Yetkili Sayısal İmza Tasarımı ve Uygulama Çatısı[1]

Alper Uğur[1] İbrahim Soğukpınar[2]

[1,2]Bilgisayar Mühendisliği Bölümü, Gebze Yüksek Teknoloji Enstitüsü, Kocaeli
[1]e-posta: augur@bilmuh.gyte.edu.tr [2] e-posta: ispinar@bilmuh.gyte.edu.tr

Abstract

Digital signature applications are used to substitute traditional handwritten signature on documents in digital environments.
Digital signature in individual usage allows control of documents integrity and verification about association of signers identification with the sign. In fact as well as above, authorization of a signer to sign any documents in an organizational workflow has to be verified. This can be done as integration of signature with appropriate authorization information to compose an authorized digital signature as a result.
In this work design of an authorized signature was presented, application framework of the authorized signature was explained and possible implementations were illustrated.
A design pattern based model was also expressed to facilitate adaptation of traditional signature applications to be an authorized digital signature.

Özetçe

Sayısal imza uygulamaları kullanım alanı olarak, yetkilendirme, kimlik denetimi ve bilgi bütünlüğü gibi güvenlik işlevlerini gerektiren gelişmiş bilgi ve belgelendirme sistemlerinde yaygınlaşmaktadır. Bu uygulamalar, sayısal ortamdaki belge için, geleneksel olarak el ile atılan ıslak imzanın karşılığını elde etmek amacıyla kullanılmaktadır.
Sayısal imza, bireysel kullanımda imzayı atan kişinin kimliğinin ve sayısal imza ile ilişkilendirilen belgenin bütünlüğünün doğrulanmasına imkan vermektedir. Oysa kurumsal belgelerde, belge üzerindeki imzayı atan kişinin imzayı atmaya yetkisinin olup olmadığının da sorgulanması gereklidir. Bu, sayısal imzanın uygun bir yetki bilgisi ile ilişkilendirilerek, yetkili sayısal imzaya dönüştürülmesi ile mümkün olabilir.
Bu çalışmada, kurumsal belgeler üzerindeki imzalar için yetki denetiminin gerçekleştirilebileceği bir yetkili sayısal imzanın tasarımı sunulmuş ve yetkili sayısal imza uygulamalarına temel oluşturacak tasarımı destekleyen gerçekleme önerileri örneklendirilmiştir. Tasarımın var olan sayısal imza uygulamaları için uyum kolaylığı sağlayacak şekilde dekoratör tasarım kalıbı yardımıyla gerçekleştirilmesine de yer verilmiştir.

1. Giriş

Bilgi sistemlerinde, sistemin genel güvenliğini ve sistem üzerindeki bilginin korunmasını destekleyen güvenlik politikaları bulunmaktadır. Bu güvenlik politikaları temellerinde; aktif verinin değiştirilmediğinin kontrolü amacıyla uygulanan veri bütünlüğü, verinin gizliliğini sağlamak için kullanılan veri şifreleme/deşifreleme ve gerek haberleşme gerek veri güvenilirliği gereksinimlerine cevap veren yetkilendirme ve kimlik denetimi fonksiyonlarını barındırır[1].

.Bahsi geçen sistemlerde, dolaşımda ya da arşivlenmiş bir belgeye eklenen sayısal imza, ilgili verinin kaynağının yani belgeyi kimin oluşturduğunun, belgenin kimden geldiğinin, verinin özgünlüğünün yani değiştirilip değiştirilmediğinin doğrulanmasına yardımcı olmaktadır.
Sayısal imza uygulamaları bahsedilen işlevleri gerçekleştirirken imzayı atan kişiye özgü benzersiz anahtar ile belgeye özgü özet bilgiyi birleştirirler. Kişiye özgü anahtar, kişinin kimlik bilgisi ile ilişkilendirildiğinden imzayı atan tarafın kimliğinin doğrulanmasını; belgeye özgü özet ise belgenin değiştirilmediğinin, aslının korunduğunun anlaşılmasını sağlar.
2007'de Uğur ve Soğukpınar, kurumsal dolaşımdaki belgelerin geçerli sayılması için sayısal imza ile kimlik doğrulamanın yanında belge üzerindeki imzanın yetkili olup olmadığının da belirlenmesi gerektiğini belirtip yetkili sayısal imza kavramını ortaya koydular[2]. Yetkili sayısal imza, imzayı atan kişinin belge üzerindeki yetkisini belirtir ve doğrulanabilir bir yetki bilgisinin imzalama işlemine dahil edilmesi ile oluşturulmaktadır[2,3].
Bu çalışmada, imzalayanın yetkisinin de denetlenmesinin gerektiği kurumlarda, dolaşımdaki ve arşivlenen belgeler üzerinde sayısal imzalama işlemi için kullanılacak, sayısal imzaya bir yetkibilgisinin eklenmesi ve yetkinin bir yetki yetkilisi tarafından kontrol edilip onaylanmasını temel alan bir yetkili sayısal imza uygulaması tasarımı sunulmaktadır.
Çalışmada ayrıca tasarımın var olan sayısal imza uygulamalarından yetkili sayısal imzaya geçiş sürecini hızlandıracak modüler bir yapı önerilmektedir. Bu yapı var olan uygulamaların köklü değişikler gerektirmeden uyumunu sağlamaktadır. Bunun gerçekleştirilmesi için yazılım mühendisliği yöntemlerinden biri olan tasarım kalıplarından faydalanılmaktadır.
Makalenin takip eden bölümlerinde sayısal imza ve yetkili sayısal imza kavramları tanımlanıp, yetkili sayısal imza tasarımının temelini oluşturan yetkibilgisi, imza şemaları ve yetki yetkilisi yapılarının tasarım ve işlevleri detaylandırılmaktadır. Son bölümde ise yetkili sayısal imza uygulamaları için tasarımın olası uygulamaları yer almakta ve tasarımın sayısal imza uygulamalarına katkıları ile makale tamamlanmaktadır.

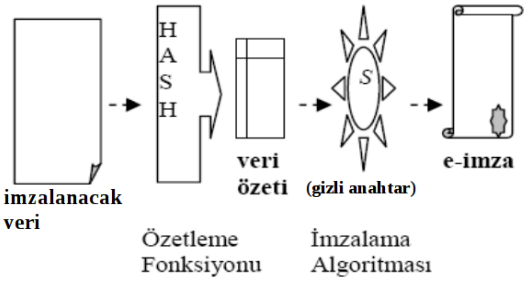
2. Sayısal İmza ve Yetkili Sayısal İmza Kavramları

Sayısal imza, sayısal bir veriye eklenen ya da o sayısal veriyle mantıksal bağlantısı olan, kimlik doğrulama amacıyla kullanılan başka bir sayısal veri olarak tanımlanabilir[4]. Sayısal imza aynı zamanda, güvenli bir imza oluşturma aracı ile oluşturulma, nitelikli bir sayısal sertifika ile imza sahibinin kimliğinin tespitini ve imzalanmış sayısal veride imza sonrası herhangi bir değişikliğin yapılıp yapılmadığını sağlayabilme yeteneğine sahip olmalıdır[4].

[1]Bu çalışma TÜBİTAK Bilimsel ve Teknolojik Araştırma Projelerini Destekleme Programı (1001) tarafından 108E132 no lu proje kapsamında desteklenmektedir.

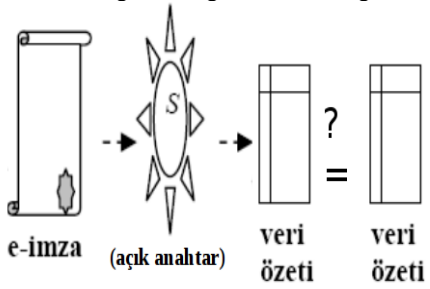
Sayısal imza şeması kavramı Diffie ve Hellman tarafından 1976'da ortaya konulmuştur[5]. 1978'de Rivest, Shamir ve Adleman günümüzde yaygın olarak kullanılan sayısal imzalama algoritmasının temellerini atmıştır[6]. Sonraki yıllarda gelişen kriptografik yöntemler ile ElGamal, ECDSA gibi bir çok sayısal imzalama şeması literatürde yerini almıştır[7].

Sayısal imzalama, imzalanacak belgenin tek yönlü bir özetleme fonksiyonu ile özgün bir özetinin elde edilmesi ve bu özetin belirlenen imzalama algoritmasından geçirilmesi aşamalarından oluşan işlemdir(Şekil 1). Bu işlemin sonucunda o belgeye ait bir sayısal imza elde edilmiş olur.



Şekil 1: Sayısal İmzalama Şeması.

Sayısal imzanın doğrulanması ise; belgenin aynı özetleme fonksiyonu kullanılarak özetinin oluşturulması ve bu özetin imzalayan kişiye özgü bir anahtar/sertifika ile çözümlenmiş özetle karşılaştırılması aşamalarını içerir (Şekil 2). Anahtar kullanımı kimliğin doğrulanmasını, özetlerin karşılaştırılması ise belgenin bütünlüğünün doğrulanmasını sağlar.



Şekil 2: Sayısal İmza Doğrulama Şeması.

Teknolojinin ihtiyaçları doğrultusunda son on yılda birçok sayısal imza şeması ortaya konmuştur. Bunlardan bir kısmı geleneksel imzalama şemalarında yer alan anahtar özgünlüğüne bağlı kimlik doğrulama yapısını hedef alarak kimlik tabanlı imza kavramı üzerinedir [8,9,10,11,12]. Bu imza şemalarında kişiye özgü (isim, e-posta adresi gibi) kimlik verileri imza ile bütünleştirilerek kimlik doğrulamada yeni yöntemler izlenmiştir. Daha sonraki yıllarda imza sahibinin yerine bir kişi ya da grubun imza atmasına imkan verecek vekil imza şemaları literatürde yerini almıştır[13,14,15].

Kimlik doğrulama işlemi belge üzerindeki imzanın kime ait olduğunu doğrulamaktadır fakat aynı kişinin o imzayı atmaya yetkili olup olmadığı konusunda bir fikir vermemektedir. Kaldı ki var olan sayısal imza uygulamaları yukarıda verilen şemalarda görüldüğü gibi kişinin yetkisi konusunda hiçbir bilgi içermemektedir. Oysa kurumsal imzalarda belgeye imza atan/onaylayan kişinin yetkisi önemlidir. Yetkisiz bir kimsenin belge üzerindeki imzası geçerli ve doğrulanabilir olsa bile o belgeyi geçerli yapmaya yetmeyecektir.

Sayısal imzalı belgelerde yetki probleminin çözümü için, yetkilerin, imza ile ilişkilendirilerek her yetkinin, yetkiye özgü imza anahtarıyla temsili ise karmaşık anahtar yönetimi ve imza doğrulanmasında kullanılacak anahtarın seçimi gibi zorluklar ortaya çıkaracaktır.

2007'de Uğur ve Soğukpınar imzaya kişinin onaylı kurumsal yetkisini içeren bir bilginin eklenerek yetkili sayısal imza elde edilebileceğini öne sürdüler [2,3].

Önerilen yaklaşım, yetkibilgisinin imza oluşturulurken ve onaylanırken kontrolünü ve böylelikle sayısal imzanın yetki denetiminin gerçekleştirilmesini olanaklı kılmaktadır. Yetkili sayısal imza şemasında yetkibilgisi iki şekilde imzaya dahil edilmektedir. Bunlardan biri yetkibilgisinin belgeyle birleştirilerek imzanın oluşturulmasıdır. Diğerinde ise yetkibilgisi imza anahtarı ile birleştirilerek aynı imza anahtarının eşi ile doğrulanabilecek yeni bir yetkili imza anahtarı oluşturulmaktadır.

Önerilen şemalarda imza anahtarı daha önce var olan anahtar eşiyle doğrulanabilir şekilde tasarlandığından anahtar yönetimine yük getirmemektedir. Bölüm 3'te önerilen yetkili sayısal imza çatısına ve bu çatıyı oluşturan temel yapıtaşlarına yer verilmiştir.

3. Yetkili Sayısal İmza Çatısı

Yetkili sayısal imza, imza ve yetki bilgisinin birleştirilmesi temeline dayanmaktadır. Bu bölümde bahsedilen birleştirme işleminin nasıl yapılabileceğine dair iki yöntem sunulmaktadır.

Bu yöntemlerden biri imzalama safhasında yetki ile iletinin birleştirilmesini, diğeri ise yetki bilgisinin imza anahtarıyla bütünleştirilmesini temel almaktadır.

3.1. Yetki Bilgisi Birleştirme Şeması

Sertifika yapısındaki yetki bilgisi; yetkinin tanımı, yetki dönemi, yetkinin ait olduğu kişiyi tanımlayan bilgi (örn. kimliğe bağlı açık anahtarı), yetkiyi veren kurum ya da şahıs, yetkibilgisinin onayı şeklinde tanımlanan alanlardan oluşmaktadır(Şekil 3).

Al_i : yetki tanımı	T-Al_i : Al_i nin (yetki) geçerlilik aralığı	
pl_i : kimlik bilgisine bağlı açık anahtar (l_i)	$p(l+1)_j$: kimlik bilgisine bağlı açık anahtar $(l+1)_j$	$p(l+n)_k$: kimlik bilgisine bağlı açık anahtar $(l+n)_k$
$SL = SAA_s(Al_i$, T-Al_i, pl_i, $p(l+1)_j$, $p(l+n)_k$)	AA : kurumsal hiyerarşik yetki onay/doğrulama birimi/yetkilisi	
t-Al_i : Kurumsal hiyerarşik yetkili imza zaman pulu	-Gelişmeler için ayrılmıştır-	

Şekil 3: Yetki Bilgisi

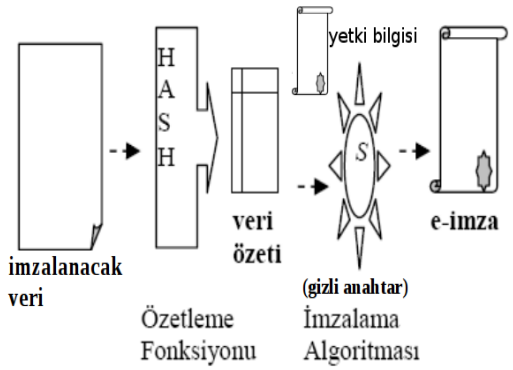
Bu yaklaşımda yetkibilgisi ileti ile birlikte kapsüllenir. Bu aşamadan sonra yapılan imzalama işlemi geleneksel sayısal imzalama şemaları ile aynıdır.

$S_{li\text{-}s}( )$; l_i kullanıcısının s_{li} anahtarıyla ürettiği imza ve L hiyerarşik yetki bilgisi olmak üzere oluşacak imza:

$[S_{li\text{-}s}\ (\ m||\ L\ )||\ m||\ L]$ şeklinde olacaktır. Bu şema Şekil 4'te özetlenmiştir.

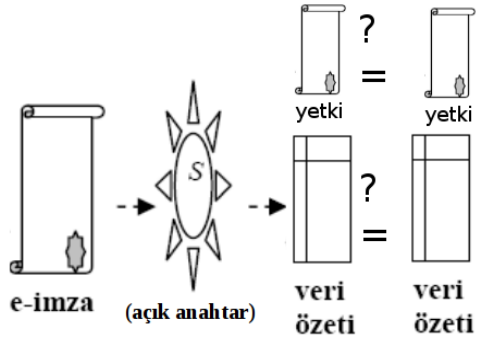
Doğrulama safhası geleneksel imza doğrulama şemasıyla farklılık göstermektedir. $S_{li\text{-}s}\ (\ m||L\ )$ s_{li} anahtarının eşleniği

olan açık anahtar p_{li} ile ya da diğer açık anahtarlı kriptografik şemalara benzer şekilde doğrulanır. Doğrulama safhasının tamamlanması için Yetki Bilgisi'nin de doğrulanması gerekmektedir. Bu işlem Yetki Yetkilisi yardımıyla gerçekleştirilmektedir. Yetki Bilgisi'ndeki $t\text{-}A_{li}$ zamanpulu alanı da bu aşamada kontrol edilmektedir.



Şekil 4: Yetkili Sayısal İmzalama Şeması

Doğrulama safhasına ait şema Şekil 5'te verilmiştir.Yetkili sayısal imza uygulaması, sayısal imza uygulamasından temelde yetki denetimi ile ayrılır. Dolayısıyla genel şemada imzanın doğrulanması yetkili sayısal imzada farklılık gösterir. Yetkinin geçerliliğinin sorgulanması Yetki Yetkilisi yardımıyla gerçekleştirilmektedir. Yetki Yetkilisi, yetkibilgilerinin oluşturulduğu onaylandığı ve doğrulandığı birimlerdir.



Şekil 5: Yetkili Sayısal İmza Doğrulama Şeması

Doğrulayan taraf, imzadan yetki bilgisini elde eder ve Yetki Yetkilisine(AA) ilgili imza ve yetki bilgisinin eşleşip eşleşmediğini sorar yani doğrulamasını ister.
AA yetkinin geçerliliği ve bütünlüğün kontrolü açısından yetki bilgisi üzerindeki S_{AA} imza alanını kontrol eder. Eğer yetki geçerli ise AA bu kez doğrulanmak üzere sunulan yetki konusunu ve yetki bilgisi üzerindeki A_{li} alan bilgisini karşılaştırır.
Bu kontrollerin yapılabilineceği iki farklı aşama vardır: ön-kontrol, son-kontrol. İsimlendirmeden anlaşılabileceği gibi doğrulanma yetkili imza oluşturulma safhasında veya imza doğrulama aşamasında olduğu gibi imzalama işlemi yapıldıktan sonra gerçekleştirilebilir.
Ön-kontrolde, yetkili imza ile imzalama işleminin, A_{li} yetki konusunun geçerli olduğu ve yetki bilgisi üzerindeki $T\text{-}A_{li}$ de belirtilen zaman aralığından önce ya da sonra gerçekleştirilmesine izin verilmeyecektir.

Son-kontrolde ise, kullanıcı tarafından oluşturulan ve yetki bilgisinde saklanan $t\text{-}A_{li}$ zaman-pulu ve $T\text{-}A_{li}$ yetki zaman aralığı AA tarafından karşılaştırılır. Eğer aralık ve yetki konusu p_{li} açık anahtarına sahip kişi için tutuyorsa yetkili imza geçerli olarak kabul edilir.

3.2. Yetkili İmza Anahtarı Şeması

Bu yaklaşımda, kullanıcının anahtarı yetki bilgisi ile bütünleştirilerek yetkili imza anahtarı elde edilmektedir.

$S_{li\text{-}s}(\ )$; *li* kullanıcısının s_{li} anahtarıyla ürettiği imza ve L hiyerarşik yetki bilgisi ve üretilen yetkili imza anahtarı

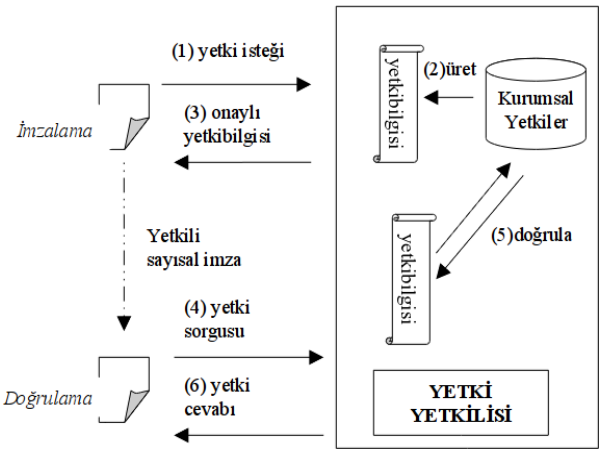
$sa_{li} = (s_{li}, L)$ olmak üzere oluşacak imza

$[\ S_{li\text{-}sa}\ (m) || m || L]$ şeklinde olacaktır.

Bu yaklaşımda imza anahtarının yetki bilgisi ile bütünleştirilmesi işleminde eşleme tabanlı kriptografiden faydalanılmıştır. Yaklaşım, anahtar üretimi ve imza doğrulama aşamalarında diğer yaklaşımdan ayrılmaktadır[3].
Yetki bilgisi L'nin doğrulanması önceki şemada olduğu gibi Yetki Yetkilisi yardımıyla olacaktır.

3.3. Yetki Yetkilisi

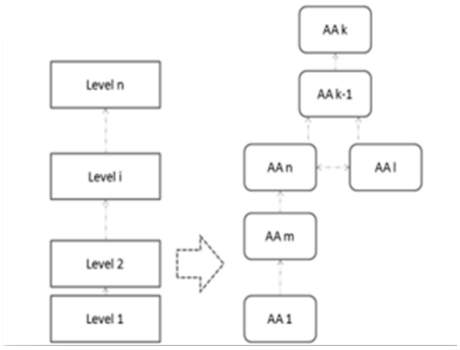
Modelin diğer temel unsuru Yetki Yetkilisidir. Bu birimler yetkibilgilerinin tutulduğu, dağıtıldığı ve çevrimiçi doğrulandığı birimler olmaktadır.
Yetki Yetkilisi(AA) yetki ve ilgili imzalayan için tanımı önceki bölümlerde yapılan ve alanları verilen yetki bilgisini oluşturur. Daha sonra imzayı kullanacak kişiye gönderir. Kullanıcı yetkili imzasını kullanacağı zaman zamanpulunu ekleyerek yetkibilgisini tamamlar. Önceki bölümlerde detaylı olarak anlatılan Yetki Yetkilisinin imza oluşturma ve doğrulama aşamalarına ait süreç şeması Şekil 6.'da özetlenmiştir.



Şekil 6: Yetki Yetkilisi Süreç Şeması

AA'nın asıl işlevi yukarıda bahsedilen imza şemalarınca oluşturulmuş yetkili imzanın doğrulanmasında ortaya çıkmaktadır.
Model tarafından desteklenen, seçmeli olarak, çevrimiçi ve çevrimdışı doğrulama olmak üzere iki ayrı yetki doğrulama yöntemi önerilmektedir:
Yetkinin çevrimdışı doğrulanması doğrulayan tarafında gerçeklenmektedir. Sıklıkla kullanılan yetkibilgileri doğrulayan tarafında güvenli şekilde saklanır. Ayrıca yetkili imza altseviyeler tarafından oluşturulmuşsa yetkibilgisinde yer alan yetki varlıkları tarafından da doğrulanabilir.
Çevrimiçi doğrulamada ise: doğrulayan taraf yetkibilgisinin geçerliliğini seviyesinin bağlı olduğu AA ya sorar. Eğer AA

yetki bilgisine sahipse karşılaştırmayı yapar ve onay ya da red bilgisi içeren bir cevabı döndürür. Eğer sorgulanan yetki bilgisine sahip değilse hiyerarşide üst seviyedeki AA ya sorguyu iletir ve yetki sorgusu cevaplanana dek iletim devam eder. Olmayan yetkinin sorgulanması gibi AA modele gereksiz yük getirecek sorgular yetkibilgisinde yer alan AA alanı kullanılarak önlenebilir. Hiyerarşik tırmanış eşik değerinin aşılmasından sonra doğrudan AA ya sorulması gibi.
Hiyerarşik AA modeli kurumdaki her kurumsal seviyeye ait bir AA olabilecek şekilde tasarlanmıştır (Şekil. 7). Bu seviyeler birimler, şubeler, bölümler ve kurumsal daireler vs olabilir. İlişkili kurumların AA yapısı da birbirleri arasında hiyerarşi ilişkisi gösterebilir.



Şekil 7: Hiyerarşik Yetki Yetkilisi Modeli

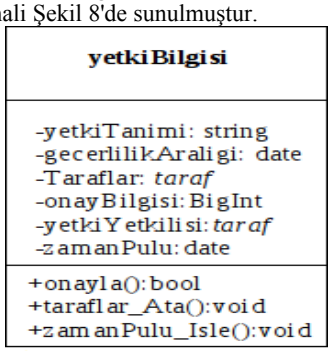
Tüm kurumsal seviyeler ve AA hiyerarşisi arasındaki iletişimin güven mekanizmaları veya şifreleme gibi yeterli güvenlik seviyesi sağlanarak yapıldığı varsayılmaktadır.
Takip eden bölümde sayısal imzalı belgelerde yetki denetimi gerektiren kurumlardaki yetkili sayısal imza uygulamaları için gerçekleme örnekleri ve var olan sayısal imza uygulamalarından yetkili sayısal imza uygulamasına geçişin uygulama tasarımı ile nasıl gerçekletirilebilineceği anlatılmaktadır.

4. Yetkili Sayısal İmza Uygulaması

Bu bölümde, yetkili sayısal imza uygulaması tasarımının farklı uygulama ortamları için nasıl gerçeklenebileceğine dair ipuçları verilmekte ve var olan uygulamaların uyumu için yetkili sayısal imzayı destekleyecek bir dönüşüm çözümü olarak uygulamaların dekoratör tasarım kalıbı ile gerçekleştirilmesi yaklaşımı sunulmaktadır.

4.1. Yetki Bilgisi

Uygulamada Yetki Bilgisini ve üzerinde tanımlı metodları gösterir yapı hali Şekil 8'de sunulmuştur.



Şekil 8. YetkiBilgisi için UML gösterim

Yetki bilgisini tanımlayan bu yapı, nesne tabanlı diller ile yazılmış uygulamalar için referans olmak üzere sunulmuştur.

4.2. XML imza sözdizimi

Xml tabanlı imza <Signature> yapısında kullanımı uygun olan <SignatureProperties> etiketi altında yetkiBilgisi (Authorization) eklenerek uyarlanması planlanmıştır. XML imza tabanlı yetkili sayısal imzayı içeren söz dizimi örneği aşağıdaki gibi olacaktır:

```
<Signature ID = "HierOrgSignature">
   <SignedInfo>
     …
    <Reference URI= "#level_i_Authority" TYPE=
"http://www.w3.org/2000/09/xmldsig#SignatureProperties">
       …
     </SignedInfo>
      <Object>
        <SignatureProperties>
          <SignatureProperty ID = "level_i_Authority"
        TARGET= "#HierOrgSignature"
            <authorization xmlns: myns=
                  "http://.. RFCsozdizimi.TXT " >
              <clearance > Level II</clearance >
              <validity>20100630:20110629</validity>
              <AuthorizationEntity>
                <authorizative ID>101110101001110101..
                </authorizative ID>
              </AuthorizationEntity>
              <AuthorizationEntity>
                <authorizative ID>101101000100110111..
                </authorizative ID>
              </AuthorizationEntity>
              <SignedInfo>
                      …
              </SignedInfo>
            </authorization>
          </SignatureProperty>
          </SignatureProperties>
        </Object>
</Signature>
```

Şekil 9. XMLSignature sözdizimi üzerinde yetkibilgisi <*authorization*> ile oluşturulmuş örnek yetkili sayısal imza

4.3. Sayısal imzaların uyarlanması

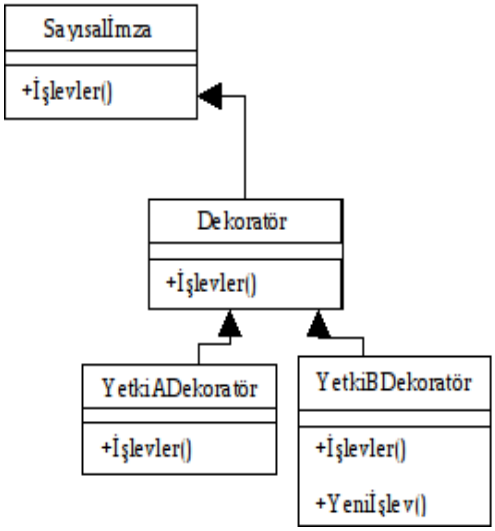
Önceki bölümlerde, var olan sayısal imza uygulamalarının yetki denetimi işlevini gerçekleştirmekten yoksun olduklarından bahsedilmiş ve bu işlevi yerine getirmek için yetkili sayısal imza yaklaşımının önerildiğinden bahsedilmiştir.
Varolan uygulamaların tamamen işlevsiz hale gelmesi yerine bu yaklaşımı destekleyecek şekilde adapte olmaları hem zaman hem de maliyet açısından verimli olacaktır.
Yetkili sayısal imza için yetki denetiminin yapılabilineceği bir yetkibilgisinin şemaya dahil edildiği iki yaklaşım sunulmuştur. Var olan sayısal imza uygulamaları göz önünde bulundurulduğunda, ikinci yaklaşım için modüler bir çözüm sözkonusu olmazken ilk yaklaşım eksik olan yetki denetimi işlevinin sayısal imza uygulamalarında yapılabilecek bir tasarım değişikliği ile eklenmesi sonucu yetkili sayısal imza uygulaması haline getirilebilir.

Bunu gerçeklemek için önerdiğimiz yaklaşım GOF[1]'un tasarım kalıpları katalogunda[16] *yapısal kalıp* sınıflandırmasının altında yer alan *dekoratör tasarım kalıbı*nın kullanılmasıdır.

Sayısal imza uygulamaları gerçekleştirilirken tasarım kalıplarının kullanılmasının yanında literatürde sayısal imzanın yetersizliklerinin çözümü için tasarım kalıplarının kullanılmasına da rastlanmaktadır[17]. Bu çalışmada sayısal imzanın sürekliliği GOF tasarım kalıpları katalogunun davranışsal kalıp sınıflandırmasının altında yer alan strateji tasarım kalıbı ile sağlanmıştır.

Katalogda yer alan dekoratör tasarım kalıbı, nesneye dinamik olarak sorumluluklar yüklenmesini sağlar.Eklenen nesnenin davranışlarını dinamik olarak genişletmeye izin verir. Dekoratör kullanımı nesne tabanlı programlamada kalıtımın aksine programın çalışma zamanında görev alır[18].

Önerilen dekoratör tasarım kalıbının, sayısal imza uygulamasında kullanılması Şekil 10'da sunulmuştur.



Şekil 10: Yetkili Sayısal İmza Dekoratörü

Sayısal imzalama işlemi gerçekleştirilirken AA desteği ile yönetilen Yetkili Sayısal İmza Dekoratörü sayısal imzaya eklenecek yetkibilgisinin seçiminde rol oynar.

Var olan sayısal imza uygulaması iletinin yanında hiçbir yetki bilgisi içermezken $S_{li\text{-}s}\ (\ m\ )$, Dekoratör yetkili sayısal imza şemasındaki ilk yaklaşımın gerektirdiği gibi yetki bilgisinin iletiyle birlikte işlem görme yetisini sayısal imza uygulamasına kazandırır. Yetki Yetkilisi de yine Dekoratör sayesinde onaylanan yetki bilgisini uygulamaya aktarır. Sonuçta sayısal imza $S_{li\text{-}s}\ (\ m||L\ )$ şeklindeki yetkili sayısal imzaya dönüşmüş olacaktır.

Aynı şekilde doğrulama safhasında ileti ile yetkinin ayrılması ve ayrı ayrı kontrolü de Dekoratör'ün sağladığı işlevler ile gerçekleşebilecektir.

5. Sonuçlar ve Öneriler

Bu çalışmada yetkili sayısal imzanın gerekliliği, yetkili sayısal imza tasarımının üzerinde durulmuş ve tasarımın gerçekleştirilmesi üzerine yaklaşımlar sunulmuş ve tasarıma ait uygulama örnekleri detaylandırılmıştır.

Yetkili sayısal imza uygulamaları ile kurum içi ve kurumlararası olası yetkisiz imza anlaşmazlıkları tespit edilebilir ve önlenebilir olabilecektir.

Yetki bilgisi arşiv niteliği taşıyan belgeler için geriye dönük doğrulamayı sağlayan bir yapıdadır.

Önerilen imza şemaları gerekli olan yetkibilgisinin eklenmesi ve doğrulanmasında işlem yükü getirsede geçerli ve gerekli bir sistem için bu yük önemsiz kalacaktır.

Bu modüler dönüşüm var olan uygulamaların yetkili sayısal imza kavramına uyumlarını kolaylaştırmakta ve bu uygulamalara gereken esneklik kazandırılmaktadır.

Yetkili sayısal imza kavramının çoklu imzalar ile uyumunun araştırılması ve örneklemeleri ileriye dönük çalışmalar olarak ele alınabilir.

6. Kaynakça

[1] W. Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall, NJ, 2003

[2] A. Uğur, İ.Soğukpınar, "A New Hierarchical Signature Scheme with Authorization", *Information Security and Cryptology Conference*, 13-14 Aralık 2007, Ankara

[3] A. Uğur, İ.Soğukpınar, "A Framework for Licensed Digital signatures", *First Int. Workshop on Network & Communications Security (NCS 2009)*,India, Aralık 2009

[4] Elektronik İmza Kanunu, Kanun No:5070, Sayı:25355, 3 Ocak 2004 Tarihli Resmi Gazete, 2004

[5] Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliskin Tebliğde Değisiklik Yapılmasına Dair Tebliğ, Sayı:26056, 21 Ocak 2006 Tarihli Resmi Gazete, 2006

[6] W. Diffie, M.E. Hellman "New Directions in Cryptography",*IEEE Transactions on Information Theory, IT-22(*6):644-654, Nov. 1976

[7] R. Rivest, A. Shamir ve L. Adleman. "A method for obtaining Digital Signatures and Public Key Cryptosystems."*Communic. of ACM.* Feb., 1978 21(2)

[8] FIPS 186-3 Digital Signature Standard. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf Feb 2009

[9] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", *CRYPTO 84, LNCS* 7:47--53, 1984.

[10] D. Boneh, M. K. Franklin, "Identity-Based Encryption from the Weil Pairing", *Advances in Cryptology - Proceedings of CRYPTO 2001* (2001).

[11] K. G. Paterson, "ID-based signatures from pairings on elliptic curves", *IEEE Communications Letters,* 38(18):1025–1026, 2002.

[12] J. C. Cha and J. H. Cheon, "An identity-based signature from gap Diffie-Hellman groups", *PKC 2003, LNCS vol. 2567 s. 18-30*. Springer-Verlag, 2003.

[13] Mambo, K. Usuda, and E. Okamoto. "Proxy signatures: Delegation of the power to sign messages". *IEICE Trans. Fundamentals*, 1996, Vol. E79-A, No. 9, s 1338-1353.

[14] G. Wang, F. Bao, J. Zhou, and R. H. Deng. "Security Analysis of Some Proxy Signatures". *ICISC 2003, LNCS 2971, s. 305-319*. Springer-Verlag, 2004.

[15] G. Wang. "Designated-Verifier Proxy Signature Schemes".*IFIP/ SEC 2005*, s. 409-423. Springer, 2005.

[16] E.Gamma, R. Helm , R.Johnson , J Vlissides , Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley, Reading, MA,1995.

[17] A.Uğur,İ.Soğukpınar, "Elektronik İmza Uygulamalarının Sürekliliği İçin Tasarım Kalıplarının Kullanılması", *1. Ulusal Elektronik İmza Sempozyumu,* 7-8 Aralık 2006, Ankara

[18] Design Pattern Framework, http://www.dofactory. com, erişim. Eylül 2009

[1]Gang of Four takma adıyla bilinen yazarlar: Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides