Güvenli Elektronik Arşivleme: Standartlar, Yapılar ve İşlevler

Mert Özarar, Burak Kırımer, Musa Öner Demirkol

***Öz* – Bir elektronik imzanın, oluşturulmasının üzerinden uzun bir süre geçtikten sonra doğrulanabilmesi, problemli olmaya aday bir konudur. Aradan geçen zaman nedeniyle ortaya çıkabilecek farklı sorunlar vardır. Bildiride, bu problemin çözümüne yönelik "Uzun Dönemli Elektronik İmzalar" kullanılarak, geleneksel arşiv sistemlerinin yerine elektronik imzalı ve zaman damgalı arşivlemeye geçilmesi gerektiği vurgulanmaktadır. Uzun ömürlü elektronik imzaların güvenli arşivlenmesi amacıyla uygulanması gereken standartlar ve yapılar sunulmaktadır. Arşive erişimin kimlik denetimiyle sağlandığı, verilerin farkında olmadan ya da kötü niyetli olarak değişime uğrayamayacağı ve sorumlusunun mesul tutularak zaman içerisinde içerdiği dokümanların tekrar kullanılabilir halde olduğu anlatılır. Her güvenli elektronik arşivlemede yer alması gereken işlevlerin, arşivleme, durum kontrolü, doğrulama, ihraç etme ve silme olduğuna yer verilmektedir.**

***Anahtar Kelimeler* – Zaman damgası, uzun dönemli elektronik imza, güvenli elektronik arşivleme**

I. GİRİŞ

Günümüz enformasyon çağı olduğundan, zamanımızın önemli bir kısmını herkes tarafından erişilebilen ağ üzerindeki bilgileri işleyerek harcamaktayız. Gelişen internet teknolojileriyle beraber elektronik formattaki belge sayısı üstel olarak artmaktadır. İşlem kayıtları, kitaplar, bilimsel çalışmalar, sözleşmeler, faturalar ve hatta kamu işlemlerinde kullanılan kağıt miktarı on sene önceki ile kıyaslanmayacak düzeydedir. Çoğu zaman, kullanılan dokümanların uzun dönemli olarak tutulması gerekir. Dokümanlara gelecekteki bir zaman diliminde, kontrol ya da bilgi amaçlı erişilmek istenebilir. Belgelerin kimin sorumluluğunda olduğunun ve geçen zaman içerisinde tahrifata uğrayıp uğramadığının bilinmesi kritik bir husustur. Elektronik imza ve şifreleme teknolojileri sayesinde bir elektronik dokümanın okunabilirliği, kaynağının doğruluğu, bütünlüğü ve geçerliliği sağlanır [1].

Zaman Damgası, 5070 sayılı Elektronik İmza Kanunu'nun üçüncü maddesinde "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt," olarak tanımlanmaktadır. Zaman damgası elektronik ortamda doküman ve sözleşme gibi elektronik verilerin, belirli bir zamandan önce var olduğunu kanıtlamak için kullanılır.

Mert Özarar, Burak Kırımer, Musa Öner Demirkol, *TÜRKTRUST Bilişim Güvenliği Hizmetleri A.Ş.*

Elektronik ortamdaki işlemlere güvenilir zaman bilgisi eklenebilmesini sağlayan zaman damgası, üzerinde zaman bilgisi olması gereken elektronik başvuru, tutanak, sözleşme ve benzeri her türlü elektronik veri üzerinde kullanılabilir [9].

Zaman içerisinde dokümanların bütünlüğü ve kaynağının doğruluğu elektronik imza ile sağlansa bile, imzaların atılmasını sağlayan elektronik sertifikaların ömrü sınırlı olduğundan, geçerlilik kontrolü bakımından yine bir açık doğabilir. Gerçek hayattan örneklemek gerekirse, şirket belgeleri, abonelik sözleşmeleri ve senetler gibi çoğu doküman uzun süre geçerliliğini devam ettirebilir ama onaylayan imzalar gizli anahtarlarının güvenlik sorunları ve idari olarak sertifikalarda yer alan bilgiler sebebiyle kısıtlı ömre sahiptirler. Olası güvenlik sorunları arasında gizli anahtarın tutulduğu aracın çalınması ya da kriptanalizin zaman içerisinde gizli anahtarı açığa çıkarması gibi örnekler sayılabilir. Dolayısıyla, ileri destek olmaksızın, tek başına elektronik imzalar, imzalı dokümanların uzun dönemli tutulması açısından uygun değildirler. İmza doğrulaması yaparken, dokümanın imzalanmış olduğu andaki gizli anahtar güvenliği ve sertifika geçerliliğinden emin olmak (hala "gizli" ve münhasıran sahibine ait) son derece önemli bir noktadır.

Bu problemin üstesinden gelmek için RFC 3161'de [3] belirtilen, "Uzun Dönemli Elektronik İmzalar" kavramı ortaya atılmış ve geleneksel arşiv sistemlerinin yerini elektronik imzalı ve zaman damgalı arşivleme tekniğinin alacağı öne sürülmüştür.

Bu bildiride, elektronik arşivleme sistemlerinde roller, yapılar, standartlar ve işlev detayları açıklanacaktır. Tasarım kararları başlıklar halinde sunulacak ve güvenli bir hizmetin verilebilmesi için hangi etmenlerin önem taşıdığı vurgulanacaktır.

Bildirinin organizasyonu şöyledir: İkinci kısımda uzun dönemli elektronik imzaların doğrulanmasında karşımıza çıkan sorunlar ele alınmakta, üçüncü kısımda elektronik imzalı bir dokümanın zaman damgalanarak nasıl güvenli arşivleneceği anlatılmakta, dördüncü kısımda uzun dönemli elektronik imza standartları ve yapıları ele alınmakta, beşinci kısımda günümüzde dünyadaki güvenli elektronik arşivleme uygulamalarından bahsedilip altıncı kısımda makale sonuçlandırılmaktadır.

II. UZUN DÖNEMLİ İMZA DOĞRULAMADA YAŞANABİLECEK SORUNLAR

Bir elektronik imzanın, oluşturulmasının üzerinden uzun bir süre geçtikten sonra doğrulanabilmesi, problemli olmaya aday bir konudur. Aradan geçen zaman nedeniyle ortaya çıkabilecek sorunlar şunlardır:

1. İmza sahibi sertifikanın imza oluşturulduğu andaki geçerlilik durumunun bilinememesi: Sertifikalar geçerlilik sürelerini henüz doldurmamışken, geçerlilik durumlarını Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) kurumların yayınladığı iptal listeleri (CRL) veya sağladıkları durum sorgulama protokolü hizmeti (OCSP) aracılığıyla öğrenmek mümkündür. Ancak geçerlilik süresi sona eren sertifikalar, iptal edilmişlerse bile CRL içeriğinden çıkarılırlar. OCSP ise anlık durumu belirten bir protokol olduğu için, OCSP ile herhangi bir sertifikanın geçmişteki bir anda geçerli olup olmadığını sorgulamak mümkün değildir.

2. ESHS kayıtlarından geçmişteki bir iptal listesini elde etmek mümkün olabilir, ancak eski iptal listelerinin çevrimiçi olarak yayınlanması yaygın bir uygulama olmadığı gibi, uzun bir süre geçtikten sonra ESHS'nin faaliyetlerine devam etmiyor olması olasılığı göz ardı edilemez.

3. ESHS gizli anahtarının çalınması: İmza sahibi sertifikayı oluşturmakta kullanılmış olan ESHS gizli anahtarının çalınması, ESHS tarafından üretilmiş geçerli sertifikalar gibi görünen sahte sertifikaların üretilmesine imkan tanıyacaktır. Böyle bir hırsızlık yaşanırsa, doğrulanan bir imzaya güvenmek için hırsızlık anından önce oluşturulmuş geçerli bir sertifika ile atıldığını kanıtlamak gerekecektir.

4. Sertifikada ve imzada kullanılan kriptografik algoritmaların güvenilirliklerini kaybetmiş olması: Sertifikalar ve imzalar oluşturulurken kullanılan özet algoritmaları (örneğin SHA-1) veya şifreleme algoritmaları (örneğin RSA) aradan geçen zamanda kriptografi ve teknoloji alanındaki gelişmeler nedeniyle güvenilirliklerini kaybedebilirler. Böyle bir gelişme, herhangi bir gizli anahtar hırsızlığı olmaksızın sahte sertifika oluşturma veya sahte imza oluşturma imkanlarını kötü niyetli kişilere tanır. Bu nedenle, doğrulanan eski bir imzanın, bu sahteciliğin teknik olarak mümkün olmadığı bir anda oluşturulmuş olduğunu kanıtlamak önem taşıyacaktır.

III. GÜVENLİ ZAMAN DAMGALI E-İMZA

Zaman damgası elektronik bir belgenin belirli bir anda varlığının tasdiğidir. Elektronik verinin korunmasına yönelik e-imza ile beraber delil niteliği taşıması açısından gerekli bir araçtır. Zaman damgası hizmeti, Zaman Damgası Hizmet Sağlayıcıları (ZDHS) tarafından verilir. Güvenli bir elektronik arşivleme için önceki kısımda yazdığımız nedenlerden ötürü zaman damgasının e-imza ile tümleşik şekilde kullanılması gerekir. Elektronik imzalı bir belgenin kullanım süresi zaman damgalama hizmeti ile uzatılabilir [4, 5].

Genelliği bozmadan, belirli anahtar uzunlukları ile açık metin D dokümanın elektronik imzası δ olan bir elektronik imzalama tekniğini varsayalım [9]. Gizli anahtar açığa çıkması, hedef uzunluk için sayısal hesaplama gücünün artması ya da algoritmada var olan bir açığın ortaya çıkması gibi herhangi bir sebepten ötürü bir zaman sonra imza geçersiz olabilir. Bu noktada doküman-imza çiftinin güvenilirliği şüphelidir zira orijinal sahibinin dışında başkaları da imzalama yapabilir. Bununla beraber, eğer (D, δ) çifti imza geçerliliğini yitirmeden zaman damgalansaydı, imza hala geçerli olacaktı çünkü imzanın atıldığı anda sadece ve sadece orijinal sahibinin sorumluluğunda olacağı garanti altında olacaktı. Anahtar açığa çıksa dahi, anahtarın açığa çıkış tarihi doküman üzerindeki zaman bilgisi ile çelişeceğinden sorun teşkil etmeyecekti.

Güvenlik açısından bakacak olursak ZDHS'ye sadece özet değer yollandığından gizlilik sağlanmış olunur [2]. Elbette ki hem imzalayan hem doğrulayan taraflar ZDHS'ye güveneceğinden dolayı bütünlük ve kimlik denetimi de vardır. Zaman damgasız elektronik imzalar sertifika iptal olunca geçersiz olacağından, inkar edilememezlik prensibine uymak için mutlaka zamanı da dokümana iliştirmek gereklidir. Hatta bu prensibi daha da sağlamlaştırmak amacıyla bağlama zaman damgası tasarıları geliştirilmiştir. Zaman damgalı verinin geçici sırasının inkar edilemez biçimde belirlenmesi amacıyla kullanılıp, ZDHS'nin mesuliyetini öne çıkarırlar. Altında yatan nokta, ileride gelecek zaman damgası isteklerinin ve özet değerlerinin bilinemeyeceğidir. Eğer belirli bir zaman damgası önceki zaman damgalarından kısımlar içeriyorsa, aralarında zamana bağımlı bir kısmi sıra kurulur ve güven ile inkar edilemezlik hiyerarşisi bu şekilde sağlanır.

IV. UZUN DÖNEMLİ ELEKTRONİK İMZA YAPILARI

İmzaların uzun dönemli saklanmasında yaşanacağı öngörülen sorunlara karşı tedbir alabilmek amacıyla, imzaların gerekli ek verilerle birlikte depolanması bir çözüm önerisi olarak sunulmuştur. İmza veri yapısı standartlarına bağlı olarak bu konuda iki standart geliştirilmiştir: Kriptografik Mesaj Sözdizimi (CMS) yapısındaki imzalar için CMS İleri Elektronik İmzalar (CAdES) [11], XML yapısındaki imzalar için XML İleri Elektronik İmzalar (XAdES) [12]. Bildirinin bu bölümünde CAdES veri yapıları incelenmiştir

CAdES bünyesinde tanımlanan veri yapıları, çekirdekte yer alan imza verisinin üzerine sağlıklı bir arşivleme için gerekli verilerin katmanlar halinde eklenmesini sağlamaktadırlar [7, 10]. Dokümanda tanımlanan yapılar ve olası problemlere karşı tedbirlere nasıl hizmet ettikleri aşağıda özetlenmiştir.

İmza verisi (Electronic Signature – ES): Çekirdekte yer alan imza verisidir. Yapısı CMS standardında, mevcut durumda kullanılmakta olan imza yapısıdır. CAdES, imza yapısının zorunlu içeriğine ek olarak, imzanın oluşturulma ilkelerini belirten bir tanımlayıcı numaranın da imzalı veri içinde imzalı özellikler (Signed Attributes) alanında bulunmasını öngörmektedir. Böyle bir numara kullanılmıyorsa, imza oluşturan taraf ilgili alanı boş bırakarak, imza oluşturma ilkelerinin imzalı içerik ve dış veriler tarafından ima edildiğini belirtebilmektedir.

Zaman damgalı imza (ES with Timestamp – ES-T): Kriptografik imza değerinin zaman damgalanması ve bu damganın bir ek değer olarak imza yapısına yerleştirilmesiyle oluşturulur. Bu zaman damgası imzanın belirtilen zamandan önce oluşturulmuş olduğunu belgeleyerek imzanın uzun dönemli güvenilirliği konusunda önemli bir boşluğu doldurur. Zaman damgası imzaya, imza oluşturulduktan hemen sonra imza sahibi tarafından eklenebileceği gibi, imzayı doğrulayan başka bir tarafça da eklenebilir. İmza doğrulama ilkeleri açısından imzanın oluşturulma zamanı ile üzerindeki zaman damgasının belirttiği zaman arasındaki fark bir kıstas oluşturabilir. İlkeler, bu farkın belirli bir değerin üzerinde olması halinde imzayı güvenilir kabul etmeyecek şekilde düzenlenebilirler.

Tam doğrulama verisi içeren imza (ES with Complete Validation Data – ES-C): ES-T verisine ESHS sertifika referanslarının ve geçerlilik durum bilgisi referanslarının eklenmesiyle oluşturulur. ESHS sertifika referansları, imza sahibi sertifikanın bağlı olduğu ESHS kök ve alt kök sertifikalarının referanslarıdır. Sertifika referansları, sertifikaların "imzalayan sertifika adı", "seri numarası" ve sertifika özeti değerlerinden oluşurlar. Geçerlilik durum bilgisi referansları, imza sahibi sertifika ile bağlı olduğu alt kök sertifikaların geçerliliklerini belgeleyen iptal listelerinin (CRL) veya OCSP sorgusu cevaplarının referanslarıdır. Bu referanslar, iptal listelerinin veya OCSP sorgu cevaplarının özet değerlerinden oluşurlar. İmza yapısına ESHS sertifika referansları ile geçerlilik durum bilgisi referansları eklendiğinde, imza sahibi sertifikanın hangi ESHS sertifikası zincirine bağlı olduğu ve geçerlilik durumunun ESHS'nin hangi bildirimiyle (CRL veya OCSP), ne zaman kontrol edildiği açık olarak ifade edilmiş olur. Bu yapının kullanılması, zaman içerisinde ESHS sertifikaları ve geçerlilik durum kontrolleri hakkında güvenlik tereddütlerinin ortaya çıkması dolayısıyla imzanın güvenilirliğinin sorgulanması durumunda fayda sağlar. İmza yapısı, imza sahibi sertifikanın geçerlilik kontrol verilerine referanslar barındırdığı için bu verilere (ESHS sertifikalarına ve CRL/OCSP verilerine) ulaşılarak sertifikanın belirtilen zamandaki geçerliliğini tekrar kontrol etmek mümkün olacaktır. Ancak böyle bir kontrolün yapılabilmesi için ilgili sertifikalar, iptal listeleri ve OCSP sorgusu cevaplarının ulaşılabilir durumda tutulması gerekmektedir.

Genişletilmiş doğrulama verisi içeren imza (ES with eXtended Validation Data – ES-X): ES-C verisine, referansları verilen ESHS sertifikaları ile iptal listesi ve OCSP sorgusu cevaplarının kendilerinin eklenmesiyle oluşturulur. Böylece doğrulama anında ESHS kök sertifikası dışında hiçbir dış veri kullanılmasına gerek kalmaz. Tüm sertifikalar, iptal listeleri ve OCSP cevapları kök sertifikadan başlayan bir zincirin halkaları olarak doğrulanabilirler.

Arşivlenmiş doğrulama verisi içeren imza (ES with Archive Validation Data – ES-A): ES-X verisindeki bilgilere zaman damgası vurularak bu zaman damgasının veriye eklenmesiyle oluşturulur. Amacı zaman damgası hizmet sağlayıcısı sertifikaları ve zaman damgalarında kullanılan algoritmaların zaman içinde zayıflamasına karşı tedbir almaktır. ES-A yapısı oluşturulurken vurulan zaman damgasında, imza ve sertifikalardakilere kıyasla daha uzun bir anahtar ve mümkünse daha kuvvetli bir algoritma kullanılmalıdır. Böylece, imza ve sertifikadaki algoritmalar güvenli olma özelliklerini belirli bir süre sonra kaybetseler bile, ES-A yapısındaki zaman damgası içerideki verilerin doğruluğunu daha uzun bir süre boyunca belgeleyebilecektir. ES-A yapıları başka ES-A yapılarının üzerine yeni bir zaman damgası eklenerek de oluşturulabilirler. Bu özellik, ES-A yapılarının üzerine periyodik olarak daha kuvvetli algoritmalarla zaman damgası ekleyerek arşivleme süresini sürekli uzatma imkanını tanır.

V. GÜVENLİ E-ARŞİVLEME İŞLEVLERİ

Değişik güvenli elektronik arşivleme yazılım ve donanım ürün ve çözümleri küresel pazarda yer almaktadır [6]. Hukuksal açıdan yeterli olmakla beraber, teknik açıdan kısmi güvenli çözümlerdir. Yerel kanunlara göre, ülkeden ülkeye amaçları, uygulama prensipleri ve güvenlik seviyeleri değişebilir. Yayınlanan tebliğler altyapıyı belirlemede kıstas oluşturur. Bazı ülkelerde elektronik dokümanların "worm-media" halinde depolanması güvenli elektronik arşivleme aracı olarak kullanılmaktadır [8].

Varolan çözümlerin standart olarak içlerinde barındırmaları gereken hizmetler vardır. Son kullanıcı ile olan iletişimde bu işlevler sayesinde etkileşim kurulur. Kısaca özetlemek gerekirse beş başlıkta toplayabiliriz.

1) *Arşivleme*: Tek ya da grup halindeki dokümanların korunumsal vasıflarının yaratılmasını tetikler.
2) *Durum*: Arşivleme işleminin ilerlemesi hakkında bilgi verir.
3) *Doğrulama*: Belli bir dokümanın korunumsal vasıflarını işlemek için doğrulama motorunu tetikler.
4) *İhraç*: Belli bir dokümanın korunumsal vasıflarının ihracı (dosyaya yazılması, diske depolanması) için gereklidir.
5) *Silme*: Arşivlenen dokümanların silinerek arşivden çıkarılması için kullanılır.

Genelliği bozmadan sağlanması gereken şartlar;

1) Arşivlenen dokümanlara uygulanan elektronik imzaların, imzalayan sertifika iptal olsa ya da geçerliliğini yitirse dahi kullanılır olması,

2) Doküman tipinden bağımsız olarak arşivlenen verinin bütünlüğünün herhangi bir zaman dilimi için korunması,
3) Arşivlenen veri ya da dokümana ait tüm değişikliklerin takip edilebilmesi,
4) Arşivlenen verideki bütün önemli alanların (sahibi, yeri, yaratılma zamanı, vb.) herhangi bir zaman çözümlenebilmesi
5) Arşivlenme teknolojisi değişse dahi arşivlenen verinin okunabilir olması,
6) Doğrulamada kullanılacak tamamlayıcı verinin her zaman hazır olması ve üçüncü güvenilir taraflarca kontrolde tutulması

olarak sıralanabilir.

VI. SONUÇLAR

Bu makalede, güvenli elektronik arşivlemede kullanılan standartlardan, yapılardan ve işlevlerden bahsedilmiştir. Herhangi bir dokümanın geçmişte imzalanmış olduğu anda sertifikanın geçerli durumda bulunduğundan emin olmak güvenlik açısından hayati bir noktadır. Makalede bahsedilen nedenlerden ötürü bu kontrolü yapmak tek başına saklanmış imzalar için mümkün olmayabilir. Bu sorunun üstesinden gelmek için uzun dönemli elektronik imzalar kullanılır. Elektronik imzaya zaman damgası ve geçerlilik durum bilgisi eklenerek oluşturulan bu yapılar sayesinde güvenli arşivleme yapılabilir.

Zaman damgası anahtarları ve algoritmalarıyla ilgili yaşanabilecek sorunlar da incelenmiştir. İlgili referanslarda belirtilen standartlar ve bunun ışığında ortaya atılan yapılar sayesinde gerçekleştirim yapılabilir. Her güvenli elektronik arşivlemede yer alması gereken işlevler vardır. Bunları arşivleme, durum kontrolü, doğrulama, ihraç etme ve silme olarak verebiliriz.

V. KAYNAKLAR

[1] D. Lekkas., "Establishing and managing trust within the Public Key Infrastructure", *Computer Communications,* sayfa 1815-1825, Vol. 26, No. 16, 2003.
[2] Dave Bayer, Stuart Haber ve W. Scott Stornetta. "Improving the efficiency and reliability of digital time-stamping". Methods in Communication, Security, and Computer Science - Sequences'91, sayfa 329-334, 1992.
[3] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). http://www.ietf.org/rfc/rfc3161.txt
[4] Meelis Roos. "Integrating time-stamping and notarization". MSc Thesis, Tartu University, http://home.cyber.ee/mroos/thesis/. Mayıs 1999.
[5] Petros Maniatis ve Mary Baker. "Enabling the archival storage of signed documents". *FAST '02: Proceedings of the 1st USENIX Conference on File and Storage Technologies*, 2002.
[6] R. Sproull, H. Besser, J. Callan, C. Dollar, S. Haber, M. Hedstrom, M. Kornbluh, R. Lorie, C. Lynch, J. Saltzer, M. Seltzer ve R. Wilensky. "*Building an Electronic Records Archive at the National Archives and Records Administration: Recommendations for a Long-term Strategy*" National Archives and Records Administration, 2005. R. Sproull ve J. Eisenberg, editörler.
[7] Stuart Haber ve W.Scott Stornetta. "How to time-stamp a digital document". Journal of Cryptology, 3(2): 99-111, 1991.
[8] Surety. http://www.surety.com.
[9] Stuart Haber ve Henry Massias. "Time-stamping". In H.C.A. van Tilborg, editor, *Encyclopedia of Cryptography and Security*. Springer, 2005.
[10] World Wide Web Consortium (W3C). Resource description framework (RDF). http://www.w3.org/RDF/.
[11] ETSI TS 101 733 v1.7.3, "Electronic Signatures and Infrastructures, CMS Advanced Electronic Signatures (CAdES)". Ocak 2007.
[12] ETSI TS 101 903 v1.3.2, "Electronic Signatures and Infrastructures, XML Advanced Electronic Signatures (XAdES)". Mart 2006.