E-DEVLET UYGULAMALARI İÇİN ELEKTRONİK İMZA FORMATLARI

GONCA HÜLYA SELÇUK
TÜBİTAK – UEKAE
Kamu Sertifikasyon Merkezi
gonca.selcuk@tubitak.gov.tr

ÖZET : Elektronik imzanın geçerliliği, imza oluşturulurken kullanılan elektronik sertifikanın geçerliliğine bağlıdır. Elektronik imzanın tam olarak elle atılan imzanın yerini alabilmesi için uzun süre geçerliliğini koruyabilmesi gerekmektedir. Ancak, elektronik imza söz dizimini tanımlamış olan Kriptografik Mesaj Söz Dizimi (CMS) ile bu ihtiyaç karşılanamamaktadır. Bu ihtiyacın karşılanabilmesi için elektronik imzaların uzun süre geçerliliklerini koruyabilecekleri genişletilmiş imza formatları bulunmaktadır. Bu çalışmada, Avrupa Birliği Telekomünikasyon Standartları Enstitüsü (ETSI) tarafından tanımlanmış olan bu formatlar tanıtılacaktır. Ayrıca, bu imza formatlarının hangi durumlarda kullanılabileceği ile ilgili önerilerde bulunulacaktır.

ANAHTAR KELİMELER: Elektronik imza, uzun süre geçerlilik, zaman damgası, arşiv

ELECTRONIC SIGNATURE FORMATS FOR E-GOVERNMENT APPLICATIONS

ABSTRACT : Validation and verification of the electronic signature are dependent to validation of the signing certificate. Due to supersede the signature, the need of long standing electronic signature is occured. This need can not be implemented by Cryptographic Message Syntax (CMS) which defines the syntax for electronic signature. For long standing signatures there are extended signature formats. In this paper, those formats which have been defined by European Telecommunications Standards Institute (ETSI) will be overviewed. Moreover, the proposals in which those signature formats can be used will be given.

KEYWORDS : Electronic signature, long standing, time stamp, archive

1. Giriş

İçinde bulunduğumuz iletişim çağında, kamu ve özel sektördeki firmalar faaliyetlerinin büyük bir kısmını dijital ortama taşımış veya taşımaktadır. Bu faaliyetlerin başarılı bir biçimde devam etmesi için güvenilir bir yola ihtiyaç duyulmaktadır. Elektronik imza da bu güvenilir yolda, dijital verinin korunmasında ve elektronik faaliyetlerdeki güven unsurunun sağlanmasında önemli bir parçayı oluşturmaktadır.

İmza, bir kimsenin, bir yazının altına bu yazıyı yazdığını veya onayladığını belirtmek için her zaman aynı biçimde yazdığı ad veya işarettir [1]. Elektronik imza ise, 5070 sayılı Elektronik İmza Kanunu [2]'nda tanımlandığı şekliyle; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi ifade eder. Elektronik İmza Kanunu'nda öngörüldüğü üzere, elektronik imza elle atılan imza ile aynı hukuki sonuçları doğuran, imzanın dijital ortamda kullanılan halidir. Elle atılan imzanın değişmeyen biçiminin aksine, elektronik imza verisi değişken bir değerdir. Elektronik imza; imzalanacak olan verinin, imzayı atacak şahsa ait özel anahtar ile birlikte birtakım matematiksel işlemlerden geçirilmesi sonucunda oluşturulan ve imzalanacak veriye eklenen sayısal bir veridir.

Elektronik imza oluşturma işlemi için tanımlanmış söz dizimi, Kriptografik Mesaj Söz Dizimi (Cryptographic Message Syntax - CMS)'dir. CMS; imza oluşturmanın yanısıra, özetleme, doğrulama ve isteğe bağlı mesaj içeriğinin şifrelenmesi için de kullanılır [3].

CMS [3], veri korunması için bir sarmalama (encapsulation) söz dizimi tanımlar. Bu söz dizimi; elektronik imzaları, şifrelemeyi ve çoklu sarmalama

işlemini de destekler. Önceden sarmalanmış bir veriye, başka bir şahıs tarafından da elektronik imza eklenebilir. Bunun yanısıra, elektronik imzaya eklenecek ve içerik ile birlikte imzalanacak olan imza tarihi gibi bazı eklentiler de CMS tarafından tanımlanmıştır. Seri imza gibi, imza değeri oluşturulduktan sonra imza ile ilişkilendirilecek olan diğer eklentiler de bu söz diziminde bulunmaktadır. CMS'e göre herhangi tipteki içeriğe sahip olan imzalı veri, içinde sıfır veya daha fazla imza değeri barındırabilir. İmzacılar, farklı tipteki içerikleri paralel olarak birçok kere imzalayabilirler [3].

İmzanın geçerlilik kontrol girdisi, imzadaki içerik özeti ve imzacının açık anahtarıdır. İmzanın doğrulanması için imzacının açık anahtarı, imzalı veride bulunan "sertifikalar verisi" içerisinde bulunmalıdır. Ayrıca, imza doğrulayıcı tarafından hesaplanan içerik özeti ile imzada bulunan içerik özetinin uyumlu olması gerekmektedir. İmzanın içerik özeti hesaplanırken kriptografik algoritmalar kullanılır. Zamanla bu algoritmaların güvenilirliği azalmakta ve zayıflamaktadır. Bu nedenle, elektronik imza değeri de zamanla zayıflamakta ve kırılabilir hale gelmektedir.

Bu çalışmada, elektronik imza oluşturulurken kullanılan algoritmaların zaman içerisinde zayıflamasına karşın imzanın nasıl güçlendirileceğinden bahsedilecektir. İmza oluşturulurken kullanılan algoritmalar zayıflasa da imza, eklenebilen ek kontrol bilgileri ile genişletilip güçlendirilebilir. İmzaya eklenebilen bu kontrol bilgileri için Avrupa Birliği Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute - ETSI) tarafından tanımlanmış olan genişletilmiş imza formatları tanıtılacaktır.

2. İmzanın Geçerliliği Uzun Süre Nasıl Korunur?

Elektronik imza değeri oluşturulurken elektronik bir sertifika kullanılır. Elektronik İmza Kanunu [2]'nda tanımlandığı şekliyle; elektronik sertifika, imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı ifade eder. Elektronik sertifikaların belirli geçerlilik süreleri bulunmaktadır. Elektronik Sertifika Hizmet Sağlayıcı (ESHS)'sından alınmış bir elektronik sertifika, yine bu ESHS tarafından belirlenmiş olan zaman aralığında geçerli elektronik imza oluşturabilmektedir. Sertifikanın geçerlilik süresi içinde oluşturulmuş olan imza, bu sertifikanın geçerlilik süresi dolduğunda veya sertifika iptal edildiğinde geçersiz duruma düşecektir. İmzayı atan kişinin belirleyeceği imza tarihi verisi de imzanın doğrulanması sırasında güvenilir olarak kabul edilemez çünkü kişi bu tarihi istediği şekilde belirleyebilmektedir. Bu noktada; imzada, imza tarihi dışında güvenilir bir zaman verisinin ve sertifikanın bu güvenilir tarihte geçerli olduğuna dair bir ispatın bulunmasının önemi belirginleşmektedir. İmzaya eklenen güvenilir zaman verisi, imzanın bu güvenilir tarihten önce var olduğunun garantisidir. İmzanın geçerliliği, dolasıyla sertifikanın geçerliliği güvenilir zamana göre kontrol edileceğinden sertifika, zaman damgasının alındığı tarihten sonra iptal edilmiş olsa bile imza geçerli olacaktır.

Ancak imzaya güvenilir zaman verisinin eklenmesi de imzanın sürekli olarak geçerli olduğunu garanti etmemektedir. Bu nedenle, imzanın geçerliliğinin kontrol edildiği sertifika iptal listesi (SİL / Certificate Revocation List – CRL), çevrimiçi sertifika durum kontrolü bilgisi (ÇİSDUP / Online Certificate Status Protocol – OCSP) gibi birtakım ek kontrol bilgilerinin de imzaya eklenmesi gerekmektedir. CMS [3]'te tanımlanan elektronik imza oluşturma söz diziminde, imzaya eklenecek olan bu eklentiler hakkında herhangi bir açıklık getirmemiştir.

Avrupa Birliği Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute - ETSI), CMS'i özelleştirerek bir standart oluşturmuştur. Bu standart ile elektronik imzanın uzun süre geçerliliğini koruyabilmesi için bazı formatlar tanımlanmıştır.

3. Genişletilmiş İmza Formatları

Basit elektronik imza, genel CMS söz dizimi [3] ile oluşturulabilen, temel olarak imzalanan içerik tipini, imzalanan içeriğin özetini ve imzayı atan sertifika bilgisini içeren imzadır. Şartlı elektronik imza ise, basit elektronik imzanın daha önceden tanımlanmış bir şarta göre oluşturulmuş halidir. Basit ve şartlı elektronik imza, temel özelliklerin yanısıra CMS [3] ve ESS (Enhanced Security Services) [4]'te tanımlanmış olan bazı eklentileri de içerebilir. CMS [3], ESS [4] ve ETSI [5] tarafından tanımlanmış olan imza eklentilerinin bir kısmı Tablo 1'deki gibidir. Buna göre; CMS [3] ve ESS [4] tarafından tanımlanmış olan eklentilerden "Seri imza" dışındaki eklentilerin, basit imza oluşturulurken belirlenen imza değeri tarafından korunması gereklidir. Bu nedenle, bu eklentiler ancak basit imzaya eklenebilmektedir. Ancak, bu basit imzanın geçerliliğini uzun süre korumasını sağlamak için imzaya imza değeri oluşturulduktan sonra eklenebilen eklentiler ise ETSI [5] tarafından tanımlanmıştır.

CMS [3] ve ESS [4]'te tanımlanmış olan eklentiler ile oluşturulan elektronik imzalar sadece imzacı sertifikasının geçerlilik süresi içinde geçerlidir. Bu nedenle; basit veya şartlı elektronik imzaların, çevrimiçi işlemlerde veya imzanın geçerliliğinin kısa süreli olarak ispat edilmesinin yeterli olduğu sistemlerde kullanılması önerilmektedir. Ancak, e-devlet uygulamalarında elektronik imzanın

yaygınlaşması ile ortaya çıkan ihtiyaçlar basit elektronik imza karşılanamamaktadır.

Standart	Eklenti	Eklenti imza değeri tarafından korunuyor mu?
CMS	İçerik tipi	Evet
	İçerik özeti	Evet
	İmza tarihi	Evet
	Seri imza	Hayır
ESS	İçerik bilgisi	Evet(İmza tarafından korunmadığı durumlar da olabilir.)
	Belge numarası	Evet(İmza tarafından korunmadığı durumlar da olabilir.)
	İçerik referans bilgisi	Evet
	İmzacı sertifikası	Evet
ETSI	İmza amacı	Evet
	İmzacı yer bilgisi	Evet
	İmzacı özellikleri	Evet
	İçerik zaman damgası	Evet
	İmza zaman damgası	Hayır
	Sertifika referansları	Hayır
	İptal bilgisi referansları	Hayır
	Sertifika değerleri	Hayır
	İptal bilgisi değerleri	Hayır
	Referanslar zaman damgası / İmza ve referanslar zaman damgası	Hayır
	Arşiv zaman damgası	Hayır

Tablo 1

3.1. Zaman Damgalı İmza ve Bütünsel Doğrulama Veri Referanslarını İçeren İmza

İmzanın uzun süre geçerliliğini koruyabilmesi için önemli olan, imzanın bir kez geçerli bulunmasından sonra aylar hatta yıllarca geçerliliğini korumasıdır [5].

Örneğin; taraflar arasında ıslak imza ile imzalanan bir anlaşma, anlaşmanın geçerli olduğu süre zarfında taraflarca saklanmalıdır. Eğer, bu anlaşma imzalanırken elektronik imza kullanılırsa da aynı ihtiyaç doğmaktadır. Anlaşma geçerli olduğu sürece üzerindeki elektronik imzaların da anlaşmadaki taraflarca geçerli olarak korunması gerekmektedir.

Bir imzanın geçerli kabul edilebilmesi için imzacı sertifikasının ve ait olduğu kök sertifikalar zincirindeki sertifikaların da geçerli olması zorunludur. İmzacı sertifikası veya ait olduğu kök sertifikalardan herhangi biri iptal edilmiş veya ilgili sertifikanın geçerlilik süresi dolmuş olsa da imzayı atan ve/veya doğrulayan taraf imzanın atıldığı tarihte ilgili sertifikanın geçerlilik süresi içinde olduğunu kanıtlamalıdır [5].

Zaman Damgası Servis Sağlayıcısı (Time-Stamping Authority - TSA)'ndan alınarak imzaya eklenmiş olan zaman damgası, imzanın alınan zaman damgası tarihinden önce var olduğunu garanti altına almaktadır. İmzaya eklenen zaman damgası, imzanın atılmış olduğu tarihi belirtmez; ancak, imzanın üzerinde bulunan zaman damgası tarihinden önce atılmış olduğunu belirtir. Eğer bir istemci imzanın geçerliliğini garanti altına almak isterse imza atıldıktan kısa bir süre sonra imzaya geçerli bir zaman damgası eklemelidir. Oluşturulan imzanın inkar edilme riskinin azaltılması için, güvenilir zaman göstergesinin imzanın oluşturulduğu zamana olabildiğince yakın olması gerekmektedir [5]. Zaman damgası eklenen imzanın, en az düzeyde basit veya şartlı imza formatında olmalıdır.

Elektronik olarak imzalanmış anlaşmaya tekrar dönmek gerekirse, bu anlaşmadaki imzaların anlaşma süresi boyunca geçerliliğinin korunabilmesi için tarafların anlaşma imzalandıktan kısa bir süre sonra imzalarına zaman damgası almaları gereklidir. Böylece anlaşmadaki her bir imzanın, üzerindeki zaman damgası tarihinden önce var olduğu garanti altına alınmış olunur.

Elektronik imzanın belirli bir tarihten önce var olduğu zaman damgası ile ispat edilebilir; ancak, imzanın geçerli olabilmesi için imzanın atılmış olduğu sertifikanın da bu tarihte geçerli olduğunun ispatı gerekmektedir. Bu nedenle, imzaya sertifika kontrolü için gerekli imzacı sertifikasının üst kök sertifikalar zinciri ve bu sertifikalara ait iptal bilgisinin kontrol edilebileceği bilgiler de eklenmelidir. Ancak, bu bilgiler imzaya eklendiğinde imzanın boyutu çok büyüyeceğinden bu bilgilere ait özet değerler imzaya eklenerek, bilgilerin imza kontrolü sırasında erişilebilecek başka bir yerde saklanması sağlanmalıdır.

İmzacı sertifikasının bağlı olduğu üst kök sertifikalar zincirinin referansları, imzacı sertifikasının ve ait olduğu kök sertifikaların iptal bilgisinin kontrolünün yapılabileceği OCSP ve/veya CRL bilgilerinin referanslarının eklendiği imza formatı, bütün doğrulama veri referanslarını içeren imzadır. Bu format, ETSI [5] tarafından "ES with Complete validation data references (ES-C)" olarak adlandırılmaktadır. Bütün doğrulama veri referanslarının imzada saklanması, imzanın geçerliliği kontrol edilirken elde edilen iptal kontrol bilgilerinin gerçekte aranan bilgiler olup olmadığı konusunda emin olunmasını sağlar [6]. Böylece sahte sertifika değerlerinden ve iptal bilgilerinden korunmuş olunmaktadır. İmzaya eklenmiş olan referanslara karşılık gelen değerlerin imzada bulunması zorunlu değildir. Ancak, bu değerlerin herhangi başka bir yerde saklanması gerekmektedir.

Bütün doğrulama veri referanslarının bulunduğu imza formatına, sertifika ve kontrol bilgilerinin sadece referanslarının eklenmesi imza boyutunun çok artmamasını sağlamaktadır. Bu nedenle sadece referansların eklendiği imza formatı, az kullanıcılı ancak imza işleminin yoğun olarak kullanıldığı sistemler için uygundur. Örneğin, böyle sistemlerde kullanıcıların sertifikalarının geçerliliğinin kontrol edileceği bilgiler ortak bir veri tabanında saklanırsa bu değerlerin her imzaya eklenmesi gerekmez. Böylece hem veri tekrarı önlenmiş hem de sistemde atılan imzaların veri boyutu azaltılmış olur.

İmzacı sertifikalarının geçerliliği kontrol edilirken sertifika iptal listesinin kullanıldığı varsayılırsa; ~1 KB'lık bir içerik imzalandığında bir adet basit imza içeren imzalı verinin boyutu ~4 KB olur. Eğer bu basit imzaya zaman damgası eklenerek imza formatı zaman damgalı formata çevrilirse, imzalı verinin boyutu ~7,5 KB'a ulaşır. Verideki imza formatı, bütün doğrulama verisini içeren formata çevrildiğindeyse veri boyutu ~9KB'a ulaşır. Nitelikli sertifikanın, üst kök sertifikalar zincirinde iki üst kökü olduğu varsayılırsa bu iki üst kök sertifikanın veri boyutu ~4,5 KB olarak kabul edilebilir. Bu iki üst kök sertifikadan en üst kök olan sertifikaya ait OCSP bilgisi veya sertifika iptal listesi yoktur. Diğer kök sertifikanın sertifika iptal listesi boyutu ise ~1 KB olarak kabul edilebilir. İmzacı sertifikasının sertifika iptal listesinin veri boyutu ise ~90 KB'tır. Bu imzacı sertifikasının attığı bir adet imza, bütün doğrulama verisi imzada tutulursa ilgili imzanın boyutu ~100 KB'a ulaşır, aynı sertifika ile günde 100 kez imza atılıyorsa, tek bir kullanıcı için ~10 MB'lık yer ayrılması gerekir. Ancak, bu ~90 KB'lık boyuta sahip olan sertifika iptal listesi ~3000 sertifika içermektedir. İptal edilen sertifika sayısı 100000'e ulaştığında sertifika iptal listesinin boyutunun da ~1 MB'a ulaşması olasıdır. Bu durumda, bütün doğrulama verisi değerleri imzada tutulduğunda bir imzanın boyutu ~1 MB değerini aşabilir. Eğer aynı sertifika bir gün içinde birçok sayıda imza atarsa atılan tüm imzaların boyutları fazlaca büyür. Bu nedenle, kullanıcıların belirli olduğu ve kullanıcı sertifikalarının geçerliliği kontrol edilirken aynı kontrol bilgilerinin kullanıldığı sistemlerde, imzada doğrulama verilerine ait referansların tutulması ve doğrulama verilerinin değerlerinin ayrı bir yerde saklanması sistemdeki imza boyutlarının fazla büyümemesi açısından daha kullanışlıdır.

3.2. Genişletilmiş İmza Formatları

İmzanın geçerliliğinin kontrolü sırasında imzayı atmış olan sertifikanın da geçerliliği kontrol edilir. İmzada bütün doğrulama veri referansları bulunuyorsa bu referanslara karşılık gelen değerler bulunur ve sertifika kontrolü yapılırken de bu değerler kullanılır. Sertifika, geçerlilik süresi dolmadan iptal edildiyse iptal edildiği bilgisi sertifika iptal listesine eklenir. Ancak, daha sonra sertifikanın geçerlilik süresi dolduğunda bu bilgi sertifika iptal listesinden silinir. Sertifikaya ait iptal bilgisi kaydı, sertifika iptal listesinden çıkarıldığında, ilgili iptal listesi imzayı atan veya doğrulayan taraflarca saklanmıyorsa iptal bilgisine ulaşmak zor hatta imkansız hale gelir. Bu nedenle, imzacı sertifikasına ait bütün doğrulama veri referanslarının yanısıra imzada bu referanslara karşılık gelen değerler de saklanmalıdır.

Örneğin, belirsiz ve çok sayıda kullanıcıya sahip olan ve bu kullanıcıların çok az sayıda imza attıkları sistemlerde doğrulama verilerinin ortak bir yerde tutulması söz konusu olamaz. Çünkü, sistemdeki her imzanın doğrulama verisi farklılık gösterir. Bu durumda, doğrulama verilerinin ortak bir noktada tutulmasındansa her imzanın kendi doğrulama verisini içinde bulundurması tercih edilmelidir. Böyle bir sistemde her ne kadar imza boyutları büyüse de, bir kullanıcı az sayıda imza attığından kabul edilebilir değerler oluşmaktadır.

Bütün doğrulama veri referanslarını içeren imzaya bu referanslara karşılık gelen doğrulama verilerinin değerleri eklenmesi ile ETSI [5] tarafından "EXtended Long Electronic Signature (ES-X Long)" olarak adlandırılan imza formatı oluşturulur.

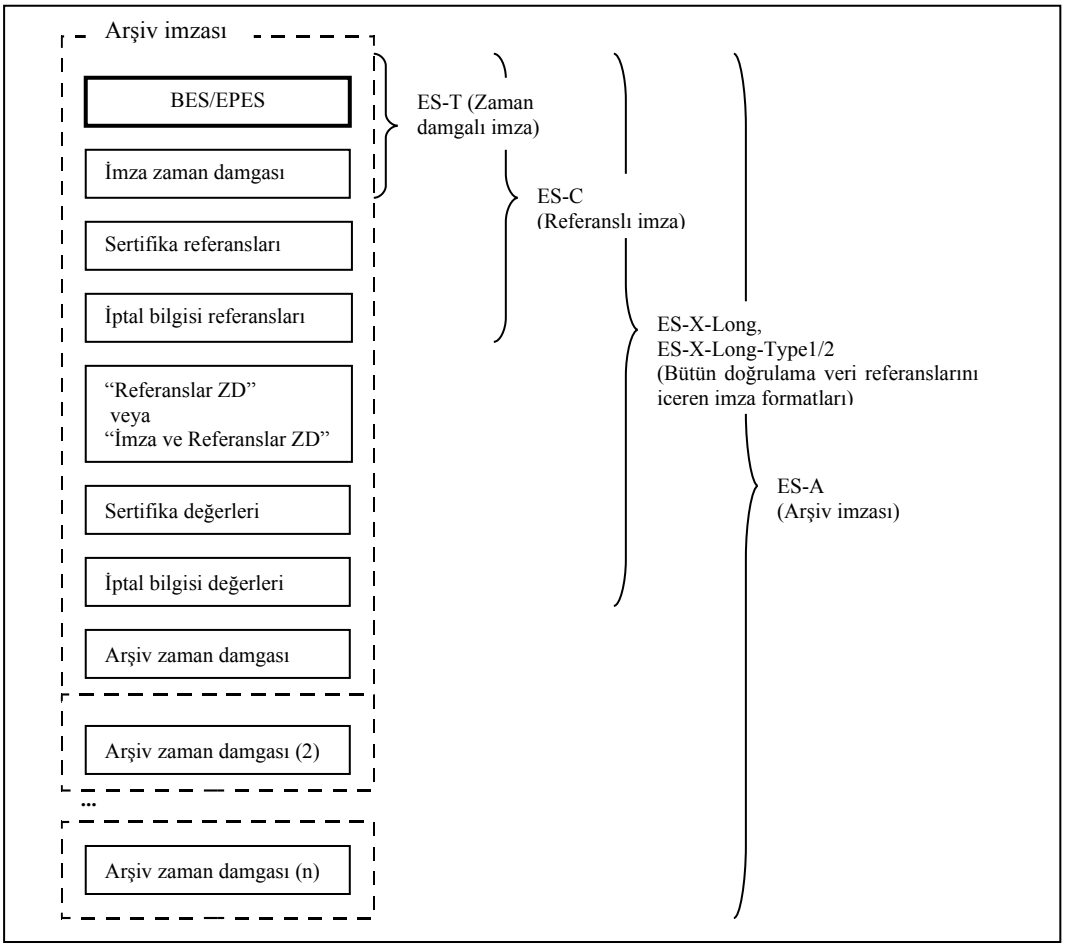
Doğrulama veri referanslarını içeren imzadaki referans değerlerine karşı oluşabilecek herhangi bir saldırı veya sahte referans üretilmesi girişimine karşılık imzaya eklenmiş olan referanslar, eklenecek bir zaman damgası ile garanti altına alınmalıdır [6].

İmzaya; imza değerini, imzayı garanti altına alan zaman damgasını ve tüm doğrulama verisi referanslarını garanti altına alan bir zaman damgası eklenebilir. Bu formattaki imza ETSI [5] tarafından "EXtended Electronic Signature with Time Type 1 (ES-X Type 1)" olarak adlandırılmaktadır. Elektronik imzadaki, imza değerinin ve doğrulama verisi referanslarının zaman damgalanması imzanın geçerliliğinin kontrolü sırasında bir belirsizlik ile karşılaşılmayacağını garanti etmektedir [5]. İmzanın daha uzun süre geçerliliğini koruyarak dayanıklı olması için, imza ve referanslar zaman damgasının da eklendiği imza formatına, daha önceden eklenmiş olan tüm doğrulama verilerinin referanslarına ait değerler de eklenebilir. Bu durumda oluşan imza formatı ETSI [5] tarafından "EXtended Long Electronic Signature with Time Type 1 (ES-X Long Type 1)" olarak adlandırılmaktadır.

İmzayı ve içerdiği doğrulama referanslarını zaman damgalayan yaklaşım çoğu zaman çok etkin olmayabilir. Örneğin, bir kurumdaki kullanıcıların sertifikalarının geçerlilik kontrolü aynı üst kök sertifika zincirinden ve aynı sertifika iptal listesinden yapılıyor ise sistemde atılmış olan her imzayı, imza değerini de kapsayacak şekilde zaman damgalamak

etkin bir yöntem olmaz. Çünkü her imza değeri için ayrı ayrı zaman damgası almak gerekir. Bu durumda, sadece doğrulama referanslarını zaman damgalayarak garanti almak daha iyi bir yöntemdir. Böylece ilgili kurumda, doğrulama referans verileri için bir kez zaman damgası alınması yeterli olacaktır. Bu ihtiyaç da ETSI [5] tarafından, "EXtended Electronic Signature with Time Type 2 (ES-X Type 2)" olarak tanımlanan imza formatı ile karşılanmıştır. Bu formatta, zaman damgası sadece imzacı sertifikasının ait olduğu üst kök sertifikalar zinciri referanslarını ve ilgili sertifikalarının geçerliliklerinin kontrol edildiği bilgilerin referanslarını garanti altına alacak şekilde eklenmektedir. Böylece aynı kök sertifika zinciri ve iptal bilgileri için tek bir zaman damgası yeterli olmaktadır.

Eğer doğrulama verilerinin referanslarına karşılık gelen değerlerin sistemde ortak bir yerde tutulması tercih edilmiyorsa, sadece referansların zaman damgalanmış olduğu imzaya da eklenebilir. Bu durumda, "ES-X Type 2" formatındaki imzaya doğrulama verilerinin referanslarına karşılık gelen değerler de eklenebilir. Değerler eklendiğinde imza daha uzun süre geçerliliğini koruduğu için "EXtended Long Electronic Signature with Time Type 2(ES-X Long Type 2)" olarak adlandırılmaktadır [5].



Şekil 1

3.3. Arşiv İmzası

Elektronik imza oluşturulurken kullanılan kriptografik algoritmalar zamanla zayıflamakta ve kırılabilir hale gelmektedir [6]. Aynı şekilde, imzaya eklenen zaman damgaları da kullanılan algoritmalara bağlı olarak zamanla zayıflamaktadır. İmza oluşturulurken kullanılan sertifikaların ait olduğu üst köklerin de belirli geçerlilik süreleri vardır. Bu zayıflamalardan dolayı, imzanın geçerliliğini koruyabilmesi için periyodik olarak tekrar güçlendirilmesi gerekmektedir. Örneğin; imza oluşturulurken SHA-1 özetleme algoritması kullanılmış ise, belirli bir süre sonra, SHA-1 özetleme algoritması kırılabilir düzeye gelmeden önce daha güçlü bir özetleme algoritması kullanılarak oluşturulmuş olan bir zaman damgası imzaya eklenerek imza güçlendirilmelidir. Hatta eklenen bu zaman damgası; imza değerini de içerek şekilde imzadaki eklentileri, imza zaman damgasını, bütün doğrulama verisi referanslarını, bu referanslara karşılık gelen değerleri, imzayı ve referansları

koruyan zaman damgasını veya sadece referansları koruyan zaman damgasını kapsayarak güçlendirmelidir.

ETSI [5]'de bu ihtiyaca arşivleme işlemi ile çözüm önerisinde bulunulmaktadır. Arşivleme işleminde, zayıflayan imzaya imzadaki tüm eklentileri kapsayacak şekilde ve imzadaki zaman damgalarından daha güçlü bir özetleme algoritması kullanılarak bir zaman damgası eklenmektedir. Eklenen bu zaman damgası arşiv zaman damgasıdır [5]. Bu formattaki imza ise ETSI tarafından tanımlanmış olan standartta [5] "Archival Electronic Signature (ES-A)" olarak adlandırılmaktadır. Arşiv imzasının içermesi gereken eklentiler Şekil 1'deki gibidir. Arşiv zaman damgası da zaman içinde güçsüzleşebilir. Bu nedenle ETSI [5] imzaya birden fazla arşiv zaman damgası eklenmesine izin vermektedir.

4. Sonuç

E-devlet uygulamalarının hayata geçmesi ve bu uygulamalarda elektronik imzanın kullanılmaya başlanmasıyla imzanın uzun süre geçerliliğini koruması bir ihtiyaçtan çok zorunluluk halini almıştır. Ancak, her kurumun imza ile ilgili ihtiyacı çeşitlilik göstermektedir ve bu ihtiyaçlar ETSI tarafından tanımlanmış olan farklı formatlar kullanılarak karşılanmaktadır. Bu nedenle, e-devlet uygulamalarında ETSI ile uyumlu elektronik imza kullanımı önerilmektedir.

5. Kaynaklar

[1] Türk Dil Kurumu Web Sitesi : www.tdk.gov.tr
[2] Elektronik İmza Kanunu : http://www.mevzuat.adalet.gov.tr/html/1328.html
[3] IETF RFC 3369 (2002): "Cryptographic Message Syntax".
[4] IETF RFC 2634 (1999): "Enhanced Security Services for S/MIME".
[5] ETSI TS 101 733 V1.5.1 (2003-7 12) : "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".
[6] CWA 14171 CEN. Workshop Agreements: "Procedures for Electronic Signature Verification".