Elektronik Sertifika Hizmet Sağlayıcılarının yayınladıkları nitelikli elektronik sertifikaların birbiriyle uyumlu olması ve birlikte çalışabilirliğinin sağlanmasına ilişkin olarak, 93/2007 Sayılı Elektronik İmza Yasası altında hazırlanarak 21.10.2008 tarihli ve R.G.186 A.E 760 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik İmza Yasasının Uygulanmasına İlişkin Usul ve Esaslar Tüzüğü'nde bir düzenleme bulunmaması nedeniyle söz konusu Tüzüğün 28'inci maddesi hükmü uyarınca Bilgi Teknolojileri ve Haberleşme Kurumu tarafından işbu "Çevrimiçi Sertifika Durum Protokolü (OCSP) İstek/Cevap Profilleri" dokümanı hazırlanmıştır.

ÇEVRiMiÇi SERTiFiKA DURUM PROTOKOLÜ
(OCSP)
İSTEK/CEVAP PROFİLLERİ

1. Çevrimiçi Sertifika Durum Protokolü (OCSP)

Burada aksi belirtilmedikçe, OCSP istek ve cevap mesajları RFC 2560 [2] 'da tanımlandığı gibi **olmalıdır**. Bu profile uyan ESHS'lerin OCSP sunucuları http üzerinden gelen isteklere cevap **verebilmelidir**.

1.1 OCSP İstek Mesajı

Bir OCSP istek mesajı ile birden fazla sertifikanın durumunu sorgulamak mümkündür.
OCSP istek mesajında genel bir eklentiler alanı bulunmaktadır. Ayrıca her bir istek için ayrı ayrı eklenti eklemek mümkündür. Aşağıdaki istek mesajı eklentileri isteğe genel eklentileri, tek istek eklentileri de her bir isteğe eklenebilecek eklentileri anlatır.

1.1.1 OCSP İstek Mesajı Eklentileri

1.1.1.1 Nonce Eklentisi

Nonce, güncel OCSP cevabı alındığından emin olunması için kullanılır. İstemcilerin gönderdikleri istekte nonce kullanılması *önerilir*. Nonce değeri olarak rastgele oluşturulmuş en az 128 bitlik bir veri kullanılması *önerilir*.

1.1.1.2 Kabuledilebilir Cevap Tipleri (Acceptable Response Types) Eklentisi

Bu eklentinin kullanılmaması *önerilir*. Bu profile uyan istemciler `id-pkix-ocsp-basic` tipinde cevap mesajlarını **algılayabilmelidirler**. Dolayısıyla, istemciler, kabul edilebilir cevap tipleri eklentisini eklemeleri durumunda, `id-pkix-ocsp-basic` tipini mutlaka eklenti içinde **bulundurmalıdırlar**.

1.1.2 OCSP Tek İstek Eklentileri

Herhangi bir tek istek eklentisi kullanılmaması *önerilir*.

1.2 OCSP Cevap Mesajı

Gelen istek mesajında, Kabuledilebilir Cevap Tipleri eklentisi bulunmuyorsa, sunucu `id-pkix-ocsp-basic` tipinde cevap **üretmelidir**. Bu profil sadece `id-pkix-ocsp-`

`basic` tipindeki cevapları tanımlar. Sunucular ve istemciler `id-pkix-ocsp-basic` tipini kullandıklarında buradaki kısıtlara uymak **zorundadır**.

1.2.1 Zorunlu OCSP Cevap Alanları

1.2.1.1 İmza Algoritması Alanı (BasicOCSPResponse yapısı signatureAlgorithm)

Cevap imzalanırken kullanılan algoritma, yönetmelikte [1] belirtilen algoritma ve anahtar boylarına uyumlu **olmalıdır**.

1.2.1.2 Sonraki Güncelleme Alanı (SingleResponse yapısı nextUpdate)

Bu profile uyan OCSP sunucuları sertifikaların gerçek zamanlı durumunu bilmek **zorundadır**. Dolayısıyla sonraki güncelleme alanı cevap yapısı içerisinde **bulunmamalıdır**.

1.2.1.3 Sebep Kodu (Revoked Info yapısı revocation Reason)

Sertifikanın iptal edilme sebebini belirtir. Eğer iptal sebebi bilinmiyorsa, belirsiz (unspecified (0)) olarak eklenmesi yerine, hiç eklenmemesi *önerilir*. Eğer sebep biliniyorsa, eklenmesi *önerilir*.

Bu eklenti kritik olarak **işaretlenmemelidir**.

1.2.2 OCSP Cevap Eklentileri

1.2.2.1 Nonce

Bu profile uyan sunucular gelen istekteki nonce değerini cevaba aynen koymak **zorundadır**. Eğer istekte nonce yok ise, sunucu, nonce eklentisini koymadan cevap **verebilmelidir**.

1.2.3 OCSP Tek Cevap Eklentileri

Herhangi bir tek cevap eklentisi kullanılmaması *önerilir*.

2. Kaynakça

[1] 25 Aralık 2008 tarih ve 223 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Yönetmelik (21 Nisan 2014 tarihli ve R.G 98 sayılı Değişiklik ile Birlikte)

[2] RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

3. Yürürlüğe Giriş

İşbu doküman, Kurul Kararı ile onaylanmasını müteakip 9 ay sonra yürürlüğe girer.