ELEKTRONİK İMZA OLUŞTURMA VE DOĞRULAMA

IŞIL HASIRCIOĞLU
TÜBİTAK UEKAE Gebze/KOCAELİ,
ihasircioglu@uekae.tubitak.gov.tr

ÖZET : Bu bildiride ETSI standardında tanımlanan Elektronik İmza yapısı ve farklı kullanım amaçları için oluşturulabilecek imza formatları incelenecek, standartlarda ayrıntıları verilen Elektronik İmza ve sertifika doğrulama adımları açıklanacaktır.

ANAHTAR KELİMELER: elektronik imza, elektronik imza formatları, imza doğrulama, sertifika doğrulama

ELECTRONIC SIGNATURE GENERATION AND VERIFICATION

ABSTRACT : In this paper, Electronic Signature structure defined by ETSI standard and different signature formats which can be used for different purposes will be examined as well as Electronic Signature and certificate verification steps of that the details are given in the standards will be explained.

KEYWORDS : electronic signature, electronic siganture formats, signature verification, certificate verification

Giriş

Elektronik imza; 1999 tarihli Avrupa Birliği direktifinde[1] ve 15 Ocak 2004 tarihli, T.C. 5070 sayılı Elektronik İmza Kanunu'nda, başka bir elektronik veriye eklenen veya mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmıştır. Pratik anlamda, güvenli bir ortamda oluşturulan, kişilerin kimlik doğrulamasını sağlayan ve içeriği onayladıklarını gösteren imzadır. Kanuni olarak elle atılan imza geçerliliğinde olan imza yapısı, nitelikli elektronik imza olarak tanımlanmıştır. Avrupa Birliği Direktifi'ne dayanarak hazırlanmış Elektronik İmza Kanunu'nda "Güvenli Elektronik İmza" olarak isimlendirilen nitelikli elektronik imza şu özellikleri taşımalıdır:

1) Sadece imza sahibine bağlı olmak
2) İmza sahibinin kimliğini tespitini sağlamak
3) Sadece imza sahibinin kontrolünde oluşturulmak
4) İmzalanmış veride sonradan değişiklik yapılıp yapılmamış olduğunun tespitini sağlamak.

Farklı amaçlara hizmet edebilecek şekilde tasarlanmış elektronik imza formatları, EESSI(European Electronic Signature Standardization Initiative) altında, ETSI (TS 101 733)[2]'de tanımlanmıştır. Yine bu kapsamda, imza ve imzada kullanılan sertifika doğrulama süreçleri, CEN/ISSS Workshop on Electronic Signatures yayını olan CWA 14171[3]'de tanımlanmış ve ayrıntılarıyla açıklanmıştır. Bu bildiride, bu standartlarda detayları verilmiş olan Elektronik İmza formatları ve Elektronik İmza doğrulama adımları açıklanacaktır.

Elektronik İmza Formatları

ETSI TS 101 733 standardında elektronik imza yapıları; elektronik imza formatları ve doğrulama verili elektronik imza formatları olmak üzere iki sınıfta tanımlanmıştır.

Elektronik imza formatları olarak Basit Elektronik İmza(BES) ve Belirlenmiş Politika Temelli Elektronik İmza(EPES) tanımlanmakta olup doğrulama verili elektronik imza formatları Zamanlı Elektronik İmza(ES-T), Doğrulama Verisi Referanslı Elektronik İmza(ES-C), Genişletilmiş Elektronik İmza ve Arşiv Elektronik İmza(ES-A) formatlarıyla açıklanmıştır.

Basit Elektronik İmza
(Basic Electronic Signature)

Elektronik imza formatlarının en basit ve minimum özelliklere sahip yapısıdır. Bu imza formatı, diğerlerine de temel teşkil etmekte olup imza yapısının iskeleti burada oluşturulmaktadır. İmzalı veri yapısı, RFC 3852 CMS(Cryptographic Message Syntax)[4] standardında açıklanmıştır.

CMS yapısı, genel olarak veri korumasına yönelik elektronik imza, özet, şifre mesaj yapılarını tanımlayan standarttır. Bu standarda göre oluşturulacak kriptografik mesaj yapısı, içerik tipi ve içerik bilgilerinden oluşmaktadır. İmza mesaj tipinde bu yapıdaki içerik tipi yine burada tanımlanmış imzalı tipinde olmalıdır. *İmzalı veri içerik tipi* herhangi bir tip içerik ve sıfır veya daha fazla imza değerinden oluşmaktadır. *İmzalı veri* oluşturmak için izlenecek adımlar, Şekil 1'de de gösterildiği gibi:

a) Her bir *imzacı* için imzacı sertifikasındaki özet algoritması kullanılarak içerik üzerinden mesaj *özet*i oluşturulması

b) Her bir imzacı için oluşturulan özetin imzacının özel imzalama anahtarı ile *imza*lanması

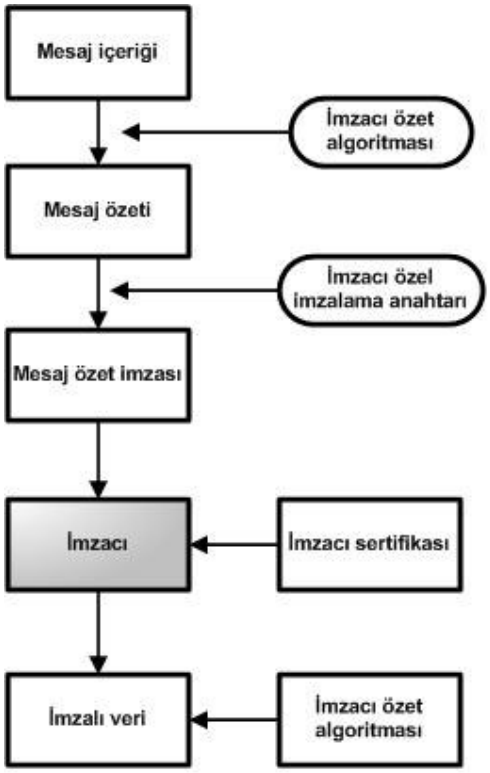
c) Her bir imzacı için oluşturulan imza değerinin ve imzacıya ait sertifika bilgisinin imza yapısındaki *imzacı* bilgisi yapısına yerleştirilmesi

d)Tüm imzacılara ait özet algoritma bilgilerinin, mesaj içeriğinin ve imzacı bilgi yapılarının *imzalı veri* yapısına yerleştirilmesi
olarak tanımlanmıştır.

İmzalı veri yapısı tüm imzacılara ait özet algoritma bilgileri, mesaj içeriği ve imzacı yapılarının yanı sıra isteğe bağlı olarak imzalama sertifikaları ve bu sertifikalara ait sertifika sil listelerini içermektedir. Ayrıca yapı içindeki isteğe bağlı alanların varlığı, içerik tipi bilgisi ve imzacı veri yapısı versiyonuna göre belirlenen ve imzalı veri yapısının sözdizimini(syntax) belirten versiyon numarası da imzalı veri yapısı içinde bulunması gereken bir alandır.

İmzalı veri yapısına paralel olarak eklenecek her bir imzayı temsil eden **İmzacı veri yapısı** da imzacı tanımlayıcı, bu tanımlayıcının tipine göre belirlenen versiyon numarası, imzacıya ait özet algoritması ve imzalama algoritması, imza değerini taşımaktadır. Ayrıca farklı tiplerde tanımlanmaları mümkün olan isteğe bağlı imzalı ve imzasız nitelikler, İmzacı yapısı içinde yer almaktadır. Bu nitelikler, temel olarak elektronik imza formatlarının birbirlerinden farklılıklarını ortaya koymaktadırlar. ETSI standardına göre, Basit Elektronik İmza formatından başlayarak yapı içerisine konulması gereken imzalı ve imzasız nitelikler(signed/unsigned attributes) tanımlanmış ve açıklanmıştır. CMS yapısında isteğe bağlı olarak görülen bu nitelik alanları, ETSI standardındaki zorunluluklar göz önünde bulundurularak doldurulmalıdır.

Basit Elektronik İmza formatında bulunması gereken nitelikler İçerik Tipi(content-type), Mesaj Özeti(message-digest) ve İmzalama Sertifikası(signing certificate) imzalı nitelikleridir. Bir



Şekil 1

CMS imza yapısının ETSI standardında tanımlanan Basit Elektronik İmza formatında olabilmesi için en azından bu nitelikleri taşıması gerekmektedir.

Belirlenmiş Politika Temelli Elektronik İmza
(Explicit Policy-based Electronic Signature)

Belirlenmiş Politika Temelli Elektronik İmza, imzalama politikası ile oluşturulmaktadır. Bu politika bilgisi, Basit Elektronik İmza yapısındaki imzalı niteliklere ilave olarak İmza Politika Belirleyicisi imzalı niteliği ile imza yapısına eklenmektedir. İmzalama politikası, elektronik imza oluşturma ve doğrulanmasıyla ilgili kuralları içermekte ve belirlenen yapı imzalı bir nitelik olarak elektronik imza yapısına dahil edilmektedir. Bu formattaki elektronik imza, tanımlanan politika esaslarına göre oluşturulmalı ve imzanın doğrulanması yine bu politikadaki ilkeler göz önünde bulundurularak gerçekleştirilmelidir.

Zamanlı Elektronik İmza
(Electronic Signature Time-stamped)

Zamanlı Elektronik İmza, doğrulama verili elektronik imza formatlarının ilkidir. Bu imza formatı, yukarıda bahsedilen iki imza türünden herhangi birine zaman damgası bilgisi içeren niteliğin eklenmesiyle

oluşturulmaktadır. Bu zaman damgası bilgisi, güvenilir bir Zaman Damgası servisi tarafından elektronik imza değerine verilen zaman damgası verisini içermekte olup yapıya imzasız bir nitelik olarak eklenmektedir. Bu imzasız nitelik eklenmesi yerine güvenilir bir servis tarafından verilecek zaman belirteci de, imzayı bu formata uygun hale getirebilmektedir.

Doğrulama Verisi Referanslı Elektronik İmza
(ES with Complete validation reference data)

Doğrulama Verisi Referanslı Elektronik İmza, Zamanlı Elektronik İmza yapısına sertifika ve iptal referans bilgilerinin eklenmesi ile oluşturulmaktadır. Bu bilgiler Tüm Sertifika Referansları ve Tüm İptal Referansları imzasız nitelikleri ile tanımlanmıştır. Tüm Sertifika Referansları, imzayı doğrulamakta kullanılacak sertifika yolu üzerindeki tüm sertifikaları içermekteyken Tüm İptal Referansları da imzayı doğrulamakta kullanılacak tüm sertifika iptal listeleri ve OCSP cevaplarını içermektedir.

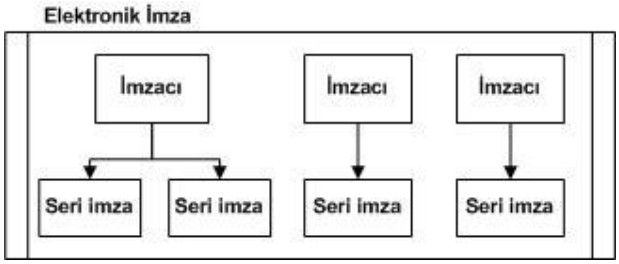
Genişletilmiş Elektronik İmza
(ES with Extended validation data)

Doğrulama Verisi Referanslı Elektronik İmza, yapısına imzasız nitelikler eklenerek genişletilebilmektedir. ETSI standardında; eklenen niteliklere göre Genişletilmiş Uzun Elektronik İmza(ES-X Long), Zamanlı Genişletilmiş Elektronik İmza Tip 1(ES-X Type 1), Zamanlı Genişletilmiş Elektronik İmza Tip 2(ES-X Type 2), Zamanlı Genişletilmiş Uzun Elektronik İmza(ES-X Long Type 1 veya Type 2) türlerinde genişletilmiş elektronik imza formatları tanımlanmıştır.

Arşiv Elektronik İmza
(ES with Archive validation data)

Arşiv Elektronik İmza, yukarıda bahsedilen Genişletilmiş Uzun Elektronik İmza veya Zamanlı Genişletilmiş Uzun Elektronik İmza formatlarına bir veya daha fazla Arşiv Zaman Damgası niteliği eklenerek oluşturulmaktadır. Bu imza formatı, uzun zamanlı imzaların arşivlenmesi için kullanılmaktadır. Zaman damgaları, tüm yapıları zayıf özet algoritmalarına veya kriptografik algoritmaların kırılmasına karşı korumaktadır.

ETSI standardında, elektronik imza formatları ve bu formatlarda bulunması zorunlu olan niteliklerden başka farklı işlevlere sahip isteğe bağlı imzalı veya imzasız nitelikler tanımlanmıştır. Bu niteliklerden İmzalama Zamanı(signing-time) imzalı niteliği, imzalama işleminin zamanı hakkında bilgi taşımaktadır. Diğer tanımlı nitelik de Seri İmza(countersignature) imzasız niteliğidir. Seri imza, imzayı imzalamak-onaylamak anlamını taşıyan bir bilgidir. Bir imzacı yapısında bulunan Seri İmza niteliği, o imzayı imzalamak olarak anlamlandırılmakta, elektronik imza uygulamalarında yaygın kullanım alanı bulmaktadır. Daha önce imza yapısında birden fazla İmzacı yapısının bulunmasını paralel imza olarak adlandırmışken her bir İmzacı yapısında buluna Seri İmza niteliği de bu İmzacı yapısının imzalanmış olduğunu göstermektedir. Şekil 2'de de gösterildiği gibi bir elektronik imza yapısı birden fazla *paralel* veya *seri* imzadan oluşabilmektedir.



Şekil 2

Elektronik İmza ve Sertifika Doğrulama

Elektronik imza verisinin doğrulanma işlemi için izlenmesi gereken adımlar, CWA 14171 dokümanında açıklanmıştır.

Bir elektronik imzanın doğrulanması için;

a)İmzalanan veri,
b)Bu verinin imzası
c)Doğrulama verisi olarak tanımlanan elektronik imzayla ilgili diğer veriler

sağlanmalıdır. Doğrulama verisi; imzalama yapan sertifikaları, iptal durumu bilgisini(sertifika iptal listeleri, OCSP cevapları) ve Zaman Damgası Sunucusu'ndan alınan güvenilir zaman damgalarını içerebilir.

İmza doğrulama, elektronik imza oluşturulduktan hemen sonra gerçekleştiriliyorsa imza durum bilgisi ve daha sonraki doğrulamalarda kullanılmak üzere oluşturulan doğrulama verisi bilgilerini verir. Elektronik imza oluşturulduktan sonra uzun dönem içinde gerçekleştirilen imza doğrulama işlemi, bu doğrulama verilerini kullanarak imza durumunu oluşturur.

İmza doğrulama sonucunda ortaya çıkabilecek imza durumları üç farklı değer alabilir. İlki elektronik imzanın geçerli olduğunu, doğrulama işlemini başarıyla geçtiğini gösterir. Diğeri imza değerinin geçersiz olmasından yani imza yapısındaki imza değerinin imzalayan sertifika tarafından doğrulanmamasından veya imzalayan sertifikanın geçersiz olmasından dolayı elektronik imzanın

geçersiz olduğunu işaret etmektedir. Diğer oluşabilecek imza durumu ise eksik doğrulamadır. Eksik doğrulama, imzanın geçerli veya geçersiz olduğunu kesin bir şekilde ifade edememekte, ulaşılamayan veya eksik olan verilerden dolayı imzanın doğrulanma işleminin tamamlanamadığını göstermektedir.

Doğrulama işlemine imzalanan veri ve oluşan imza verisiyle birlikte adımlarda kullanılmak üzere doğrulama verileri de verilmelidir. Bu veriler; imzalayan sertifikalar ve bu sertifikaları doğrulamakta kullanılacak kök sertifikaya kadar giden yol üzerindeki tüm sertifikalar veya bu sertifikalara ulaşılabilecek adresler ve tüm bu sertifikalara ait iptal durumu bilgilerini içermelidir. İmza formatlarına göre bu doğrulama verisi, imzalı verinin yapısında da bulunabilmektedir. Doğrulama Verisi Referanslı Elektronik İmza, doğrulama işleminde gerekli olan tüm verileri içermektedir ve doğrulama işlemi için sadece imzalı veri yapısının verilmesi yeterli olacaktır. Aynı uygulama, tüm doğrulama verilerini içeren Genişletilmiş Elektronik İmza Formatları için de geçerlidir. Uzun dönemli imza doğrulama işlemi için imzanın atıldığı tarihin ispatlanabilmesi için, imza formatının Zamanlı Elektronik İmza olması gerekmektedir. Güvenilir Zaman Damgası Sunucusu tarafından verilen zaman damgası sayesinde imza tarihi tespit edilir ve imzanın, imza atan sertifikanın bu tarihteki geçerliliği kontrol edilir. İnkar etme durumunu engelleyebilmek için Zamanlı Elektronik İmza oluşturulurken imzalama işleminden sonra en kısa zaman içinde Zaman Damgası oluşturulmalıdır. Elektronik imzanın Zaman Damgası tarafından oluşturulmuş zaman bilgisi içermemesi durumunda doğrulama işlemi, imza yapısına eklenen İmzalama Zamanı niteliğinden alınan zaman bilgisi ile gerçekleştirilebilir.

*Elektronik İmza Kanunu'nda tanımlanan Güvenli elektronik imza*nın geçerli olabilmesi için imzanın güvenli imza oluşturma aracı kullanımını gerektiren *Nitelikli Sertifika* ile oluşturulmuş olması gerekmektedir. Nitelikli Sertifika detayları RFC 3739[5] ve ETSI TS 101 862[6] dokümanlarında açıklanmıştır. Genel olarak Nitelikli Sertifika'da, tanımlanmış bir eklenti bulunma zorunluluğu vardır. Güvenli imza kontrollerinde, sertifika doğrulama adımında bu eklenti kontrolü yapılmalıdır.

Öncelikle doğrulanacak Elektronik İmza yapısının yukarıda bahsedilen imza formatlarından birinde oluşturulmuş olması gerekmektedir. Elektronik imza, en azından Basit Elektronik İmza formatında olmalı ve bu format için zorunlu kılınan nitelikleri taşımalıdır. Doğrulama işleminin ilk adımı olarak bu format kontrolü yapılabilir.

Elektronik imza doğrulama işleminde, imza verisinin geçerlilik kontrolünden önce bu veriyi oluşturan sertifikanın geçerliliği kontrol edilmelidir. Bu sertifikanın imzalama tarihinde geçerli olduğu sonucu alındıktan sonra imza verisi ile imzalanan veri bu sertifikadaki açık anahtar ile doğrulanır. Tarih bilgisi yukarıda belirtilen yöntemlerle elde edilebilir.

Sertifika doğrulama işlemi detayları RFC 3280[7] dokümanında açıklanmaktadır. Bir sertifikanın geçerli olabilmesi için sertifikadan kök sertifikasına giden yol üzerindeki tüm sertifikaların geçerli olması gerekmektedir. Doğrulama işleminde güvenilir nokta olarak verilen kök sertifikaya kadar tüm sertifikaların geçerlilik kontrolleri yapılması neticesinde sertifikanın geçerlilik durumu tespit edilebilir. Bu yol üzerindeki son sertifika olan kök sertifika, sertifika doğrulama işlemine güvenilir sertifika olarak verilmelidir. Güvenilir sertifika olarak verilen sertifikanın kök sertifikası olmadığı durumlar da mümkün olabilmekte, sertifika zinciri üzerindeki herhangi bir sertifika güvenilir olarak belirlenmişse sertifika doğrulama işlemi bu sertifikaya gelindiği noktada son bulup kök sertifikaya kadar gitme zorunluluğu olmayabilmektedir.

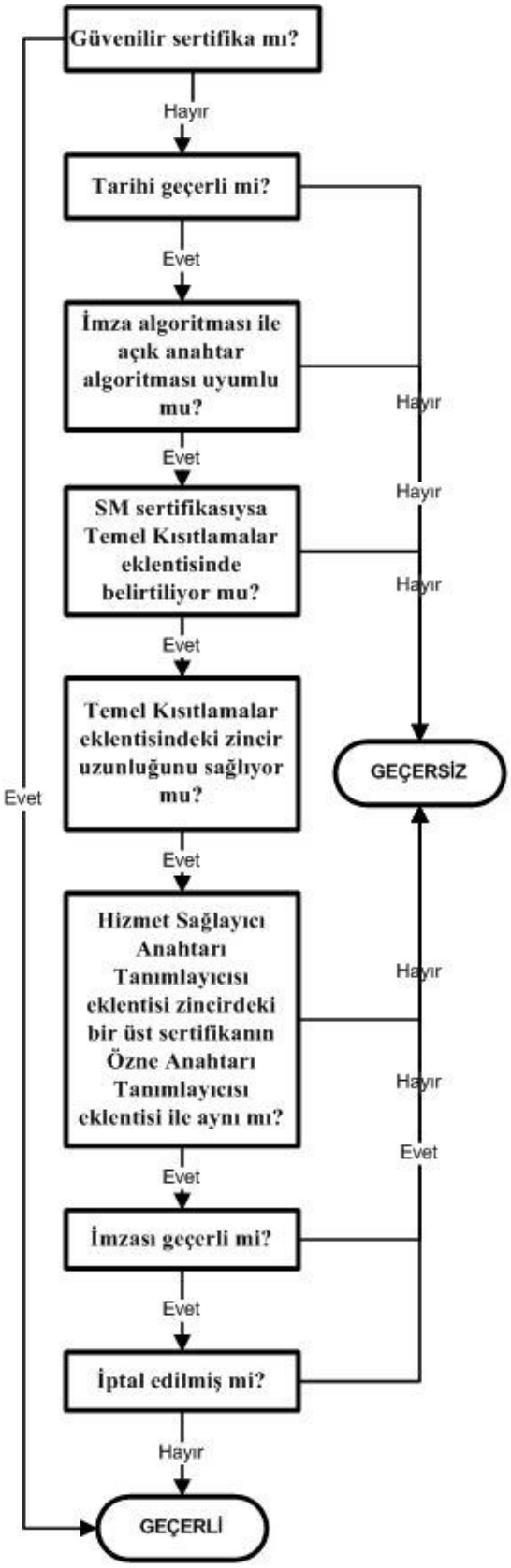
Sertifika doğrulama adımları, Şekil 3'te ana başlıklarıyla gösterilmiştir. Öncelikle sertifikanın doğrulama işlemine verilen güvenilir sertifika olup olmadığı sertifikaların değerleri karşılaştırılarak kontrol edilir. Geçerliliği kontrol edilen sertifika, zaten güvenilir sertifika olarak verilmişse doğrulama işlemi sertifikanın geçerli olduğu sonucu ile sona erdirilir. Aksi durumda sertifika doğrulama işlemi, sonraki adımlarla devam eder.

***Sertifika geçerlilik tarihi kontrolü*:** Sertifikanın geçerli olduğu zaman aralığı, sertifikada bulunan Geçerlilik Başlangıcı ve Geçerlilik Sonu alanları ile belirlenerek sertifikanın geçerlilik kontrolünün yapılmak istendiği zamanın bu aralıkta olup olmadığı kontrol edilir.

***İmza algoritması-Açık anahtar imza algoritması uyumluluk kontrolü*:** RFC 3280 standardına göre sertifikadaki *İmza Algoritması* alanındaki algoritma bilgisi ile Açık Anahtar alanındaki verinin içerdiği algoritma bilgileri aynı olmalıdır. Aksi takdirde sertifika geçersiz olarak kabul edilmektedir.

***Temel kısıtlamalar eklentisi SM belirteci*:** Doğrulama işlemi yapılacak sertifika, zincir üzerindeki ara sertifikalardan biri olarak SM sertifikasıysa bu özelliği sertifikadaki Temel Kısıtlamalar eklentisinde belirtilmelidir. Bu eklentideki Konu Türü değeri CA olarak tanımlanmış olmalıdır.

Temel kısıtlamalar eklentisi yol uzunluğu kısıtlaması: Sertifikadaki Temel Kısıtlamalar eklentisinde yol uzunluğu kısıtlanmışsa, kontrolü yapılan sertifikaya kadar geçilen yolun uzunluğu ile



Şekil 3

bu belirtilen değer kontrol edilmelidir. Yol uzunluğu, kısıtı geçmeyen bir değerde olmalıdır.

***Hizmet Sağlayıcı Anahtarı Tanımlayıcısı- Özne Anahtarı Tanımlayıcısı uyumluluk kontrolü*:** Sertifikadaki Hizmet Sağlayıcı Anahtarı Tanımlayıcısı eklentisi ile sertifikanın bir üst SM sertifikasındaki Özne Anahtarı Tanımlayıcısı değerleri aynı olmalıdır.

İmza kontrolü: Sertifikanın imzası, sertifikayı imzalayan SM sertifikası açık anahtarı ile kontrol edilmelidir. Burada da imza doğrulama işlemi yapılacağı için imza değerinden önce sertifikayı imzalayan SM sertifikası geçerlilik kontrolü yapılmalıdır. Sertifika doğrulama işlemindeki zincir oluşturma adımı bu noktada başlamakta olup bir üst SM sertifikası en başından itibaren tüm adımlardan geçip doğrulanması başarıyla yapıldıktan sonra bu sertifikadaki açık anahtar ile sertifikanın imzası kontrol edilir. Tüm sertifikalar için imza doğrulama işlemi yapılması gerektiği için kök sertifikaya veya güvenilir sertifikaya kadar yol üzerindeki tüm sertifikaların doğrulanma işlemi gerçekleşmiş olur. Bir sertifikanın üst SM sertifikasına ulaşabilmek için sertifikadaki Hizmet Sağlayıcı Bilgi Erişimi eklentisindeki bilgiler kullanılabilir. Bu eklentide SM sertifikasının ldap veya http adresi verilmiştir, erişim yöntemleriyle bu uzaktaki konumlardan alınan SM sertifikası ile doğrulama işlemine devam edilir. Elektronik İmza doğrulama sürecinde bu sertifikalar imzalı veri yapısında veya dışarıdan sertifika doğrulama işlemine verilebilir, bu durumda uzak konumlara bağlantı kurma ihtiyacına gerek kalmadan verilen bu sertifikalar kullanılarak doğrulama adımı gerçekleştirilebilir.

***İptal durumu kontrolü*:** Seritifikanın doğrulamasının yapılacağı zamandaki iptal durumu kontrol edilmelidir. Sertifika çeşitli sebeplerle geçerlilik zamanı dolmuş olmasa bile askıya alınmak veya iptal edilmek suretiyle geçersiz hale gelmiş olabilir. Sertifikanın iptal durumu, sil servisleri tarafından periyodik olarak yayımlanan Sertifika İptal Listeleri veya anlık sertifika durumunu verebilecek OCSP sunucuları kullanılarak öğrenilebilir. Sertifika iptal listelerinde iptal edilmiş veya askıya alınmış tüm sertifikalar listelenmektedir. OCSP sunucuları da herhangibir sertifika durum istek mesajına o sertifikanın o andaki durumunu içeren mesaj ile cevap vermektedir. Sertifika iptal listeleri veya OCSP cevapları, Elektronik İmza yapısında doğrulama verisi olarak verilebileceği gibi bu verinin bulunmaması durumunda sertifikadaki CRL Dağıtım Noktaları eklentisinde Sertifika İptal Listelerinin yayımlandığı adreslerden veya Hizmet Sağlayıcı Erişim Bilgisi eklentisinde verilmiş olan OCSP sunucusu adresinden edinilebilir. İptal kontrolü yapılma aşamasında kullanılan iptal listelerinin geçerlilik kontrolü de doğrulama işleminin başka bir adımıdır. Bu kontrol

tarih, imza kontrolü gibi adımlardan oluşmaktadır. Aynı şekilde OCSP cevaplarının geçerlilikleri de kontrol edilmelidir. Bu yöntemlerle doğrulaması yapılan sertifikanın askıda olduğu veya iptal edilmiş olduğu bilgisinin alınması durumunda sertifika geçersiz olarak kabul edilir.

İmza kontrolü adımında geçerli SM sertifikasına, iptal kontrolü adımında geçerli sertifika iptal listesi veya OCSP cevabına ulaşılamadığı durumda sertifika geçerliliği eksik olarak sonuçlandırılır. Bu durumlarda, ilki için sertifikanın imzası geçersiz bulunamadığından ikincisi için sertifika iptal veya askı durumunda bulunamadığı için geçersiz sonucu verilememekte, geçerli-geçersiz durumlarına ilave olarak tanımlanmış eksik sonucu verilmektedir. Böyle bir durumda, sertifika doğrulama işleminin yapıldığı uygulama tarafından sertifika geçerliliği başka bir zamanda tekrarlanabilir veya sertifika geçersiz olarak kabul edilebilir.

Sonuç

Elektronik imza, kanuni olarak ıslak imzanın yerini tutmakta olup imzalayanın kimliğini doğrulayan veri yapısıdır. Farklı kullanım amaçlarını destekleyen tanımlanmış formatlarda oluşturulabilen Elektronik İmza, farklı uygulamalarda kullanılabilmektedir. Elektronik İmzayı uygulamalarında kullanmak isteyen taraflar, ETSI standardında tanımlanmış yapıda imza verisi oluşturmalı ve ihtiyaçları doğrultusunda uygun formattaki imza yapısını seçmelidirler.

İmzanın imzalayan kişiye ait olduğunun ispatı için gerçekleştirilen doğrulama işlemi için standartlara uygun uygulamalar geliştirilmeli, tam ve kesin sonuç için doğrulama adımları doğru bir şekilde uygulanmalıdır.

Kaynaklar

[1] The European Directive 1999/93/EC on a Community Framework for Electronic Signatures

[2] ETSI TS 101 733 V1.5.1 (2003-12) Technical Specification: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats

[3] CEN Workshop Agreement CWA 14171, July 2001

[4] IETF RFC 3852: Cryptographic Message Syntax (CMS)

[5] IETF RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

[6] ETSI TS 101 862: Qualified Certificate profile. June 2004

[7] IETF RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile