E-imza'da Format Seçimi (XML, PDF'e karşı)

F. Koray ATSAN

***Özet* - Son yıllarda, ülkemizde e-imza'nın yaygınlaşmaya başladığına ve gerek kamu gerekse özel sektör kurum ve kuruluşlarının daha önce başlattıkları e-imza projelerini hayata geçirdiklerine tanık oluyoruz. Şüphesiz ki, bu projelerin ve yeni başlatılacak olan projelerin hayata geçmesi ve başarılı olabilmesi için, e-imza konusunda yapılacak bazı kritik seçimlerin isabetli yapılması gerekmekte.Bu seçimlerden biri de, e-imza formatı seçimidir. Zira, format seçimi e-imzalı uygulamaların başarıya ulaşmasında kilit faktörlerden biridir.Bu makalede, format seçimi ile ilgili önemli bazı unsurlara değineceğiz.**

***Anahtar Kelimeler* – e-imza, format, xml,pdf**

I. GİRİŞ

E-imza'nın yaygınlaşmaya başladığı bu günlerde e-imzaya geçmek isteyen kurum ve kuruluşların karşısına çıkacak olan kaçınılmaz soru şu olacaktır: İmzalanacak olan form veya dokümanlar için ***hangi format tercih edilmeli*?** Web üzerinde çalışan bir online formun formatı muhtemelen .html, .aspx, .jsp, veya .php dir. Doküman yönetim sistemlerinde kullanılan format ise, .doc, .pdf, .tif vb. olabilir.

Yukarıdaki sorunun yanıtı ihtiyaçlara ve uygulamaya göre değişebilecektir. Örneğin kullanılmakta olan uygulama yukarıda belirtilen formatları veya düz metin formatını kullanıyorsa ve kullanıcılara e-imzalı dokümanları göstermek (görsellik) gibi bir endişe yoksa e-imzaya geçişte bu formatları kullanmaya devam etmek tercih edilebilir. Aksine, e-imza hizmeti müşterilere sunulmak isteniyorsa, bu durumda son kullanıcılara görselliği daha yüksek ve daha anlaşılabilir ve kullanım kolaylığı sağlayacak bir format tercih edilebilir.

E-imza için güncel olarak 2 temel imzalama formatı kullanılmaktadır:

- XML
- PDF

Bu iki formatın da avantaj ve dezavantajları vardır. Bunları konu başlıkları halinde aşağıda inceleyeceğiz.

F. Koray ATSAN, *EBG Bilişim Hizmetleri ve Teknolojileri A.Ş. (e-tugra), Mecidiyeköy, İSTANBUL, e-posta: katsan@e-tugra.com*

II. GÖRSELLİK

İngilizce de bir tabir vardır : "Seeing is believing" : Görmek inanmaktır. Her ne kadar bu deyiş tartışmaya açık olsa da (bazen görülen yok, görülemeyen de var olabilir), insanoğlunun gördüğüne inanmaya eğilimi olduğunu söyleyebiliriz. Bu nedenle de matematik temeline dayanan ve zaten soyut bir kavram olan e-imzaya somut bir görsellik özelliği katmak teknolojinin kullanımı açısından faydalı olacaktır.

PDF formatında imzalama denildiğinde aslında, PDF dokümanı açtığınız zaman, e-imzanın dokümanın içinde görsel olarak görülebilmesinden bahsedilmektedir. Aksi takdirde PDF imzalamanın diğer dosyaların imzalanması arasında bir fark kalmaz. PDF formatında imzalamanın en büyük avantajı, imzanın görsel olarak kullanıcıya gösterilebilmesi ve görselliğin belirli bir çerçeve de isteğe göre özelleştirilebilmesidir. Genel olarak e-imza teknolojisi ile ilgili bilgisi olmayan ortalama kullanıcılar için e-imzayı somutlaştıran bir unsur olarak oldukça faydalıdır.

XML formatında ise, doküman kendi başına görsellikten uzak, özellikle imza kısmı ilginç karakterlerden ibarettir. Neyse ki bu durum, XSL formatı ile düzeltilebilmektedir. Yani, bir XML dosyanın görüntüsü diğer bir XSL dosya yoluyla istenen şekilde ayarlanabilmektedir. Aşağıdaki örnekler de çeşitli gösterimler sunulmaktadır:

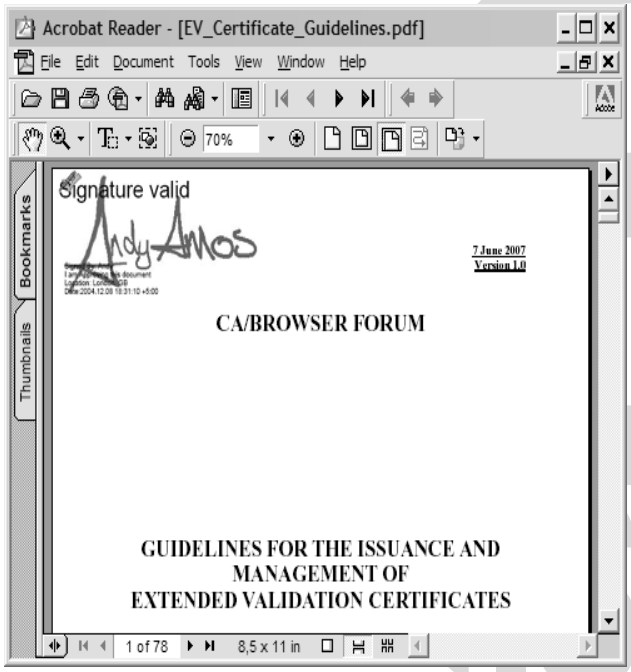
A. Anlaşılabilir olmaktan uzak bir İmzalı XML gösterimi

```
<?xml version='1.0' encoding='UTF-8' ?>
<?xml-stylesheet type='text/xsl' href='Belge.xsl'?>
<Veri xmlns:ds="Veri" Id='#SignedData'>
<Belge>
<BelgeTar>05.07.2007</BelgeTar>
<BelgeSayi>43839</BelgeSayi>
</Belge>
<ds:Signature>MIIKzwYJKoZIhvcNAQcCoIIKwDCCCrwCA
QMxCTAHBgUrDgMCGjCCAxMGCSqGSI
MADQo8R2FyYW50aUJlbGdlc2k+DQo8QmVsZ2VUYXI+
MDUuMDcuMjAwNzwvQmVsZ2VUYXI+DQo8
QmVsZ2VTYXlpPjQzODM5PC9CZWxnZVNheWk+DQo8R
2VjZXJsaWxpa1Rhcj4wNS4wNy4yMDA5PC9H
ZWNlcmxpbGlrVGFyPg0KPFVudmFuPlNFTEtBID/HIFZFI
ERJPyBUP0NBUkVUIChF3DpTRUxLQSA/
VEhBTEFUID9IUkFDQVQgVkUgUEFaQVJMQU1BKTwv
VW52YW4+DQo8QWRyZXM+3HNr/HAgQ2FkZGVz
</ds:Signature>
</Veri>
```

B. XSL formatında anlaşılabilir bir imzalı dosya gösterimi

Şekil 1 : İmzalı Dosya Görünümü (XSL Formatı)

C. Anlaşılabilir bir PDF imzalı dosya gösterimi:



Şekil 2 : İmzalı Dosya Görünümü (PDF Formatı)

E-imza'nın görselliği ile ilgili önemli bir nokta, WYSIWYS (What you see is what you sign) prensibidir. Bunun anlamı, kullanıcıya ne imzalayacaksa veya ne imzaladıysa onun gösterilmesi gerektiğidir.

III. İMZALI VERİ PAYLAŞIMI

E-imzalı verilerin diğer bir kurum ile paylaşılması söz konusu ise bu durumda, veri paylaşımı için en uygun formatı seçmekte fayda olacaktır. Şüphesiz ki yapılacak seçim e-imzalı verilerin ne kadarının paylaşılmak istendiğine, ne kadarının ise paylaşılmak istenmediğine göre de şekillenecektir.

Örneğin e-imzalı bir dosyanın tamamı paylaşılmak isteniyorsa, bu durumda dosya olduğu gibi paylaşıma açılabilir. Eğer e-imzalı dosyanın sadece belirli bir kısmı paylaşılmak isteniyorsa (Örnek: Sadece genel müdürün belge üzerinde imzaladığı belirli bir veri paylaşılmak isteniyor ama diğer verilerin kurumun gizlilik politikasından dolayı veya yaptığı gizlilik anlaşmasından dolayı paylaşılması mümkün gözükmüyor) bu durumda verinin belirli bir kısmını paylaşılmasına izin verecek formatı seçmek daha doğru olacaktır.

XML formatındaki bir dosyanın istenilen kısımlarının imzalanması ve değişik kısımlarını değişik kullanıcılara imzalattırılması mümkündür. Bu veri paylaşımında oldukça esneklik sağlayan bir yöntemdir. XML formatının veri paylaşımını esas alan bir format olması, aynı esnekliği imzalı XML veriler için de geçerli kılmasına şaşırmamak lazım.

PDF formatında ise, dosyanın bir kısmını imzalanması veya paylaşılması mümkün olmamaktadır. PDF imzalama kullanılıyorsa dosyanın tamamını paylaşmak zorunda kalınacaktır.

IV. KULLANIM KOLAYLIĞI

Kullanım kolaylığı konusunda PDF'in açık ara önde olduğunu belirtmeliyiz. PDF imzalama için kullanılacak imzalama aracı, kendi başına PDF imzalayabilir veya Adobe araclarından birine entegre çalışabilir olacaktır.Her iki durumda da kolay bir imzalama arayüzüne sahip olunacaktır. İmza doğrulamada ise eğer kullanılan araç, Adobe imza formatına uygun imzalama yapıyorsa, bu durumda ücretsiz olan "Adobe Reader" ile imza doğrulanabilecektir. Doğrulama tamamen Adobe Reader veya diğer bir PDF Reader tarafından gerçekleştirilir.

XML de ise muhtemelen, imzalama ve imza doğrulama işlemlerini kendiniz gerçekleştirmek durumunda kalırsınız veya bir XML aracı bulunsa dahi, ihtiyaçlar doğrultusunda özelleştirmek gerekecektir.

V. HUKUKİ AÇIDAN FORMAT SEÇİMİ

E-imza'nın hukuki boyutu ülkemizde 5070 sayılı e-imza kanunu [1] ve ilgili yönetmelik ve tebliğlerle düzenlenmiştir. Bu yönetmelikler de e-imza ile ilgili Avrupa birliği standartlarına da atıflar yapılarak bunlara uyum sağlanması istenmektedir.

E-imza formatı seçimi, e-imza'nın geçerliliği'nin ispatı bakımından da önem arz etmektedir. Örnek olarak, ilk doğrulama ardından, sonraki doğrulamalarda e-imza'nın geçerliliğinin hukuki olarak ispat edilebilmesi için ilk imza doğrulamada kullanılan doğrulama bilgisinin saklanarak veya imza bilgisine eklenerek, daha sonraki doğrulamalarda bu bilginin kullanılması gerekmektedir. Bu şekilde bir kullanım ise E-imza formatları'nın kullanımını da tanımlayan standartlara uyum yoluyla sağlanabilecektir.

XML formatına ait e-imzalama ve imza doğrulama süreci W3C nin XAdes (XML Advanced Electronic Signatures)[2] standardında net olarak tanımlanmıştır. XAdes standardı ise Avrupa Komisyonu E-imza direktifine uyum sağlamak

amacıyla XML İmzalama spesifikasyonu'nun genişletilmiş halidir. XAdes standardına uyum sağlanması, 5070 sayılı e-imza kanunu ve ilgili yönetmelik ve tebliğlere büyük ölçüde uyum sağlanması anlamını taşımaktadır. Standart dışında e-imza uygulamasının yerine getirmesi gereken şartlar da mevcuttur.

PDF formatı ise RFC 3778 "The application/pdf Media Type" [3] ile tanımlanmış uluslararası bir standart olmasına rağmen, E-imzalama ve imza doğrulama ile ilgili uluslararası kabul görmüş bir standardı bulunmadığından dolayı PDF formatında atılan e-imza'nın geçerliliği mevcut pdf imzalama kütüphaneleri çerçevesinde uygulama geliştirici'nin insiyatifi dahilinde olacaktır.

VI. ARŞİVLEME

Hukuki açıdan incelediğimiz XAdes standardı esasen uzun dönemli imzaları tanımlar. Uzun dönemli imzaların temel hedefi, imzalı doküman arşivleme ve ilerki bir tarihte yasal zeminde imzayı doğrulayabilmekdir.

PDF'in de, ISO tarafından Adobe un desteği ile yayınlanmış olan, arşivleme standardı (ISO 19005-1) [4] mevcuttur. Bu standart ile PDF formatı arşivlemeye uygun hale getirilmiş, örneğin PDF içerikte javascript ve çalıştırılabilir dosyaların kullanımı engellenmiştir.

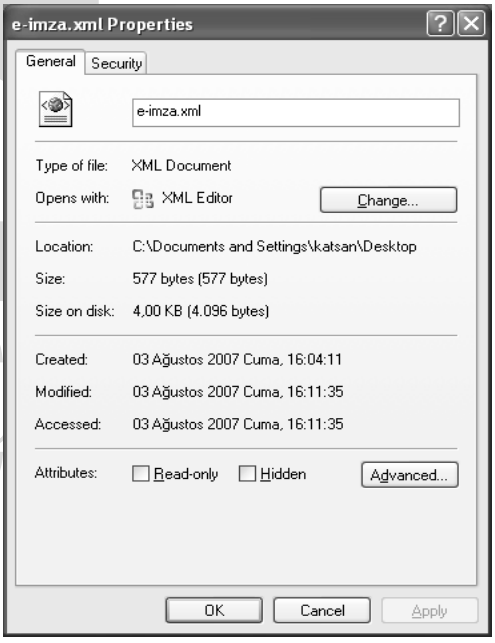
Arşivleme noktasından bakıldığında, XML formatının e-imzalı doküman arşivleme konusunda daha etkin bir format olduğu görülmektedir.

VII. VERİ BÜYÜKLÜĞÜ (BOYUTU)

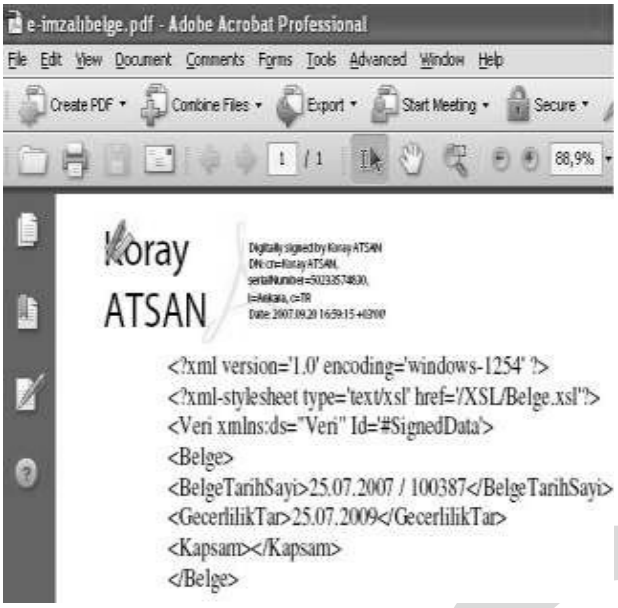
XML formatı, düz metin bazlı bir format olduğundan dolayı, aynı içerik için, PDF formatına göre daha küçük boyutta olacaktır. Aşağıdaki şekillerde, aynı içerik için bir XML dosya ile PDF dosyanın boyutlarının karşılaştırılması görülmektedir. Aynı veriler için e-imzalı verinin boyutlarının da aynı olması beklenir. Dolayısıyla, boyut farkı tamamen format farkından ileri gelmektedir.

Windows sisteminde, örnek imzalı XML formatındaki dosyanın boyutu 577 byte iken, PDF formatındaki imzalı dosyanın boyutu 80.5 kb olarak görülmektedir.

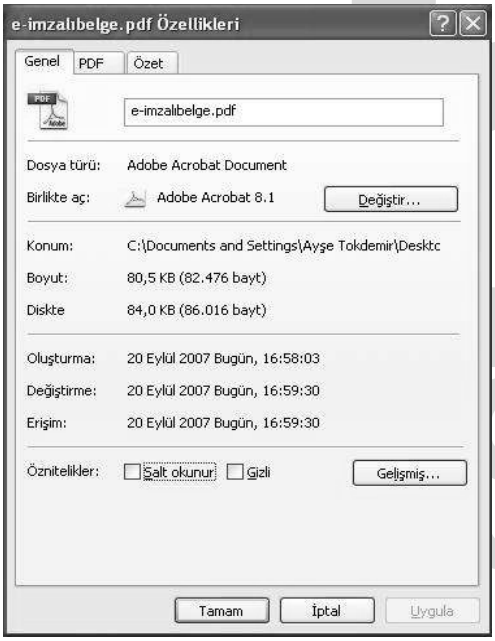
Şekil 3 : XML Formatında İmzalı Veri Örneği



Şekil 4 : İmzalı XML Veri'nin Windows Sisteminde kapladığı boyut



Şekil 5 : PDF formatında İmzalı Veri Örneği



Şekil 6 : İmzalı PDF Veri'nin Windows Sisteminde kapladığı boyut

VIII. STANDARDİZASYON

Standartlaşmanın anlamı temelde herkesin aynı dili konuşabilmesidir. E-imza için standartlaşma, herhangi bir kişi veya kurumun imzaladığı belge/dosyaların, diğer bir kişi/kurum tarafından e-imzalı olduğunun anlaşılabilmesi ve işlenebilmesi anlamına gelmektedir. E-imza belirli bir kurum veya kuruluş içinde kullanılıyorsa, standartlaşma problemi bir nebze de olsa çözülmüş kabul edilebilir, şöyle ki: belirli bir standardı uygulamamış (kendi standardınızı uygulamış) veya o standardı yanlış uygulamış olabilirsiniz. Her iki durumda da sadece kurum uygulaması kullanıldığından dolayı, muhtemelen bir problem yaşamazsınız.

Standardın uygulanması gerekmediğine veya maliyetinin yüksek olduğuna inanılıyorsa, fakat aynı zamanda diğer bir uygulama ile konuşmak gerekiyorsa, bu durumda, diğer uygulama ile anlaşabilmek için standart uyumu sağlayan bir gateway kullanmak faydalı olacaktır.

XML formatının hem kendisi hem de e-imzası ile ilgili olarak oturmuş standartları vardır :
"Extensible Markup Language (XML) 1.0 W3C Recommendation 16 August 2006" , RFC 3275 (Extensible Markup Language) XML-Signature Syntax and Processing [5] standartları uluslar arası kabul görmüş ve yaygınlaşmış standartlardır. XML imza'yı gerçeklerken bu standardın kullanılması kaçınılmaz olacaktır.

PDF'de kabul görmüş bir uluslar arası standart olmasına rağmen, e-imza konusunda henüz kabul edilmiş ortak bir standardı yoktur ve PDF imzalama için, "Adobe Systems" ın kendi spesifikasyonu kullanılmaktadır.
Standardizasyon açısından XML'in PDF den birkaç adım önde olduğunu söylemek mümkündür.

IX. SONUÇ

Sonuç olarak, bu iki formatın da birbirlerine üstün ve zayıf oldukları taraflar vardır. Bu noktada yapılacak olan seçimin, ihtiyaçlara göre şekillenmesi gerektiğini söyleyebiliriz. XML formatının, boyut, standart kullanım, arşivleme ve hukuki açıdan avantajları olduğunu söylemek mümkündür. Bunun yanında PDF formatı da, uluslararası e-imza standartlarına uyum ile ilgili bir kaygı yoksa (örneğin sadece kurum içinde kullanılacaksa, bu durumda kurum içinde bir e-imza politikası yayınlayarak kullanıcılar bu politika ile bağlanabilir.) görsellik ve kullanım kolaylığı ön planda olması gerekiyorsa tercih edebilir.

KAYNAKLAR

[1] http://www.tbmm.gov.tr/kanunlar/k5070.html - 5070 sayılı E-imza kanunu
[2] http://www.w3.org/TR/XAdES/ - XML Advanced Electronic Signatures (XAdES)
[3] http://www.faqs.org/rfcs/rfc3778.html - RFC 3778 The application/pdf Media Type
[4] http://www.iso.org - ISO 19005-1, Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)
[5] http://www.faqs.org/rfcs/rfc3275.html - RFC 3275 - (Extensible Markup Language) XML-Signature Syntax and Processing
[6] http://www.ascertia.com/Products/pdfsignseal/default.aspx - Pdf Sign&Seal
[7] http://uri.etsi.org/01903/v1.1.1/ - ETSI TS 101 903 V1.1.1, XML Advanced Electronic Signatures (XAdES)
[8] http://www.adobe.com/products/acrobat/pdfs/pdfarchiving.pdf - Pdf as a Standart for archiving