının oluşturabileceği dinamik güvenlik değerine kriptografik olarak bağlanabilir.

Bazı uygulamalarda, uygulama tanımlayıcısı veya uygulama kimliğinin karşılık gelen temsili, üretilen dinamik güvenlik değerine doğrudan kriptografik olarak bağlanır. Örneğin, bazı uygulamalarda, uygulama tanımlayıcısı veya uygulamanın karşılık gelen temsili (veya uygulama tanımlayıcısı veya uygulamanın karşılık gelen temsili ile matematiksel olarak ilişkili bir veri elemanı), dinamik güvenlik değerini üretecek

kullanıcı kimlik doğrulama cihazı tarafından kullanılan kriptografik algoritma için giriş veri elemanlarından biridir.

Bazı uygulamalarda, uygulama tanımlayıcısı veya uygulama kimliğinin karşılık gelen temsili dolaylı olarak üretilen dinamik güvenlik değerine kriptografik olarak bağlanır. Örneğin bazı uygulamalarda, Kimlik Doğrulama Başlatma Mesajında yer alan uygulama tanımlayıcısı, kullanıcı kimlik doğrulama cihazı tarafından, dinamik güvenlik değerini oluşturmak için kullanıcı kimlik doğrulama cihazı tarafından kullanılan kriptografik algoritma için girdi veri elemanları olarak kullanılabilen Kimlik Doğrulama Başlatma Mesajındaki (örneğin bir sunucu kimlik bilgisi aracılığıyla) diğer veri elemanlarına kriptografik olarak bağlıdır. Bazı uygulamalarda, uygulama tanımlayıcısı ile Kimlik Doğrulama Başlatma Mesajında bulunan diğer veri elemanları arasındaki bu kriptografik bağlantı, kullanıcı kimlik doğrulama cihazı tarafından doğrulanabilir. Örneğin, bazı uygulamalarda, uygulama tanımlayıcısı, kullanıcı kimlik doğrulama cihazının (sunucu kimlik bilgisinin başarılı bir şekilde doğrulanmasından sonra), dinamik güvenlik değerinin oluşturulması için kriptografik algoritmada girdi olarak kullandığı Kimlik Doğrulama Başlatma Mesajında başka veri elemanlarına (bir kimlik sorma veya oturum tanımlayıcısı gibi) bir sunucu kimlik bilgisi (bir sunucu imzası veya anahtarlanmış bir sağlama veya bir Doğrulama Başlatma Mesajı verileri üzerinden bir MAC) ile kriptografik olarak bağlanır.

Bazı uygulamalarda Kimlik Doğrulama Başlatma Mesajı, bir kriptografik olarak (örneğin bir sunucu kimlik bilgisi ile) bağlantılı bir uygulama tanımlayıcısı ve sunucu tarafından oluşturulan bir dinamik güvenlik değeri içerebilir, böylece kullanıcı kimlik doğrulama cihazı, bu sunucu tarafından üretilen dinamik güvenlik değerini Yanıt Mesajına dahil edebilir, burada bu kapsama, uygulama tanımlayıcısı ve Kimlik Doğrulama Başlatma Mesajında sunucu tarafından üretilen dinamik güvenlik değeri arasındaki kriptografik bağlantının kullanıcı kimlik doğrulama cihazı tarafından başarılı bir şekilde doğrulanmaya bağlı olabilir.

Buluşu gerçekleştirme modları

Buluşa göre yöntemlerin bazı uygulamaları.

Mevcut buluşun yöntemlerinin birinci uygulama sınıfı olup, söz konusu uygulamayı barındıran bir uygulama sunucusuna bağlı bir erişim cihazı aracılığıyla söz konusu uygulamaya uzaktan erişen bir kullanıcı tarafından bir uygulama ile etkileşimin sağlanması için yöntemler içerir; yöntemler aşağıdaki adımları içerir:

bir kullanıcı kimlik doğrulama cihazında erişim cihazı tarafından yayılan bir sinyalin yakalanması, söz konusu sinyal bir kimlik doğrulama başlatma mesajı ile kodlanır; söz konusu kimlik doğrulama başlatma mesajı, uygulamanın bir kimliğine karşılık gelen en az bir uygulama tanımlayıcıyı içerir;

kullanıcı kimlik doğrulama cihazında söz konusu sinyalin kodunun çözülmesi ve kimlik doğrulama başlatma mesajının elde edilmesi;

kullanıcı kimlik doğrulama cihazında kimlik doğrulama başlatma mesajından uygulama tanımlayıcısının geri alınması;

kullanıcı kimlik doğrulama cihazında, uygulama kimliğinin bir insan tarafından yorumlanabilir temsilini elde etmek için kimlik doğrulama başlatma mesajından geri alınan uygulama kimlik tanımlayıcısının kullanılması ve kullanıcı kimlik doğrulama cihazının bir kullanıcı çıktı arayüzünü kullanarak kullanıcıya elde edilen uygulama kimlik temsilinin sunulması;

kullanıcı kimlik doğrulama cihazında kullanıcı kimlik doğrulama cihazının bir kullanıcı giriş arayüzünün kullanılması, bir yanıt mesajı üretmek ve oluşturulan doğrulama mesajını söz konusu doğrulama sunucusuna temin etmek için bir onay alınması;

kullanıcı kimlik doğrulama cihazında kriptografik dinamik güvenlik değeri oluşturma anahtarı ile parametrelenmiş bir birinci kriptografik algoritmayı kullanan ve belirli bir kullanıcı veya belirli bir kullanıcı kimlik doğrulama aracı ile ilişkili en az bir kişiselleştirilmiş veri elemanını kullanan bir dinamik güvenlik değeri oluşturulması, burada oluşturulan dinamik güvenlik değerinin, kullanıcıya sunulan uygulama kimliğine kriptografik olarak bağlıdır;

kullanıcı kimlik doğrulama cihazında en azından üretilen dinamik güvenlik değerini içeren bir yanıt mesajının oluşturulması;

doğrulama sunucusuna oluşturulan yanıt mesajının yapılması;

doğrulama sunucusunda yanıt mesajının alınması;

dinamik güvenlik değerinin geçerliliğini doğrulaması dahil olmak üzere yanıt mesajının doğrulanması;

yanıt mesajının uygulamaya doğrulanması sonucunun iletilmesi.

Mevcut buluşa göre yöntemlerin bir ikinci uygulama sınıfı olup, birinci sınıf yöntemleri içerir, burada yanıt mesajı, kullanıcının bir kimliğinin veya kullanıcı kimlik doğrulama cihazının bir kimliğinin göstergesi olan bir veri elemanıdır ve burada söz konusu veri elemanı kullanıcı kimliğinin göstergesidir veya kullanıcı kimlik doğrulama cihazı kimliği bir kullanıcı kimliğini belirlemek için kullanılır ve burada söz konusu kullanıcı kimliği aynı zamanda uygulamaya iletilir.

Mevcut buluşun yöntemlerinin bir üçüncü uygulama sınıfı olup, birinci ve ikinci sınıfların herhangi bir yöntemini içerir, burada kullanıcı kimliği uygulama kimliğinin bir fonksiyonu olarak da belirlenir.

Mevcut buluşun yöntemlerinin bir dördüncü uygulama sınıfı olup, birinci ila üçüncü sınıfların yöntemlerinden herhangi birini içerir, burada, uygulama kimliği temsilini elde etmek için kullanılan tüm uygulamaya bağımlı veriler, kullanıcı kimlik doğrulama cihazı tarafından, kullanıcı kimlik doğrulama cihazına harici bir kaynaktan veya kimlik doğrulama başlatma mesajından elde edilmektedir.

Mevcut buluşun yöntemlerinin beşinci bir uygulama sınıfı olup, birinci ila dördüncü sınıfların yöntemlerinden herhangi birini içerir ve bunlar ayrıca, kimlik doğrulama başlatma mesajına dahil edilecek bir sunucu kimlik bilgisinin üretilmesi, bir kriptografik sunucu kimlik bilgisi oluşturma anahtarı ile parametrelenmiş söz konusu ikinci bir kriptografik algoritma kullanılarak üretilmesi; kullanıcı kimlik doğrulama cihazında, kimlik doğrulama başlatma mesajından içerdiği sunucu kimlik bilgisinin geri alınması; ve kullanıcı kimlik doğrulama cihazında doğrulama, bir kriptografik sunucu kimlik doğrulama cihazında kimlik doğrulama anahtarı ile parametrelenmiş üçüncü bir kriptografik algoritma kullanarak sunucu kimlik bilgisinin doğrulanması adımlarını içerir.

Mevcut buluşun yöntemlerinin altıncı bir uygulama sınıfı olup, beşinci sınıfa ait yöntemlerden herhangi birini içerir, burada kimlik doğrulama başlatma mesajında yer alan uygulama tanımlayıcısı, kriptografik olarak sunucu bilgisine bağlıdır.

Mevcut buluşa göre yöntemlerin bir yedinci uygulama sınıfı olup, birinci ila altıncı sınıfların yöntemlerinden herhangi birini içerir, burada bir yanıt mesajının üretilmesi adımı, ayrıca kullanıcı kimlik doğrulama cihazında kullanıcı kimlik doğrulama cihazı

tarafından üretilen yanıt mesajında kullanıcıya sunulan uygulama kimliği temsilini gösteren bir veri elemanını da içerir.

Mevcut buluşa göre yöntemlerin bir sekizinci uygulama sınıfı olup, yedinci sınıfın herhangi bir yöntemini içerir, ayrıca, doğrulama sunucusunda, kullanıcıya sunulan uygulama kimliği temsilinin göstergesi olan veri elemanının, kimlik doğrulama başlatma mesajında yer alan uygulama tanımlayıcısı tarafından belirtilen uygulama kimliğiyle tutarlı olup olmadığını doğrulamayı içerir.

Mevcut buluşa göre yöntemlerin bir dokuzuncu uygulama sınıfı olup, aşağıdaki adımları içeren birinci ila sekizinci sınıf yöntemlerinden herhangi birini içerir: kullanıcı kimlik doğrulama cihazında kimlik doğrulama başlatma mesajında yer alan kimlik doğrulama başlatma mesaj işlemiyle ilgili verilerin geri alınması; kullanıcı kimlik doğrulama cihazında, kullanıcı kimlik doğrulama cihazının bir kullanıcı çıkış arayüzü kullanılarak alınan işlemle ilgili verilerin sunulması; burada üretilen dinamik güvenlik değeri, işlemle ilgili verilere kriptografik olarak bağlıdır.

Mevcut buluşun yöntemlerinin bir onuncu uygulama sınıfı olup, dokuzuncu sınıf yöntemlerden herhangi birini içerir ve ayrıca kimlik doğrulama başlatma mesajına dahil edilecek bir sunucu kimlik bilgisinin üretilmesi; söz konusu üretme bir kriptografik sunucu kimlik bilgisi oluşturma anahtarı ile parametrelenmiş ikinci bir kriptografik algoritması kullanılarak yapılır; kullanıcı kimlik doğrulama cihazında, kimlik doğrulama başlatan mesajın içerdiği sunucu kimlik bilgisinden alınması; kullanıcı kimlik doğrulama cihazında, bir kriptografik sunucu kimlik doğrulama doğrulama anahtarı ile parametrelenmiş üçüncü bir kriptografik algoritma kullanarak sunucu kimlik bilgisi doğrulama; burada sunucu kimlik bilgisi, işlemle ilgili verilere kriptografik olarak bağlıdır.

Mevcut buluşa göre yöntemlerin bir on birinci uygulama sınıfı olup, dokuzuncu sınıfın yöntemlerinden herhangi birini içerir ayrıca, kullanıcıya sunulan işlemle ilgili verilerin göstergesi olan kullanıcı kimlik doğrulama cihazı veri elemanları tarafından oluşturulan yanıt mesajını içeren kullanıcı kimlik doğrulama cihazında; ve doğrulama sunucusunda, kullanıcıya sunulan işlemle ilgili verilerin göstergesi olan veri elemanlarının, doğrulama başlatma mesajında yer alan işlemle ilgili veriler ile tutarlı olup olmadığının doğrulanmasını içerir.

Bu buluşun yöntemlerinin bir on ikinci uygulama sınıfı olup, birinci ila on birinci sınıfların yöntemlerinden herhangi birini içerir; burada dinamik güvenlik değeri oluşturma anahtarı, bir gizli kişiselleştirilmiş anahtar içerir; ve burada kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değeri oluşturma anahtarını en az bir dinamik giriş değeri ile kriptografik olarak birleştirerek dinamik güvenlik değerini hesaplar; ve burada söz konusu dinamik girdi değeri, kullanıcı kimlik doğrulama cihazında bir zaman mekanizması tarafından sağlanan zamanla ilgili bir değerden en az birini, kullanıcı kimlik doğrulama cihazı tarafından depolanan ve muhafaza edilen sayaçla-ilişkili bir değeri veya kimlik doğrulama başlatma mesajında yer alan bir kimlik sormayı içerir.

Mevcut buluşa göre yöntemlerin bir on üçüncü uygulama sınıfı olup, onikinci sınıftaki yöntemlerden herhangi birini içerir, burada kullanıcı kimlik doğrulama cihazı, dinamik güvenlik değeri oluşturma anahtarını, kullanıcıya sunulan uygulama kimliği temsilini gösteren bir veri elemanı ile kriptografik olarak birleştirerek dinamik güvenlik değerini hesaplar.

Mevcut buluşa göre yöntemlerin bir on dördüncü uygulama sınıfı olup, onikinci sınıfın yöntemlerinden herhangi birini içerir, burada kullanıcı kimlik doğrulama cihazı, kimlik doğrulama başlatma mesajında yer alan kimlik doğrulama başlatma mesaj işlemi ile ilgili verileri alır ve bu işlemle ilgili verileri kullanıcıya sunar; ve burada kullanıcı kimlik doğrulama cihazının, dinamik güvenlik değeri oluşturma anahtarını, kullanıcıya sunulan işleme ilişkin verilerin göstergesi olan veri elemanları ile kriptografik olarak birleştirerek dinamik güvenlik değerini hesaplar.

Buluşa göre aparat

Mevcut buluşun cihazlarının bir birinci sınıfı, veri işlemek için uyarlanmış bir işlem bileşenini içeren kimlik doğrulama bilgilerinin üretilmesi için aparat; veri depolamak için bir depolama bileşeni; bir kullanıcı için çıktıları temsil eden bir birinci kullanıcı çıkış arayüzü ve kullanıcıdan girdi almak için bir giriş kullanıcı arayüzü içeren bir kullanıcı ara yüzü bileşeni ve kullanıcının bir uygulamayı bir bilgisayar ağı üzerinden bir uygulamaya uzaktan erişmek için kullandığı bir erişim cihazının bir ikinci kullanıcı çıkış arayüzü tarafından yayılan bir sinyali yakalayacak şekilde uyarlanmış bir veri giriş arayüzü, söz konusu sinyal, bir kimlik doğrulama başlatma mesajı ile kodlanır, söz konusu uygulamanın kimliğine karşılık gelen en az bir uygulama tanımlayıcısını içeren

kimlik doğrulama başlatma mesajı içerir, burada aparat, söz konusu sinyalin kodunu çözmek ve kimlik doğrulama başlatan mesajı almak üzere uyarlanır, kimlik doğrulama başlatma mesajından uygulama tanımlayıcısının geri alınması, uygulama kimliğinin insan tarafından yorumlanabilir bir temsilini elde etmek için uygulama tanımlayıcısını kullanımı ve elde edilen uygulama kimlik temsilini birinci kullanıcı çıkış arayüzünün kullanımı ile kullanıcıya sunulması, kullanıcı giriş arayüzünü kullanarak, bir yanıt mesajı oluşturulması ve bir kimlik doğrulama sunucusuna yanıt mesajını vermek için bir onay almak suretiyle kullanıcıdan elde edilir; kriptografik dinamik güvenlik değeri oluşturma anahtarı ile parametrelenmiş bir ilk kriptografik algoritma kullanarak ve kullanıcı veya aparatla ilişkili en az bir kişiselleştirilmiş veri elemanı kullanarak bir dinamik güvenlik değeri üretilmesi, burada üretilen dinamik güvenlik değerinin, kullanıcıya sunulan uygulama kimliğine kriptografik olarak bağlıdır; ve en azından üretilen dinamik güvenlik değerini içeren bir yanıt mesajı oluşturulmasını içerir.

Mevcut buluşun cihazlarının bir ikinci uygulama sınıfı, birinci kullanıcı çıkış arayüzünü kullanan kullanıcıya oluşturulan yanıt mesajını sunmak için daha fazla uyarlanan birinci aparat sınıfındaki aparatlardan herhangi birini içerir.

Mevcut buluşun cihazlarının bir üçüncü uygulama sınıfı, ayrıca, söz konusu yanıt mesajını bir doğrulama sunucusuna iletmek üzere uyarlanmış bir veri iletişim arayüzü içeren birinci aparat sınıfındaki aparatlardan herhangi birini içerir.

Mevcut buluşun bir siteminin bir uygulaması, söz konusu uygulamayı barındıran bir uygulama sunucusuna bağlı bir erişim cihazı aracılığıyla söz konusu uygulamaya uzaktan erişen bir kullanıcı tarafından bir uygulama ile etkileşimi sağlamak için bir sistem içerir, yukarıda tarif edildiği gibi çok sayıda kullanıcı kimlik doğrulama cihazı ve çok sayıda kullanıcı kimlik doğrulama cihazından herhangi biri tarafından üretilen bir yanıt mesajını almak üzere uyarlanmış ve alınan dinamik güvenlik değerinin geçerliliğinin doğrulanması dahil olmak üzere alınan yanıt mesajının doğrulanması için uyarlanmış ve yanıt mesajının doğrulanmasını uygulamaya iletmek üzere uyarlanmış bir doğrulama sunucusu içerir.

Avantajlı etkiler

Yukarıda tarif edilen buluşun avantajları aşağıdakileri içerir.

Gerçek çoklu uygulama desteği.

Güven modeli.

Buluş, aşağıdaki güven modeline sahip bir çoklu uygulama ortamı için uygundur. Kullanıcılar, kimlik doğrulama bilgilerini bir dizi uygulamaya doğru şekilde işlemek için ve güvenilir kimlik doğrulama cihazı tarafından sağlanan ve/veya denetlenen bir kullanıcı kimlik doğrulama cihazına güvenmek ve belirli bir şekilde sağladıkları belirli verileri doğru şekilde yönetmek için güvenilir bir kimlik doğrulama sunucusuna güvenir. Uygulamalar, kimlik doğrulama bilgilerinin doğrulanmasıyla (diğer bir deyişle Yanıt Mesajlarında yer alan dinamik güvenlik değerleri) ilgili güvenilir kimlik doğrulama sunucusuna güvenir. Uygulamaların birbirlerine güvenmesi gerekmez. Daha da önemlisi, şifreleri birbirleriyle paylaşmak zorunda değillerdir. Kullanıcılar belirli bir uygulamaya yalnızca söz konusu uygulamanın kapsamı ve bağlamı içinde güvenirler. Diğer bir deyişle kullanıcılar, herhangi bir uygulamanın kapsamı ve bağlamında kullanıcı adına sorumlu davranmaya yönelik herhangi bir uygulamaya güvenmez ve bu nedenle, kullanıcı adına diğer uygulamalara erişmek için kullanabilecekleri kimlik bilgilerini uygulamaya sunmak istemezler.

Uygulamanın bazı uygulamalarında, dinamik güvenlik değeri, kullanıcıya sunulan, onaylanan ve incelenen bir uygulama tanımlayıcısına kriptografik olarak bağlıdır. Bu kriptografik bağlantı, oluşturulan bir Yanıt Mesajının geçerliliğini belirli bir uygulamaya etkili bir şekilde sınırlar ve bir uygulama için oluşturulan kimlik bilgilerinin (Yanıt Mesajlarının) başka bir uygulama için geri dönüştürülemeyeceğini garanti eder.

Ekstra uygulamaları desteklemek için esneklik

Kullanıcı kimlik doğrulama cihazı farklı uygulamalar için farklı kriptografik anahtarları veya farklı konfigürasyon verileri gerektirmediğinden (özellikle örneğin uygulama kimliklerinin temsili gibi herhangi bir uygulamaya özgü veriyi saklamak için kullanıcı doğrulama cihazlarına gerek yoktur), ekstra uygulamalar kolayca desteklenebilir. Ekstra bir uygulama için desteklenmesi gereken tek şey, bu ekstra uygulamanın güvenilir kimlik doğrulama sunucusuyla bir güven ilişkisi kurmasıdır.

Yüksek güvenlik.

Kullanıcı kimlik doğrulama cihazları, herhangi bir belirli kullanıcı kimlik doğrulama cihazına özgü dinamik güvenlik değerleri üretebilecek ve böylece (belirli bir kullanıcı kimlik doğrulama cihazı ile ilgili kullanıcı arasındaki bilinen ilişki sayesinde) bireysel kriptografik anahtarları ile bu kimlik doğrulama cihazının yasal kullanıcısı için kişiselleştirilmiştir. Belirli bir kullanıcı kimlik doğrulama cihazı tarafından üretilen herhangi bir kimlik bilgisi bu nedenle bu kullanıcı kimlik doğrulama cihazına (ve ilgili kullanıcıya) kriptografik olarak bağlıdır.

Dinamik güvenlik değerlerinin hesaplanmasında dinamik bir değişkenin (bir kimlik sorma veya bir sayaç veya bir zaman değeri gibi) kullanılması, üretilen dinamik güvenlik değerlerinin öngörülemezliğini sağlar ve tekrar saldırılarına karşı koruma sağlar.

Uygulama kimliğinin ve kriptografik bağlantının dinamik güvenlik değeri ile insan tarafından yorumlanabilen ve tanınabilir bir temsilinin sunulması, diğer uygulamalara erişim için bunları kullanmak üzere dolandırıcılık uygulamaları (örneğin gerçek zamanlı kimlik avı saldırıları) tarafından geçerli kimlik bilgilerinin toplanmasına karşı korur.

Güvenilir kullanıcı kimlik doğrulama cihazı üzerindeki işlem verilerinin sunumu ve onaylanmış işlem verilerinin dinamik güvenlik değerinin hesaplanmasına dahil edilmesi, bir dolandırıcı tarafın bir uygulamaya meşru bir kullanıcı tarafından gönderilen işlem verileri ile kesiştiği ve değiştirdiği MITM (ortadaki adam) saldırılarına karşı koruma sağlar.

Yüksek kullanıcı rahatlığı.

Kullanıcının uygulamaya özel şifreler gibi uygulamaya özel güvenlik verilerini hatırlaması gerekmemektedir. Bu buluş, kimlik doğrulama sunucusu tarafından uygulamaya otomatik kullanıcı kimliğinin tanımlanmasına bile izin verir, böylece kullanıcı artık hatırlamak zorunda kalmaz, aynı zamanda uygulamaya özel kullanıcı adı veya kullanıcı id'si girmez. Buluş aynı zamanda yaygın olarak çok çeşitli uygulamalara (iletişim bilgileri, adres veya kredi kartı numarası) temin edilmesi gereken diğer verilerin

uygulamalarına yönelik otomatik iletişimi sağlar, böylece sıkıcı manuel veri girişini önler.

Buluş herhangi bir normal standart erişim cihazı ile çalışabildiğinden ve erişim cihazında herhangi bir özel donanım veya yazılımın bulunmasını gerektirmediğinden (diğer bir deyişle uygulama ile etkileşime girmek için standart bir web tarayıcısı ve Kimlik Doğrulama Başlatma Mesajını yaymak için normal bir kullanıcı çıkış arayüzü) bu buluş, kullanıcılara çok yüksek bir hareketlilik ve özgürlük sağlar.

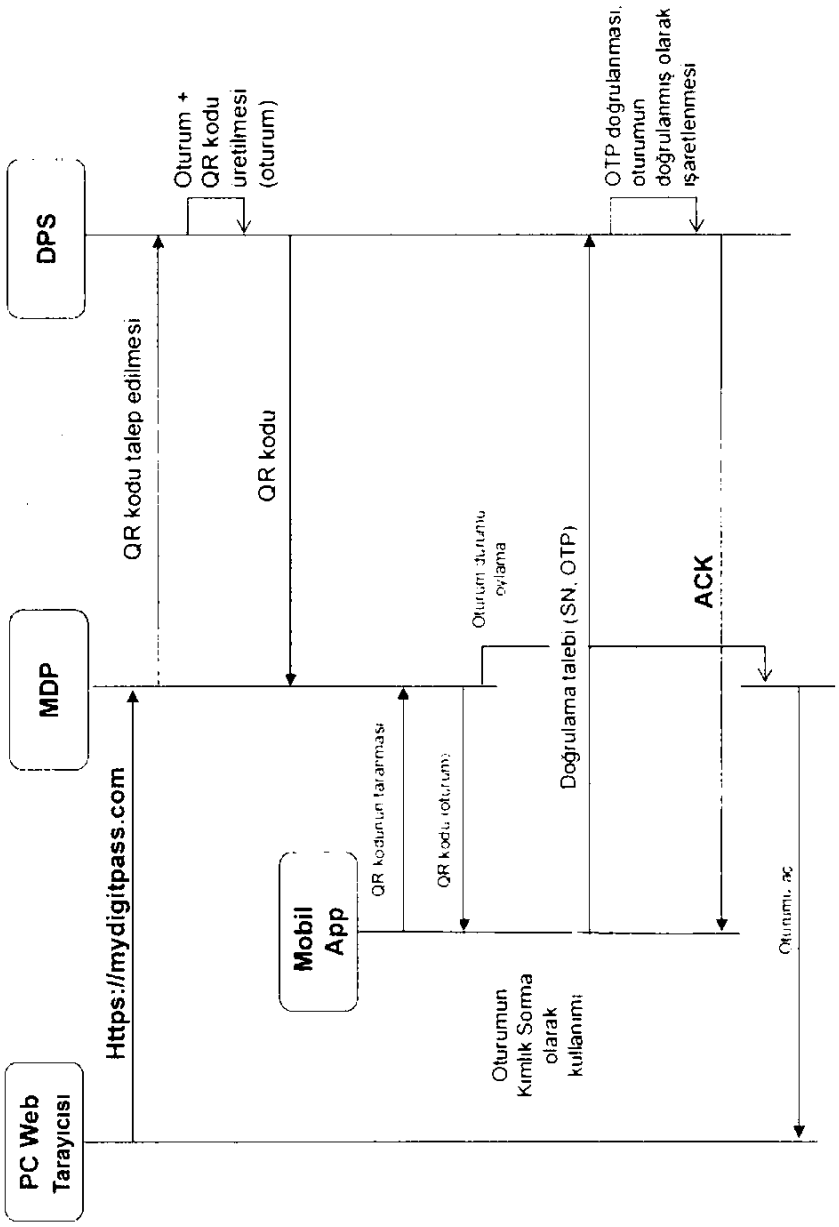
Maliyet etkinliği.

Doğası gereği sınırsız sayıda uygulama için aynı kullanıcı kimlik doğrulama cihazı kullanılabildiğinden, buluşun çözümü çok uygun maliyetlidir. Ayrıca, çözüm erişim cihazına çok az gereksinim bulunduğundan (Kimlik Doğrulama Başlatma Mesajını kodlayan sinyali vermek için normal bir kullanıcı çıkış arayüzüne sahip olması gerekir), genellikle erişim sırasında belirli donanım ve/veya yazılım cihazlarını (örneğin akıllı kart okuyucular ve bunlarla bağlantılı sürücüler) yükleme ile ilgili sıkıcı ve maliyetli destek sorunları yoktur.

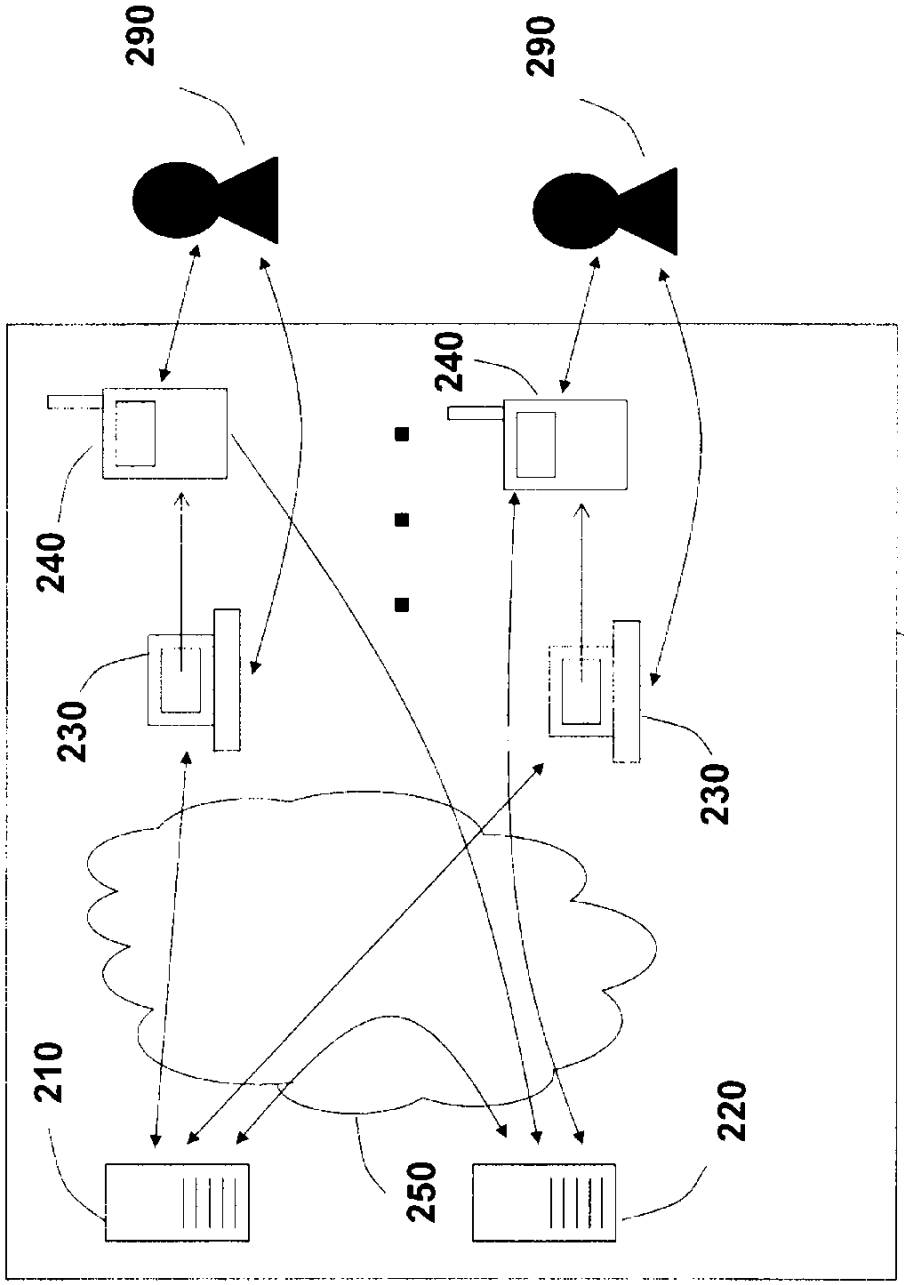
Kullanıcı kimlik doğrulama cihazının bazı uygulamaları sadece simetrik kriptografiye dayanır ve asimetrik kriptografiyi kullanmaz. Bu uygulamalar, daha kısa kriptogramlarla çalışabilmeleri ve asimetrik kriptografiye dayanan uygulamalardan daha az işlem gücü gerektirmeleri avantajına sahiptir.

Birtakım uygulamalar tarif edilmiştir. Bununla birlikte, çeşitli modifikasyonların yapılabileceği anlaşılacaktır. Örneğin, bir veya daha fazla uygulamanın elemanları, başka uygulamalar oluşturmak için birleştirilebilir, silinebilir, değiştirilebilir veya tamamlanabilir. Buna göre, diğer uygulamalar ekli istemlerin kapsamı dahilindedir. Ek olarak, mevcut buluşun özel bir uygulama özelliği, çeşitli uygulamalardan sadece biri ile ilgili olarak açıklanabilirken, bu özellik, herhangi bir belirli veya belirli bir amaç için arzu edilen ve avantajlı olabilen diğer uygulamaların bir veya daha fazla başka özelliği ile birleştirilebilir. Mevcut buluşun çeşitli uygulamaları yukarıda açıklanmış olmakla birlikte, bunların sadece örnek yoluyla sunulmuş olduğu ve sınırlama olmadığı anlaşılmalıdır. Özellikle, koruma isteminde bulunuman konuyu tanımlamak amacıyla her türlü bileşenin veya metodolojinin herhangi bir kombinasyonunu tarif etmek mümkün

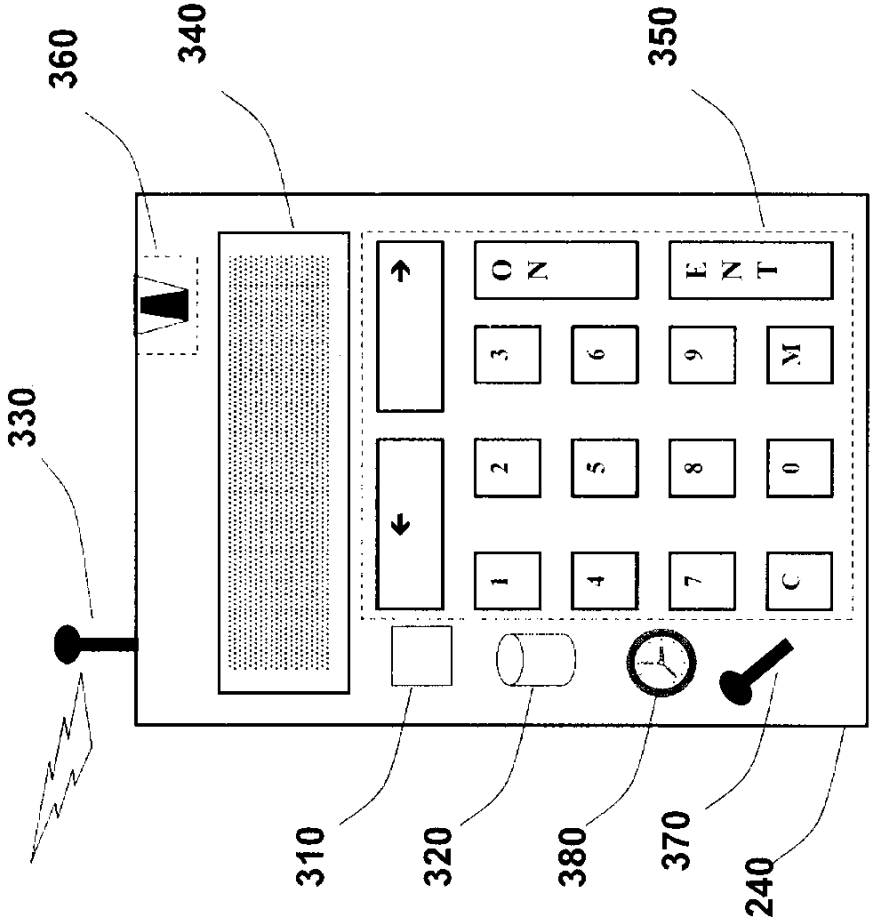
değildir, fakat teknikte uzman bir kişi, mevcut buluşun birçok kombinasyonunun ve permütasyonunun mümkün olduğunu fark edebilir. Bu nedenle, mevcut buluşun içeriği ve kapsamı, yukarıda tarif edilen örnek uygulamaların herhangi biri ile sınırlandırılmamalı, sadece aşağıdaki istemlere ve eşdeğerlerine göre tanımlanmalıdır.


DPS
MDP
Mobil App
PC Web Tarayıcısı
Oturum + QR kodu üretilmesi (oturum)
OTP doğrulanması, oturumun doğrulanmış olarak işaretlenmesi
QR kodu talep edilmesi
QR kodu
Oturum durumu sorgulama
Doğrulama talebi (SN, OTP)
ACK
QR kodunun taranması
QR kodu (oturum)
Https://mydigitpass.com
Oturumu Kimlik Sorma olarak kullanımı
Oturumu aç

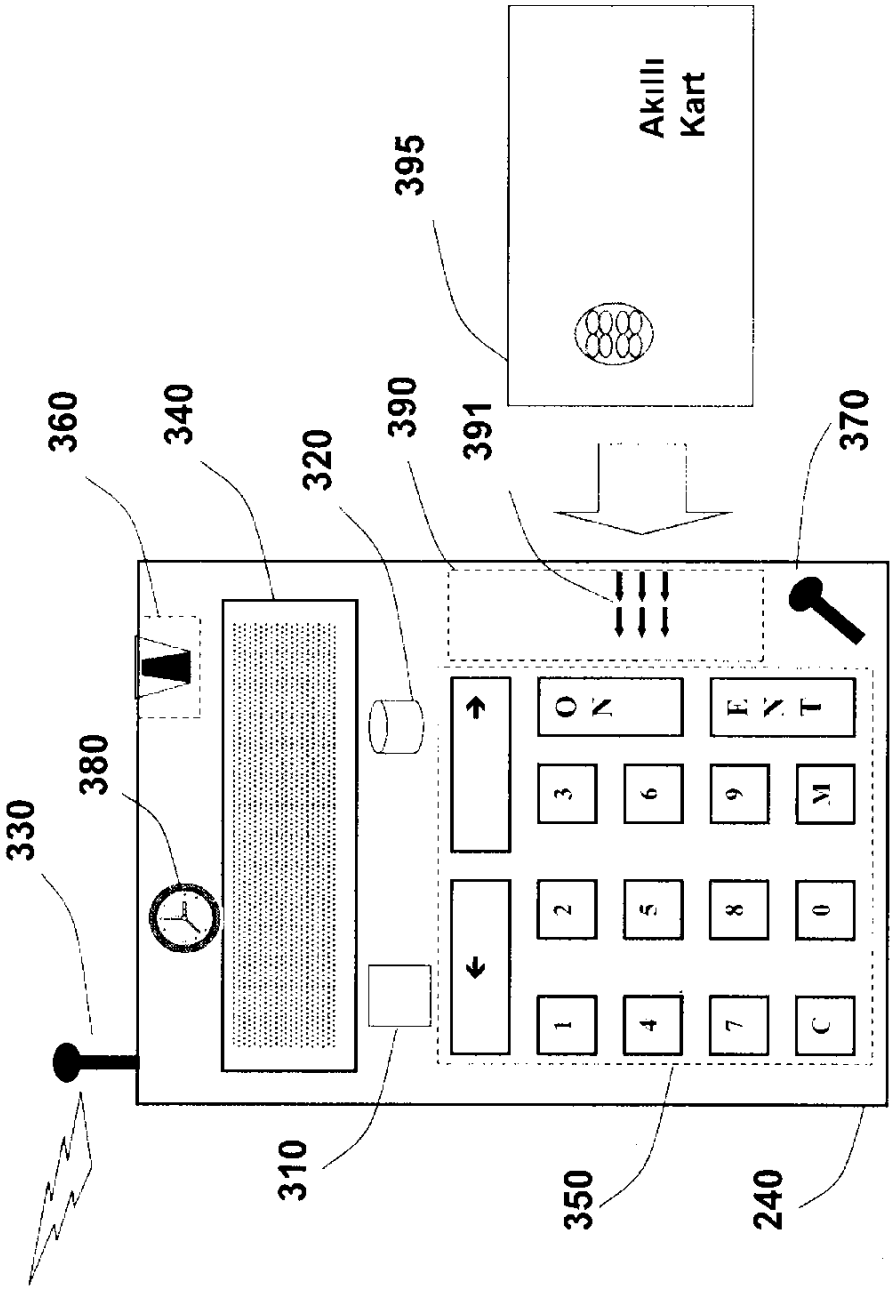
Şekil 1



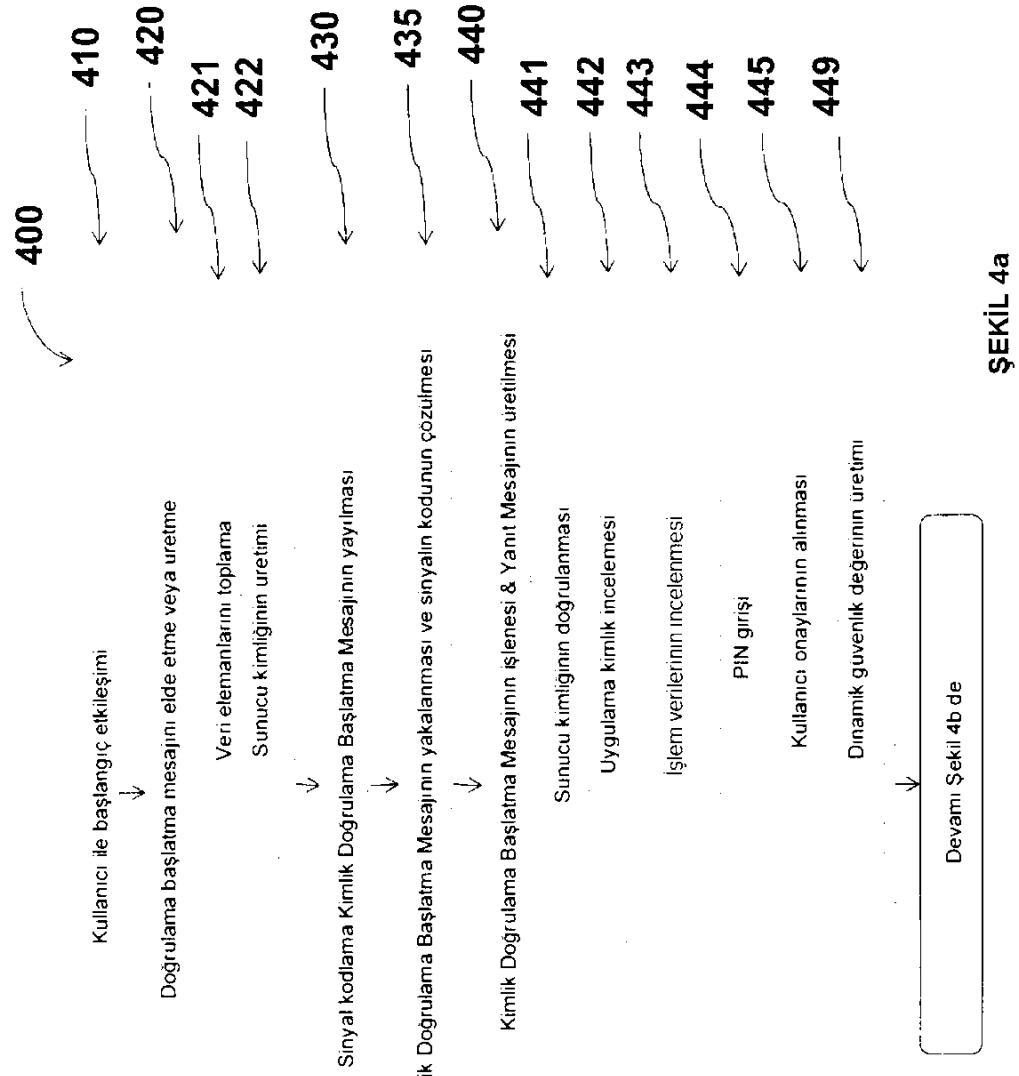
Şekil 2



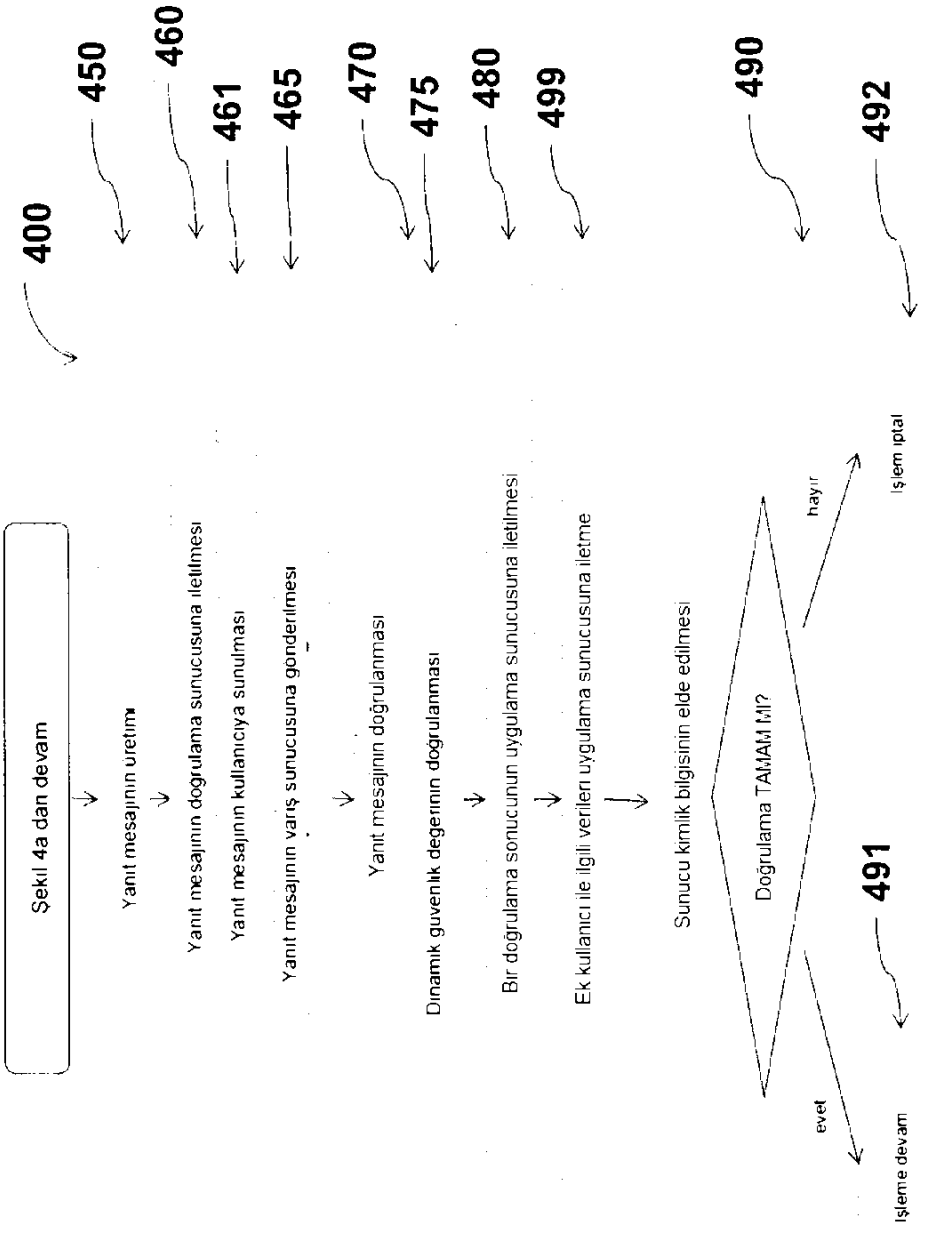
Şekil 3a


Akıllı Kart
395
360
340
320
390
391
370
380
330
310
350
240
ON
ENT
3
6
9
M
2
5
8
0
1
4
7
C

Şekil 3b


400
410
Kullanıcı ile başlangıç etkileşimi
420
Doğrulama başlatma mesajını elde etme veya uretme
421
Veri elemanlarını toplama
422
Sunucu kimliğinin üretimi
430
Sinyal kodlama Kimlik Doğrulama Başlatma Mesajının yayılması
435
Kimlik Doğrulama Başlatma Mesajının yakalanması ve sinyalin kodunun çözülmesi
440
Kimlik Doğrulama Başlatma Mesajının işlenesi & Yanıt Mesajının üretilmesi
441
Sunucu kimliğinin doğrulanması
442
Uygulama kimlik incelemesi
443
İşlem verilerinin incelenmesi
444
PİN girişi
445
Kullanıcı onaylarının alınması
449
Dinamik guvenlik değerinin üretimi
Devamı Şekil 4b de

ŞEKİL 4a


400
Şekil 4a dan devam
450
Yanıt mesajının üretimi
460
Yanıt mesajının doğrulama sunucusuna iletilmesi
461
Yanıt mesajının kullanıcıya sunulması
465
Yanıt mesajının varış sunucusuna gönderilmesi
470
Yanıt mesajının doğrulanması
475
Dinamık guvenlık degerının doğrulanması
480
Bir doğrulama sonucunun uygulama sunucusuna iletilmesi
499
Ek kullanıcı ile ilgili verileri uygulama sunucusuna iletme
490
Sunucu kimlik bilgisinin elde edilmesi
Doğrulama TAMAM MI?
hayır
İşlem iptal
492
evet
491
İşleme devam

Şekil 4b