NİTELİKLİ ELEKTRONİK SERTİFİKA, SİL VE OCSP İSTEK/CEVAP MESAJLARI PROFİLLERİ

NİSAN 2007

İÇİNDEKİLER

1. Amaç ve Kapsam

23 Ocak 2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu [1] ve buna bağlı olarak Telekomünikasyon Kurumunun hazırlamış olduğu ikincil düzenlemeler ile Elektronik Sertifika Hizmet Sağlayıcılarının (ESHS) kurulması ve işletilmesi için gerekli kurallar tanımlanmıştır. Bu kurallar ve atıfta bulundukları standartlar elektronik sertifika ve elektronik imzayla ilgili genel çerçeveyi çizmektedir.

ESHS'lerin yayınladıkları nitelikli elektronik sertifikaların birbiriyle uyumlu olması, birlikte çalışabilirliğin sağlanması açısından oldukça önem arz eden bir husus haline gelmiştir. ESHS'lerin ortak bir elektronik sertifika profili kullanarak sertifika oluşturmaları, problemleri ortadan kaldıracak ve elektronik imza yazılımlarının sorunsuz olarak yazılarak Türkiye'de elektronik imza kullanımının yaygınlaşmasını sağlayacaktır.

Bu bağlamda, sertifikalar arasındaki uyumun sağlanması amacıyla Kurumumuzda gerçekleştirilen koordinasyon faaliyetleri sonucunda tüm ESHS'lerin üzerinde uzlaşıya vardığı bir "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi" oluşturulmuştur.

Bu doküman, elektronik imza mevzuatına uygun nitelikli elektronik sertifika profili, SİL profili ve OCSP profili tanımlamakta ve nitelikli elektronik sertifika profilinin kanunda tanımlanan nitelikli elektronik sertifika şartlarını nasıl sağladığını ifade etmektedir. Dokümanın son bölümünde de bu profillere göre oluşturulmuş örnek sertifika, SİL ve OCSP istek ve cevap mesajları kodlaması gösterilmektedir.

2. Dayanak

6 Ocak 2005 tarih ve 25692 sayılı Resmi Gazete yayımlanan 5070 Sayılı Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 35 inci maddesinde *"Elektronik imzayla ilgili bu Yönetmelikte hüküm bulunmayan haller için Kurul Kararı ile düzenleme yapılır"* hükmü yer almaktadır.

Bu bağlamda ESHS'lerin yayınladıkları nitelikli elektronik sertifikaların birbiriyle uyumlu olması ve birlikte çalışabilirliğin sağlanması açısından varolan ihtiyaçların karşılanmasına yönelik olarak söz konusu Yönetmeliğin 35 inci maddesine istinaden "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi" oluşturulmuştur.

3. Tanımlar ve Kısaltmalar

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı,

ETSI (European Telecommunications Standards Institute): Avrupa Telekomünikasyon Standartları Enstitüsü,

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri,

IETF RFC (Internet Engineering Task Force Request for Comments): İnternet Mühendisliği Görev Grubu Yorum Talebi,

ISO/IEC (International Organisation for Standardisation / International Electrotechnical Commitee): Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi,

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği,

OCSP (Online Certificate Status Protocol): Çevrimiçi Sertifika Durum Protokolü,

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması Nesne Belirteci (Object Identifier),

SİL : Sertifika İptal Listesi

4. Sertifika Profili

Bu profil, temel olarak ETSI TS 101 862 [2] 'de tanımlanan nitelikli sertifika profilini alarak T.C. 5070 sayılı Elektronik İmza Kanunu [1] 'nda belirtilen Nitelikli Elektronik Sertifika için bir profil tanımlar. Profil tanımlanırken Telekomünikasyon Kurumu tarafından yayınlanan tebliğ [3] göz önünde bulundurulmuş ve tebliğe uygunluk sağlanmıştır. ETSI TS 101 862 [2] temel olarak alındığından, RFC 3739 [4] , RFC 3280 [5] ve X.509 [6] 'da ifade edilenlerin tümü (tersi burada açık bir şekilde belirtilmediği sürece) geçerlidir.

4.1 Zorunlu Sertifika Alanları

Aşağıda belirtilenler dışındaki zorunlu alanlar diğer dokümanlarda tanımlandığı gibidir.

4.1.1 Genel kurallar

Subject ve Issuer gibi alanlarda kullanılan niteliklerde değer olarak genelde `DirectoryString` tipi kullanılmaktadır. `DirectoryString` tipi `PrintableString`, `TeletexString`, `BMPString`, `UTF8String` ve `UniversalString` tiplerinden birinin seçilmesi olarak [5] tanımlanmıştır. `DirectoryString` tipi ile tanımlanan nitelikler kullanıldığında `UTF8String` seçeneği kullanılarak kodlama **yapılmalıdır**. `C`, `serialNumber` ve `dc` gibi `DirectoryString` olmayan diğer nitelikler kullanıldığında kodlama niteliğin tanımlandığı gibi **yapılmalıdır**. Eğer tanımda `UTF8String` seçilebilirse, `UTF8String` **kullanılmalıdır**. `C` ve `serialNumber` için `PrintableString`, `dc` için `IA5String` kodlaması **kullanılmalıdır** [5] .

4.1.2 Geçerlilik (Validity) Alanı

RFC 3280 [5] 'de belirtildiği gibi 2049 yılına kadar UTCTime **kullanılmalı** ve zaman GMT(Zulu) olarak **kodlanmalıdır**. Detaylar için [5] 4.1.2.5 geçerlidir.

4.1.3 Yayımcı (Issuer) Alanı

Bu alanda Telekomünikasyon Kurumu tarafından onaylanmış bir isim **bulunmalıdır**. `O` niteliğinde ESHS'nin resmi adı yer **almalıdır** ve `C` niteliği "TR" **olmalıdır**. Bu alanda yer alacak diğer nitelikler ESHS'nin seçimine bağlıdır.

4.1.4 Özne (Subject) Alanı

Bu alan, sertifikanın verileceği kişinin ayırtedilebilir adını içerir. Özne alanı RFC 3739 [4] 'daki şartlara uygun olarak doldurulmalıdır. Bu şartlara ek olarak `commonName`, `serialNumber` ve `C` niteliklerinin bulunması **zorunludur**. `CommonName` niteliğinde sertifika alan kişinin tam adı (adı ve soyadı), `serialNumber` niteliğinde T.C. Kimlik numarası ve `C` niteliğinde "TR" değeri **bulunmalıdır**. Sertifika Türk vatandaşına verilmiyorsa `serialNumber` alanı pasaport numarasını **içermelidir**. `C` niteliği bu durumda da "TR" değerini **içermelidir**. `CommonName` niteliğine isim yazılırker kısaltmalar **kullanılmamalı** ve tam isim **yazılmalıdır**. Bu nitelik yazılırken ismin ilk harflerinin büyük diğer harflerinin küçük ve soyismin tüm harflerinin büyük olarak yazılması *önerilmektedir*. `Title` niteliği sertifika alan kişinin meslek ve/veya ünvan bilgisini içerebilir. Fakat bu nitelik sadece bilgi amaçlı kullanılabilir, meslek ve/veya ünvan belirtmek zorunda değildir.

4.1.5 Açık Anahtar (Public Key) Alanı

Verilecek sertifikaların anahtarları, tebliğde [3] belirtilen algoritma ve anahtar boylarına uyumlu **olmalıdır**.

4.2 Eklentiler

4.2.1 Yetkili Anahtarı Tanımlayıcısı (Authority Key Identifier) ve Özne Anahtarı Tanımlayıcısı (Subject Key Identifier) Eklentileri

Bu iki eklentinin de sertifikada bulunması *önerilir*.

Özne anahtar tanımlayıcısı eklenti değerinin RFC 3280 [5] 4.2.1.2 de geçen iki yöntemden birincisi ile oluşturulması *önerilir*. Buna göre, `subjectPublicKey` değeri (`BIT STRING` içine kodlanmadan önceki hali) 160 bit SHA-1 ile özetlenip kullanılır.

Yetkili Anahtar tanımlayıcısı eklentisinin değeri aşağıdakilerden biri **olmalıdır**:

1. AuthorityKeyIdentifier ASN1 yapısı içindeki `keyIdentifier` kullanılır ise; sertifikayı yayımlayan yetkilinin sertifikasındaki özne anahtarı tanımlayıcısı buraya **yazılmalıdır**.
2. AuthorityKeyIdentifier ASN1 yapısı içindeki `authorityCertIssuer` ve `authorityCertSerialNumber` kullanılır ise; sertifikayı yayımlayan yetkilinin sertifikasındaki yayımcı ve seri numarası **bulunmalıdır**.

Bu iki yöntemden birincinin kullanılması *önerilmektedir*.

Bu eklentilerin kritik değil olarak işaretlenmesi **gerekmektedir**.

4.2.2 Anahtar Kullanımı (Key Usage) Eklentisi

Anahtar Kullanımı eklentisi RFC 3739 [4]'da belirtildiği gibi bulunmak **zorundadır**. Anahtarların sadece elektronik imza amaçlı kullanıldığının ifade edilmesi için `nonRepudiation` (inkar edilemezlik) alanının tek başına veya `digitalSignature` (elektronik imza) alanıyla birlikte kullanılması, bunlar dışındaki anahtar kullanım alanlarının nitelikli elektronik sertifika içeriğinde bulunmaması **gerekmektedir**.

Bu eklentinin kritik olarak işaretlenmesi *önerilir*.

4.2.3 Sertifika İlkeleri (Certificate Policies) Eklentisi

Sertifika ilkeleri eklentisi RFC 3739 [4] 'da belirtildiği gibi bulunmak **zorundadır**. Sertifika ilkesinin ilke tanımlayıcısı (Certificate Policies-Policy Identifier) için ESHS, TSE'den almış olduğu nesne belirtecinin altında tahsis ettiği sertifika ilke tanımlayıcısını **kullanmalıdır**. Sertifika ilkesi içinde, kullanıcı uyarısı (user notice) alanına, açık metin olarak aşağıdaki açıklamanın yazılması **zorunludur**.

```
Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre
nitelikli elektronik sertifikadır.
```

Bu eklentinin kritik değil olarak işaretlenmesi *önerilir*.

4.2.4 Temel Kısıtlar (Basic Constraints) Eklentisi

Kullanıcılara verilen sertifikalarda temel kısıtlar eklentisinin olması, `cA` değerinin yanlış(false) ve `pathLenConstraint` değerinin de bulunmaması *önerilir*. Böylece verilen sertifikanın kullanıcıya (end entity) ait olduğu açık olarak ifade edilmiş olacaktır. Bu eklentinin kritik değil olarak işaretlenmesi *önerilir*.

4.2.5 Genişletilmiş Anahtar Kullanımı (Extended Key Usage) Eklentisi

Bu eklentinin kullanılmaması **gerekir**.

4.2.6 Özne Alternatif Adı (Subject Alternative Name) Eklentisi

Bu eklentinin kullanılmaması *önerilir*. Eğer elektronik sertifikada e-posta adresi bulunması isteniyorsa, e-posta adresi `rfc822Name` içine `IA5String` tipinde [5] **kodlanmalıdır**. Bu durumda sertifikayı oluşturan ESHS, e-posta adresinin sertifika sahibine ait olduğunu belirtmiş olacaktır. Bu nedenle sertifikalara yazılacak e-posta adreslerinin kurumsal e-posta adresi olması ve e-posta adresini veren kurumdan alınacak bir belge ile sahibine ait olduğunun ispat edilmesi *önerilir*. Kullanılması durumunda, bu eklentinin kritik değil olarak işaretlenmesi *önerilir*.

4.2.7 Özne Dizin Nitelikleri (Subject Directory Attributes) Eklentisi

Sertifikanın verildiği kişi hakkında ekstra bilgi bu eklentide verilebilir. Kişinin doğum tarihi (`dateOfBirth`), doğum yeri (`placeOfBirth`), cinsiyeti (`gender`), uyruğu (`countryOfCitizenship`) ve yaşadığı ülke (`countryOfResidence`) bilgileri RFC 3739 [4] 'da belirtildiği şekilde bu eklenti içine **yazılmalıdır**. Kişinin görevini sertifikada göstermek için özne dizin nitelikleri eklentisi içinde X.509 [6] 14.4'de tanımlanan `role` kullanılması *önerilir*. X.509 [6] 13.2 bu uygulamaya temel teşkil etmektedir. `Role` niteliği `generalNames` tipinde olmasına rağmen değer olarak `registeredID` seçeneği kullanılması *önerilir*.

Bu eklentinin kritik değil olarak işaretlenmesi **zorunludur** [4].

4.2.8 Nitelikli Sertifika İbareleri (Qualified Certificate Statements)

RFC 3739 [4] 3.2.6'da tanımlanan `qcStatements` eklentisi nitelikli sertifika ibareleri için kullanılacaktır. Bu eklentinin nesne belirteci değeri RFC 3739 [4] 'da tanımlanmıştır. Oluşturulacak sertifikalarda aşağıda tanımlanan iki nitelikli sertifika ibaresi de **bulunmalıdır**. Para limiti ibaresi ise istenirse eklenebilir. Bu eklentinin kritik değil olarak işaretlenmesi *önerilir*. Bu alanın kritik olarak işaretlenmesi, içindeki tüm ibarelerin kritik olarak işaretlenmesi anlamına gelir.

4.2.8.1 ETSI TS 101 862 Nitelikli Sertifika İbaresi

ETSI TS 101 862 ile uyumlu sertifikalar üretmek için, bu dokümanda tanımlanan `id-etsiqcs-QcCompliance` nesne belirtecini içeren ve değeri boş olan bir ibare **bulunmalıdır**.

4.2.8.2 Telekomünikasyon Kurumu Nitelikli Elektronik Sertifika İbaresi

Telekomünikasyon kurumu tarafından belirlenen nesne belirteci 2.16.792.1.61.0.1.5070.1.1 `{ joint-iso-itu-t(2) ülke(16) tr(792) yürütme(1) tk(61.0.1) nes-profili(5070) nes-ibaresi (1) nesuygunluğu (1)}` kullanılarak oluşturulacak bir ibare bulunmak **zorundadır**. Bu ibare değer olarak `UTF8String` tipinde bir ASN1 yapısı içerebilir. Görsel olarak, bu sertifikanın nitelikli elektronik sertifika olduğu, değerde yazılacaktır. Aşağıdaki yazının değer olarak kullanılması *önerilmektedir*.

```
Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre
nitelikli elektronik sertifikadır.
```

4.2.8.3 Para Limiti İbaresi

Sertifikanın kullanılacağı işlemler için para limiti olması durumunda kullanılacaktır. ETSITS 101 862 [2] 'de tanımlandığı gibi olacaktır. ETSI TS 101 862 [2] 'de tanımlanan `Iso4217CurrencyCode` yapısında, seçeneklerden `PrintableString` tipindeki `alphabetic` kullanılacaktır. Bu değer ISO 4217'de tanımlanan 3 karakterli para birimlerinden biri **olmalıdır**.

Türk Lirası için "TRL", Yeni Türk Lirası için de "TRY" **kullanılmalıdır**.

4.2.9 SİL Dağıtım Noktası (CRL Distribution Points) Eklentisi

Sertifikayla ilgili yayınlanacak SİL'e ulaşmak için gerekli bilgiyi içerir. Bu eklentinin yayınlanan nitelikli sertifikalarda bulunması **gerekmektedir**. 6. 'da belirtildiği gibi, SİL ve sertifika yayınlayan makamlar aynı olmak zorunda olduğundan, eklenti içindeki `distributionPoint` alanı dolu **olmalıdır**. Belirtilen yerdeki SİL'in, tüm iptal sebepleri için durumu belirtmesi **gerekmektedir**. Dolayısıyla değer içindeki `reasons` alanı **kullanılmamalıdır**.

Kritik değil olarak işaretlenmesi *önerilir*.

4.2.10 Hizmet Sağlayıcı Bilgi Erişimi (Authority Information Access) Eklentisi

Hizmet sağlayıcı bilgi ve servislerine ulaşmak için kullanılır. Bu profile uyan sertifikalarda, erişim metodu olarak `id-ad-ocsp` seçilerek OCSP servisine ulaşım noktasının bulunması **gerekir**. Ayrıca erişim metodu olarak `id-ad-caIssuers` seçilerek hizmet sağlayıcı sertifikasına ulaşım noktasının bulunması da *önerilmektedir*. Böylece sertifikayı işleyen istemcilerin hizmet sağlayıcıyla ilgili bilgilere erişimi kolaylaştırılmış olacaktır.

Kritik olarak **işaretlenmemelidir**.

5. Nitelikli Elektronik Sertifika Şartları ile Uyum

Aşağıdaki tablo, Elektronik İmza Kanunu [1] Madde 9'da tanımlanan nitelikli elektronik sertifikada bulunması zorunlu bilgilerin bu profil kullanılarak nasıl karşılandığını göstermektedir.

Nitelikli Elektronik Sertifika Tanımı	**Bu profile göre istenen şartın nasıl sağlanacağı**
a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare	Bu dokümanda, 4.2.8 Nitelikli Sertifika İbareleri (Qualified Certificate Statements)'daki ibarelerden 4.2.8.1 ve 4.2.8.2 ibareleri ile.
b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adı	Bu dokümanda 4.1.3 Yayımcı (Issuer) Alanı ile.
c) İmza sahibinin teşhis edilebileceği kimlik bilgileri	Bu dokümanda 4.1.4 Özne (Subject) Alanı ile.
d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi	Bu dokümanda 4.1.5 Açık Anahtar (Public Key) Alanı ile
e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihleri	Bu dokümanda 4.1.2 Geçerlilik (Validity) Alanı ile
f) Sertifikanın seri numarası	X.509 [6] ve RFC 3280 [5] 'de geçen sertifika seri numarası (Serial number) ile.
g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi	Bu dokümanda 4.2.7 Özne Dizin Nitelikleri (Subject Directory Attributes) Eklentisi belirtilen `role` niteliği ile.
h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgileri	Bu dokümanda geçen 4.1.4 Özne (Subject) Alanı dışında ihtiyaç duyulursa RFC 3739 [4] 3.2.1 ve 3.2.2'de tanımlanan `Subject Alternative Name` ve `Subject Directory Attributes` eklentileri ile.
i) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgiler	Kullanım şartları, bu dokümandaki 4.2.2 Anahtar Kullanımı (Key Usage) Eklentisi ve 4.2.3'de belirtildiği gibi eklenen sertifika politikası içinde belirtilir. Maddi sınırlamalara ilişkin bilgi bu dokümandaki 4.2.8.3 Para Limiti İbaresi ile belirtilir.
j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzası	X.509 [6] ve RFC 3280 [5] 'de tanımlandığı gibi sertifika imzalanır.

6. Sertifika İptal Listesi (SİL) Profili

Her ESHS, verdiği sertifikalarla ilgili iptal bilgisini içeren sertifika iptal listesi **yayımlamalıdır**. ESHS'nin sertifika ve SİL yayınlayan sertifika makamları aynı **olmalıdır**. Sertifika makamı tarafından yayımlanan SİL'ler, o sertifika makamı tarafından verilmiş tüm sertifikaları **kapsamalıdır**.

6.1 Zorunlu SİL Alanları

Aşağıda belirtilenler dışındaki zorunlu alanlar diğer dokümanlarda tanımlandığı gibidir.

6.1.1 Versiyon

Bu profile uygun olarak yayınlanan tüm SİL'lerin versiyonu v2 **olmalıdır**. Versiyonun v2 olması 1 olarak kodlanması ile sağlanır.

6.1.2 İmza Algoritması

SİL imzalamak için kullanılan algoritma, tebliğde [3] belirtilen algoritma ve anahtar boylarına uyumlu **olmalıdır**.

6.1.3 Yayımcı (Issuer Name) Alanı

Sertifika profili 4.1.3'de belirtilen yayımcı alanı ile aynı **olmalıdır**. Sadece görsel değer olarak değil, kodlama olarak da aynı olması **zorunludur**.

6.1.4 Yayınlama Tarihi (This Update)

SİL'in yayınlandığı tarihi gösterir. RFC 3280 [5] 'de belirtildiği gibi 2049 yılına kadar UTCTime **kullanılmalı** ve zaman GMT(Zulu) olarak **kodlanmalıdır**. Detaylar için [5] 4.1.2.5 geçerlidir.

6.1.5 Sonraki Yayınlama Tarihi (Next Update)

Bir sonraki SİL'in yayınlanacağı en geç tarihi gösterir. ESHS'ler bu tarihten önce mutlaka yeni SİL yayınlamak **zorundadırlar**. Sonraki Yayınlama Tarihi, daha önce yayınlanmış tüm SİL'lerin sonraki yayınlama tarihlerinden sonra **olmalıdır**.

ASN1 yapısında seçimli (optional) görünmesine rağmen, bu alanın SİL'lerde bulunması **zorunludur**.

RFC 3280 [5] 'de belirtildiği gibi 2049 yılına kadar UTCTime **kullanılmalı** ve zaman GMT(Zulu) olarak **kodlanmalıdır**. Detaylar için [5] 4.1.2.5 geçerlidir.

6.2 SİL Eklentileri

6.2.1 Yetkili Anahtarı Tanımlayıcısı (Authority Key Identifier) Eklentisi

Bu eklentinin SİL'de bulunması **zorunludur**. Değeri 4.2.1'de açıklanan yetkili anahtar tanımlayıcısı gibi **olmalıdır**.

Bu eklenti kritik olarak **işaretlenmemelidir**.

6.2.2 SİL Numarası (CRL Number) Eklentisi

Bu eklentinin SİL'de bulunması **zorunludur**. Bu numara, ESHS'nin yayınladığı SİL'ler için düzenli olarak **artmalıdır**. Böylece yayınlanan iki SİL'den hangisinin daha önce yayınlandığı kesin olarak bilinebilir.

Bu eklenti kritik olarak **işaretlenmemelidir**.

6.3 SİL Eleman Eklentileri

6.3.1 Sebep Kodu (Reason Code) Eklentisi

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**.

7. Çevrimiçi Sertifika Durum Protokolü (OCSP)

Burada aksi belrtilmedikçe, OCSP istek ve cevap mesajları RFC 2560 [7] 'da tanımlandığı gibi **olmalıdır**. Bu profile uyan ESHS'lerin OCSP sunucuları http üzerinden gelen isteklere cevap **verebilmelidir**.

7.1 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.

7.1.1 OCSP İstek Mesajı Eklentileri

7.1.1.1 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*.

7.1.1.2 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**.

7.1.2 OCSP Tek İstek Eklentileri

Herhangi bir tek istek eklentisi kullanılmaması *önerilir*.

7.2 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**.

7.2.1 Zorunlu OCSP Cevap Alanları

7.2.1.1 İmza Algoritması Alanı (BasicOCSPResponse yapısı signatureAlgorithm)

Cevap imzalanırken kullanılan algoritma, tebliğde [3] belirtilen algoritma ve anahtar boylarına uyumlu **olmalıdır**.

7.2.1.2 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**.

7.2.1.3 Sebep Kodu (RevokedInfo yapısı revocationReason)

6.3.1'de anlatıldığı gibi sertifikanın iptal edilme sebebini belirten yapının eklenmesi *önerilir*. 6.3.1'deki şartlar burada da geçerlidir.

7.2.2 OCSP Cevap Eklentileri

7.2.2.1 Nonce

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

7.2.3 OCSP Tek Cevap Eklentileri

Herhangi bir tek cevap eklentisi kullanılmaması *önerilir*.

8. Örnek Kodlamalar

Örnek kodlamalarda, ":" öncesindeki sayılar sırasıyla, verinin kaçıncı baytında olduğumuzu, tag baytının değerini ve bu elemanın uzunluğunu ifade eder.

8.1 Örnek Nitelikli Elektronik Sertifika Kodlaması

```
   0 30 2138: SEQUENCE {
   4 30 1602:   SEQUENCE {
   8 A0    3:     [0] {
  10 02    1:       INTEGER 2
             :       }
  13 02    1:     INTEGER 44
  16 30   13:     SEQUENCE {
  18 06    9:       OBJECT IDENTIFIER
             :         sha1withRSAEncryption (1 2 840 113549 1 1 5)
  29 05    0:       NULL
             :       }
  31 30   98:     SEQUENCE {
  33 31   11:       SET {
  35 30    9:         SEQUENCE {
  37 06    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
  42 13    2:           PrintableString 'TR'
             :           }
             :         }
  46 31   24:       SET {
  48 30   22:         SEQUENCE {
  50 06    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
  55 0C   15:           UTF8String 'ESHS Resmi Adı'
             :           }
             :         }
  72 31   57:       SET {
  74 30   55:         SEQUENCE {
  76 06    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
  81 0C   48:           UTF8String
             :             'Test Elektronik Sertifika Hizmet Sağlayıcısı'
             :           }
             :         }
             :       }
 131 30   30:     SEQUENCE {
 133 17   13:       UTCTime '070321120955Z'
 148 17   13:       UTCTime '091215120955Z'
             :       }
 163 30   74:     SEQUENCE {
 165 31   11:       SET {
 167 30    9:         SEQUENCE {
 169 06    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 174 13    2:           PrintableString 'TR'
             :           }
             :         }
 178 31   20:       SET {
 180 30   18:         SEQUENCE {
 182 06    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
 187 13   11:           PrintableString '12345678901'
             :           }
             :         }
```

```
200 31   37:       SET {
202 30   35:         SEQUENCE {
204 06    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
209 0C   28:           UTF8String 'Çiğdem Işıl ÜSTÜNOĞLU'
           :           }
           :         }
           :       }
239 30  290:     SEQUENCE {
243 30   13:       SEQUENCE {
245 06    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
256 05    0:         NULL
           :         }
258 03  271:       BIT STRING 0 unused bits, encapsulates {
263 30  266:           SEQUENCE {
267 02  257:             INTEGER
           :               00 B6 6C 37 30 66 A3 6F 73 D4 86 36 8C E5 12 41
           :               6A 59 B6 9F B0 F7 5A 4E 78 46 25 5D 84 B0 9B 55
           :               53 1A 49 2F 05 6F 87 51 EB BA 60 A7 2E BB CA 24
           :               5B EE D5 46 ED 4D 12 2C A4 B1 DC D1 2E B7 F1 D2
           :               67 9D 70 D5 1A 08 3C 92 BF 32 67 55 81 44 52 05
           :               36 5D 70 8A 31 C4 E5 6A C1 03 88 D1 96 CF 9A 89
           :               3E ED 5A 52 11 99 F3 CF 06 71 4D 77 EE F9 2A 78
           :               48 DA A3 F7 58 F8 59 FF 38 FA 94 1B E2 8F 0B B2
           :                       [ Another 129 bytes skipped ]
528 02    3:             INTEGER 65537
           :             }
           :           }
           :       }
533 A3 1073:     [3] {
537 30 1069:       SEQUENCE {
541 30   31:         SEQUENCE {
543 06    3:           OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
548 04   24:           OCTET STRING, encapsulates {
550 30   22:               SEQUENCE {
552 80   20:                 [0]
           :                   41 57 F5 72 7F CD AD 65 3A 51 67 CB 68 A2 89 92
           :                   59 BC 69 11
           :                 }
           :               }
           :           }
574 30   29:         SEQUENCE {
576 06    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
581 04   22:           OCTET STRING, encapsulates {
583 04   20:               OCTET STRING
           :                 43 02 6F 7E D8 0D 67 2A 23 24 2B B1 DB 18 C1 70
           :                 B5 53 E0 3C
           :               }
           :           }
605 30   14:         SEQUENCE {
607 06    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
612 01    1:           BOOLEAN TRUE
615 04    4:           OCTET STRING, encapsulates {
617 03    2:               BIT STRING 6 unused bits
           :                 '11'B
           :               }
           :           }
621 30  308:         SEQUENCE {
625 06    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
630 04  299:           OCTET STRING, encapsulates {
634 30  295:               SEQUENCE {
638 30  291:                 SEQUENCE {
642 06   11:                   OBJECT IDENTIFIER '2 16 792 1 2 1 1 5 7 1 1'
655 30  274:                   SEQUENCE {
659 30   47:                     SEQUENCE {
661 06    8:                       OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
671 16   35:                       IA5String 'http://www.testsm.net.tr/TESTSM_SUE'
           :                       }
708 30  222:                     SEQUENCE {
711 06    8:                       OBJECT IDENTIFIER
           :                         unotice (1 3 6 1 5 5 7 2 2)
721 30  209:                       SEQUENCE {
```

```
 724 1E  206:                          BMPString
           :                    'Bu sertifika, 5070 sayılı Elektronik İmza Kan'
           :                    'ununa göre nitelikli elektronik sertifikadır.'
           :                          }
           :                        }
           :                      }
           :                    }
           :                  }
           :                }
           :              }
 933 30    9:           SEQUENCE {
 935 06    3:             OBJECT IDENTIFIER basicConstraints (2 5 29 19)
 940 04    2:             OCTET STRING, encapsulates {
 942 30    0:               SEQUENCE {}
           :               }
           :             }
 944 30  181:           SEQUENCE {
 947 06    3:             OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
 952 04  173:             OCTET STRING, encapsulates {
 955 30  170:               SEQUENCE {
 958 30   44:                 SEQUENCE {
 960 A0   42:                   [0] {
 962 A0   40:                     [0] {
 964 86   38:                       [6] 'http://www.testsm.net.tr/TESTSMSIL.crl'
           :                       }
           :                     }
           :                   }
1004 30  122:                 SEQUENCE {
1006 A0  120:                   [0] {
1008 A0  118:                     [0] {
1010 86  116:                       [6]
           :                     'ldap://dizin.testsm.gov.tr/C=TR,O=TESTSM,CN=TEST'
           :                     'SMSIL?certficateRevocationList?base?objectclass='
           :                     'cRLDistributionPoint'
           :                       }
           :                     }
           :                   }
           :                 }
           :               }
           :             }
1128 30  223:           SEQUENCE {
1131 06    8:             OBJECT IDENTIFIER
           :               authorityInfoAccess (1 3 6 1 5 5 7 1 1)
1141 04  210:             OCTET STRING, encapsulates {
1144 30  207:               SEQUENCE {
1147 30   47:                 SEQUENCE {
1149 06    8:                   OBJECT IDENTIFIER
           :                     caIssuers (1 3 6 1 5 5 7 48 2)
1159 86   35:                   [6] 'http://www.testsm.net.tr/TESTSM.crt'
           :                   }
1196 30  116:                 SEQUENCE {
1198 06    8:                   OBJECT IDENTIFIER
           :                     caIssuers (1 3 6 1 5 5 7 48 2)
1208 86  104:                   [6]
           :                   'ldap://dizin.testsm.net.tr/C=TR,O=TESTSM,CN=TEST'
           :                   'SM?cACertificate?base?objectclass=certificationA'
           :                   'uthority'
           :                   }
1314 30   38:                 SEQUENCE {
1316 06    8:                   OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
1326 86   26:                   [6] 'http://ocsp.testsm.net.tr/'
           :                   }
           :                 }
           :               }
           :             }
1354 30   87:           SEQUENCE {
1356 06    3:             OBJECT IDENTIFIER subjectDirectoryAttributes (2 5 29 9)
1361 04   80:             OCTET STRING, encapsulates {
1363 30   78:               SEQUENCE {
1365 30   16:                 SEQUENCE {
1367 06    8:                   OBJECT IDENTIFIER
```

```
           :                     countryOfCitizenship (1 3 6 1 5 5 7 9 4)
1377 31    4:                   SET {
1379 13    2:                     PrintableString 'TR'
           :                     }
           :                   }
1383 30   16:                 SEQUENCE {
1385 06    8:                   OBJECT IDENTIFIER
           :                     countryOfResidence (1 3 6 1 5 5 7 9 5)
1395 31    4:                   SET {
1397 13    2:                     PrintableString 'TR'
           :                     }
           :                   }
1401 30   15:                 SEQUENCE {
1403 06    8:                   OBJECT IDENTIFIER gender (1 3 6 1 5 5 7 9 3)
1413 31    3:                   SET {
1415 13    1:                     PrintableString 'F'
           :                     }
           :                   }
1418 30   23:                 SEQUENCE {
1420 06    8:                   OBJECT IDENTIFIER
           :                     placeOfBirth (1 3 6 1 5 5 7 9 2)
1430 31   11:                   SET {
1432 0C    9:                     UTF8String 'İstanbul'
           :                     }
           :                   }
           :                 }
           :               }
           :             }
1443 30  164:           SEQUENCE {
1446 06    8:             OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
1456 01    1:             BOOLEAN TRUE
1459 04  148:             OCTET STRING, encapsulates {
1462 30  145:                 SEQUENCE {
1465 30    8:                   SEQUENCE {
1467 06    6:                     OBJECT IDENTIFIER
           :                       id-etsi-qcs-QcCompliance (0 4 0 1862 1 1)
           :                     }
1475 30   21:                   SEQUENCE {
1477 06    6:                     OBJECT IDENTIFIER
           :                       id-etsi-qcs-QcLimitValue (0 4 0 1862 1 2)
1485 30   11:                     SEQUENCE {
1487 13    3:                       PrintableString 'TRY'
1492 02    1:                       INTEGER 1
1495 02    1:                       INTEGER 3
           :                       }
           :                     }
1498 30  110:                   SEQUENCE {
1500 06   11:                     OBJECT IDENTIFIER
           :                       Telekomunikasyon Kurumu NES OID (2 16 792 1 61 0 1
5070 1 1)
1513 0C   95:                     UTF8String
           :                     'Bu sertifika, 5070 sayılı Elektronik İmza Kan'
           :                     'ununa göre nitelikli elektronik sertifikadır.'
           :                     }
           :                   }
           :                 }
           :               }
           :             }
           :           }
           :         }
1610 30   13:     SEQUENCE {
1612 06    9:       OBJECT IDENTIFIER
           :         sha1withRSAEncryption (1 2 840 113549 1 1 5)
1623 05    0:       NULL
           :       }
1625 03  513:     BIT STRING 0 unused bits
           :       09 97 D6 C2 2F 31 80 8B 5B C6 98 B0 A0 1A EE 28
           :       B7 51 0B FC EF 69 55 B9 D1 8F 5C 00 13 9F 11 E3
           :       1F 24 27 33 9B F0 77 6A 51 48 84 C5 4A 93 2F 25
           :       D8 BE AE 67 1E 83 5E 47 88 1F 8D 15 A6 C5 89 EA
           :       11 B9 9B AA C5 97 7D F9 8D EE 93 CC 8E 61 DC 7D
```

```
           :     9D 9D 0E 38 75 85 CD C5 33 A2 C4 84 16 CB 09 3A
           :     A1 5B AE E8 38 A5 E7 E3 E8 E0 E1 FF 15 E5 C2 F3
           :     A6 76 52 CE 00 9F BD EB 45 74 0B CB B7 20 2C 2C
           :             [ Another 384 bytes skipped ]
           :   }
```

8.2 Örnek SİL Kodlaması

```
  0 30  768: SEQUENCE {
  4 30  233:   SEQUENCE {
  7 02    1:     INTEGER 1
 10 30   13:     SEQUENCE {
 12 06    9:       OBJECT IDENTIFIER
           :         sha1withRSAEncryption (1 2 840 113549 1 1 5)
 23 05    0:       NULL
           :       }
 25 30   98:     SEQUENCE {
 27 31   11:       SET {
 29 30    9:         SEQUENCE {
 31 06    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 36 13    2:           PrintableString 'TR'
           :           }
           :         }
 40 31   24:       SET {
 42 30   22:         SEQUENCE {
 44 06    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 49 0C   15:           UTF8String 'ESHS Resmi Adı'
           :           }
           :         }
 66 31   57:       SET {
 68 30   55:         SEQUENCE {
 70 06    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
 75 0C   48:           UTF8String
           :             'Test Elektronik Sertifika Hizmet Sağlayıcısı'
           :           }
           :         }
           :       }
125 17   13:     UTCTime '070320134858Z'
140 17   13:     UTCTime '070321134858Z'
155 30   34:     SEQUENCE {
157 30   32:       SEQUENCE {
159 02    1:         INTEGER 21
162 17   13:         UTCTime '070320134543Z'
177 30   12:         SEQUENCE {
179 30   10:           SEQUENCE {
181 06    3:             OBJECT IDENTIFIER cRLReason (2 5 29 21)
186 04    3:             OCTET STRING, encapsulates {
188 0A    1:                 ENUMERATED 1
           :                 }
           :             }
           :           }
           :         }
           :       }
191 A0   47:     [0] {
193 30   45:       SEQUENCE {
195 30   10:         SEQUENCE {
197 06    3:           OBJECT IDENTIFIER cRLNumber (2 5 29 20)
202 04    3:           OCTET STRING, encapsulates {
204 02    1:               INTEGER 21
           :               }
           :           }
207 30   31:         SEQUENCE {
209 06    3:           OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
214 04   24:           OCTET STRING, encapsulates {
216 30   22:               SEQUENCE {
218 80   20:                 [0]
           :                   41 57 F5 72 7F CD AD 65 3A 51 67 CB 68 A2 89 92
           :                   59 BC 69 11
           :                 }
           :               }
```

```
           :           }
           :         }
           :       }
           :     }
240 30   13:   SEQUENCE {
242 06    9:     OBJECT IDENTIFIER
           :       sha1withRSAEncryption (1 2 840 113549 1 1 5)
253 05    0:     NULL
           :     }
255 03  513:   BIT STRING 0 unused bits
           :     4A C8 19 6D DA AA 89 10 2A 6E 30 70 71 34 39 0B
           :     0D 2B 07 65 7E 89 46 A2 F0 17 9F 0D EC 0F 31 1C
           :     82 21 F4 AD 0B 5F E6 16 A4 9F EE F5 6B 2A 6A 1B
           :     78 3E 2E 61 2B 1E BC 3B BE A4 20 41 87 DA 42 E7
           :     CE 0F 39 F1 18 6D 68 A0 E3 9C BA 49 7F 09 78 AF
           :     EA AF EC 5C 91 EA 83 A8 29 8F 8A 2C C0 44 39 20
           :     08 51 B1 43 2C 37 CA D3 B8 A7 89 B8 70 E0 5B EA
           :     FD B0 A3 FC E0 41 E3 46 91 5B 82 AB D4 D5 6D B1
           :             [ Another 384 bytes skipped ]
           :   }
```

9. Kaynakça

[1] 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu

[2] ETSI TS 101 862 Qualified Certificate profile 2004-03

[3] 6 Ocak 2005 tarih ve 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

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

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

[6] ITU-T X.509 The Directory: Public-key and attribute certificate frameworks

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