BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURULU
KARARI

Karar Tarihi	: 24.01.2023
Karar Sayısı	: 2023/İK-BTD/43
Gündem Konusu	: Nitelikli Elektronik Mühür Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi

KARAR : Bilgi Teknolojileri Dairesi Başkanlığının hazırladığı takrir ve ekleri incelenmiştir.

ESHS'lerin yayınladıkları nitelikli elektronik mühür sertifikalarının birbiriyle uyumlu olması, birlikte çalışabilirliğin sağlanabilmesi ve Ülkemizde elektronik mühür kullanımında uygulamalarda yaşanabilecek uyum problemlerinin engellenebilmesi amacıyla "Nitelikli Elektronik Mühür Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi" hazırlanmıştır. ESHS'lerin nitelikli elektronik mühür sertifikası, SİL ve OCSP istek/cevap mesajlarını "Nitelikli Elektronik Mühür Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi"ne uygun yayımlamaları hususunda Kurul Kararı alınması ve söz konusu Kurul Kararı ve ekinin Kurum internet sayfasında yayınlanarak kamuoyuna duyurulması hususlarına karar verilmiştir.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

K-Q TSE-ISO-EN 9000

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

Sürüm 1.0

Ocak 2023

İÇİNDEKİLER

1. Amaç ve Kapsam 4

2. Dayanak 4

3. Tanımlar ve Kısaltmalar 5

4. Sertifika Profili 5

4.1 Zorunlu Sertifika Alanları 5

4.1.1 Genel kurallar 6

4.1.2 Geçerlilik (Validity) Alanı 6

4.1.3 Yayımcı (Issuer) Alanı 6

4.1.4 Özne (Subject) Alanı 6

4.1.5 Açık Anahtar (Public Key) Alanı 7

4.2 Eklentiler 7

4.2.1 Yetkili Anahtarı Tanımlayıcısı (Authority Key Identifier) ve Özne Anahtarı Tanımlayıcısı (Subject Key Identifier) Eklentileri 7

4.2.2 Anahtar Kullanımı (Key Usage) Eklentisi 7

4.2.3 Sertifika İlkeleri (Certificate Policies) Eklentisi 7

4.2.4 Temel Kısıtlar (Basic Constraints) Eklentisi 7

4.2.5 Genişletilmiş Anahtar Kullanımı (Extended Key Usage) Eklentisi 8

4.2.6 Özne Alternatif Adı (Subject Alternative Name) Eklentisi 8

4.2.7 Özne Dizin Nitelikleri (Subject Directory Attributes) Eklentisi 8

4.2.8 Nitelikli Sertifika İbareleri (Qualified Certificate Statements) 8

4.2.8.1 ETSI TS 101 862 Nitelikli Sertifika İbaresi 8

4.2.8.2 Bilgi Teknolojileri ve İletişim Kurumu Nitelikli Elektronik Mühür Sertifika İbaresi 8

4.2.8.3 Para Limiti İbaresi 8

4.2.8.4 Kullanım Kısıtı 8

4.2.9 SİL Dağıtım Noktası (CRL Distribution Points) Eklentisi 9

4.2.10 Hizmet Sağlayıcı Bilgi Erişimi (Authority Information Access) Eklentisi 9

5. Nitelikli Elektronik Sertifika Şartları ile Uyum 9

6. Sertifika İptal Listesi (SİL) Profili 10

6.1 Zorunlu SİL Alanları 10

6.1.1 Versiyon 10

6.1.2 İmza Algoritması 10

6.1.3 Yayımcı (Issuer Name) Alanı 10

6.1.4 Yayımlama Tarihi (This Update) 10

6.1.5 Sonraki Yayımlama Tarihi (Next Update) 10

6.2 SİL Eklentileri 11

6.2.1 Yetkili Anahtarı Tanımlayıcısı (Authority Key Identifier) Eklentisi 11

6.2.2 SİL Numarası (CRL Number) Eklentisi 11

6.2.3 Hizmet Sağlayıcı Bilgi Erişimi (Authority Information Access) Eklentisi 11

6.3 SİL Eleman Eklentiler 11

6.3.1 Sebep Kodu (Reason Code) Eklentisi 11

7. Çevrimiçi Sertifika Durum Protokolü (OCSP) 11

7.1 OCSP İstek Mesajı 11

7.1.1 OCSP İstek Mesajı Eklentileri 11

7.1.1.1 Nonce Eklentisi 11
7.1.1.2 Kabul edilebilir Cevap Tipleri (Acceptable Response Types) Eklentisi 12
7.1.2 OCSP Tek İstek Eklentileri 12
7.2 OCSP Cevap Mesajı 12
7.2.1 Zorunlu OCSP Cevap Alanları 12
7.2.1.1 İmza Algoritması Alanı (BasicOCSPResponse yapısı signatureAlgorithm) 12
7.2.1.2 Sonraki Güncelleme Alanı(SingleResponse yapısı nextUpdate) 12
7.2.1.3 Sebep Kodu (RevokedInfo yapısı revocationReason) 12
7.2.2 OCSP Cevap Eklentileri 12
7.2.2.1 Nonce 12
7.2.3 OCSP Tek Cevap Eklentileri 12
8. Örnek Kodlamalar 12
8.1 Örnek Nitelikli Elektronik Sertifika Kodlaması 12
8.2 Örnek SİL Kodlaması 17
9. Kaynakça 19

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 Bilgi Teknolojileri ve İletişim Kurumu'nun hazırlamış olduğu ikincil düzenlemeler ile Elektronik Sertifika Hizmet Sağlayıcılarının (ESHS) bildirim usulune göre yetkilendirilmeleri ve faaliyetlerinin devamı için gerekli kurallar belirlenmiştir. Müteakiben Ülkemizde elektronik mührün hukuki ve teknik altyapısının oluşturulması ihtiyacı hasıl olmuş ve bu kapsamda 03/02/2021 tarihli ve 31384 sayılı Resmi Gazete'de yayımlanan 7263 sayılı Teknoloji Geliştirme Bölgeleri Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 14'üncü maddesi ile, Avrupa Parlamentosu tarafından 23/07/2014 tarihinde kabul edilen "Elektronik Kimlik Belirleme ve Elektronik Ortamda Gerçekleştirilen İşlemlerde Kullanılan Güven Hizmetlerine İlişkin Düzenlemesi (eIDAS Tüzüğü) ile uyumlu olacak şekilde 5070 sayılı Elektronik İmza Kanunu'na Elektronik Mühre ilişkin Ek Madde 1'eklenmiştir. Bu değişiklik uyarınca, elektronik mührün ülkemizde uygulanabilmesi için gerekli teknik ve idari kriterlerin belirlenebilmesi amacıyla hazırlanan Elektronik Mühre İlişkin Usul Ve Esaslar Hakkında Yönetmelik 14.09.2022 tarihli ve 31953 sayılı Resmî Gazete'de yayımlanatak yürürlüğe girmiştir. Bu kurallar ve ilgili mevzuat ile atıfta bulunulan standartlar ile elektronik sertifika, elektronik imza ve elektronik mühürle ilgili genel çerçeve çizilmiştir.

Elektronik Mühre İlişkin Usul Ve Esaslar Hakkında Yönetmeliğin yayımlanması ile ESHS'ler tarafından yayımlanan nitelikli elektronik sertifikaların birbiriyle uyumlu olması gibi, ESHS'lerin yayımladıkları nitelikli elektronik mühür sertifikalarının da birbiriyle uyumlu olması, birlikte çalışabilirliğin sağlanması açısından oldukça önem arz eden bir husus haline gelmiştir. ESHS'lerin ortak bir elektronik mühür sertifika profili kullanarak sertifika oluşturmaları sonucu, Türkiye'de elektronik mühür kullanımında yaşanabilecek uyum problemlerinin engellenmesini sağlayacaktır.

Bu bağlamda, sertifikalar arasındaki uyumun sağlanması amacıyla Kurumumuz koordinasyonunda tüm ESHS'lerin üzerinde uzlaşıya vardığı bir "Nitelikli Elektronik Mühür Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi" oluşturulmuştur.

Bu doküman, elektronik mühür mevzuatına uygun nitelikli elektronik mühür sertifika profili, SİL profili ve OCSP profili tanımlamakta ve nitelikli elektronik mühür sertifika profilinin Kanunda tanımlanan nitelikli elektronik mühür 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

5070 sayılı Elektronik İmza Kanunu'nun "Yönetmelik" başlıklı 20'nci maddesinde yeralan "*Bu Kanunun uygulanmasına ilişkin usul ve esaslar, ilgili kurum ve kuruluşların görüşü alınarak Kurum tarafından çıkarılacak yönetmeliklerle düzenlenir*." hükmü ile Kanun kapsamında düzenlenen elektronik imza, elektronik mühür, elektronik sertifika ile ilgili düzenlemeleri hazırlama görevi Bilgi Teknolojileri ve İletişim Kurumuna verilmiştir.

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.

14.09.2022 tarihli ve 31953 sayılı Resmî Gazete'de yayımlanan Elektronik Mühre İlişkin Usul Ve Esaslar Hakkında Yönetmelik ile elektronik mührün hukuki ve teknik yönleri ile uygulanmasına ilişkin usul ve esaslar belirlenmiştir.

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

3. Tanımlar ve Kısaltmalar

a) ESHS : Elektronik Sertifika Hizmet Sağlayıcısı

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

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

d) ETSI EN : ETSI Avrupa Normları (ETSI European Norms)

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

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

g) ITU : Uluslararası Telekomünikasyon Birliği (International Telecommunication Union):

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

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

j) SİL : Sertifika İptal Listesi

4. Sertifika Profili

Bu profil, temel olarak ETSI TS 101 862 [3] ve bu standartın güncel versiyonu olan ETSI EN 319 412-5'de tanımlanan nitelikli sertifika profilini alarak T.C. 5070 sayılı Elektronik İmza Kanunu [1] uyarınca hazırlanan ve "Elektronik Mühre İlişkin Usul Ve Esaslar Hakkında Yönetmelik"te [2] belirtilen Nitelikli Elektronik Mühür Sertifikası için bir profil tanımlar. Profil tanımlanırken Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanarak 6 Ocak 2005 tarih ve 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğe [4] uygunluk sağlanmıştır. ETSI TS 101 862 (ETSI EN 319 412-5) temel olarak alındığından, RFC 3739 [[5] , RFC 5280 [6] ve X.509 [7[7] 'de 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 [6] 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** [6] .

4.1.2 Geçerlilik (Validity) Alanı

RFC 5280 [6]]'de belirtildiği gibi 2049 yılına kadar *UTCTime* **kullanılmalı** ve zaman GMT(Zulu) olarak **kodlanmalıdır**. Detaylar için [6] 4.1.2.5 geçerlidir.

4.1.3 Yayımcı (Issuer) Alanı

Bu alanda Bilgi Teknolojileri ve İletişim 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 tüzel kişinin ayırtedilebilir adını içerir. *Subject* alanı RFC 3739 [5] [5] 'daki şartlara uygun olarak doldurulmalıdır. Bu şartlara ek olarak *commonName, serialNumber, OrganizationIdentifier* ve *C* niteliklerinin bulunması **zorunludur**.

CommonName niteliğinde, sertifika alan tüzel kişi eğer ticaret şirketi ise şirketin tam adı, eğer ticaret şirketi değil ise tüzel kişinin bağlı bulunduğu resmî sicile tescil edilen veya ilgili mevzuat ile belirlenen adı/unvanı **bulunmalıdır**. *CommonName* niteliğine isim yazılırken tümü büyük harf olacak şekilde ve kısaltmalar **kullanılmadan** tam isim **yazılmalıdır.** *OrganizationName* niteliği opsiyonel olarak *CommonName* niteliği ile uyumlu olacak şekilde kullanılabilir.

SerialNumber niteliğinde, sertifika alan; gerçek kişi veya tek ortaklı şahıs şirketi olması halinde T.C. Kimlik Numarası, tüzel kişiliğin kamu kurum kuruluşu olması halinde DETSİS Numarası, diğer her türlü durumda Vergi Kimlik Numarası **bulunması esastır**. Sertifika alan tüzel kişinin Vergi Kimlik Numarasının tanımlı olmaması halinde veya *SerialNumber* niteliğine ilişkin farklı bir uyumluluk ihtiyacının ortaya çıkması durumunda bu nitelikte, MERSİS numarası veya Ticaret Sicil Numarası veya tüzel kişinin bağlı bulunduğu resmî sicile tescil edilen veya ilgili mevzuat ile belirlenen tekil kayıt numarası **bulunmalıdır.**

OrganizationIdentifier niteliğinde, sertifika alan; gerçek kişi veya tek ortaklı şahıs şirketi olması halinde T.C. Kimlik Numarası, diğer her türlü durumda (kamu ya da, özel tüzel kişilikleri fark etmeksizin) Vergi Kimlik Numarası **bulunması esastır**. **S**ertifika alanın, Vergi Kimlik Numarasının tanımlı olmaması halinde *OrganizationIdentifier* niteliğinin değeri **"0" (sıfır) olarak girilir.**

Yabancı Kimlik Numarası kullanılması gereken durumlarda, T.C. Kimlik Numarası ile ilgili esaslar uygulanır.

C niteliği "TR" değerini **içermelidir**.

4.1.5 Açık Anahtar (Public Key) Alanı

Verilecek sertifikaların anahtarları, Tebliğde [4] belirtilen algoritma ve parametrelerin anahtar boyları ile 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*.

Subject anahtar tanımlayıcısı eklenti değerinin RFC 5280 [6] 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 [5]'de 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 mühür sertifika içeriğinde bulunmaması **gerekmektedir**.

Bu eklentinin kritik olarak işaretlenmesi *önerilir*.

4.2.3 Sertifika İlkeleri (Certificate Policies) Eklentisi

Sertifika ilkeleri eklentisi RFC 3739 [5] 'de 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 mühür sertifikasıdır."

Bu eklentinin kritik değil olarak işaretlenmesi *önerilir*.

4.2.4 Temel Kısıtlar (Basic Constraints) Eklentisi

Kullanıcılara verilen sertifikalarda temel kısıtlar eklentisinin olması halinde, *cA* değerinin yanlış(false) ve *pathLenConstraint* değerinin de bulunmaması ***zorunludur.*** 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 [6] **kodlanmalıdır**. Kullanılması durumunda, bu eklentinin kritik değil olarak işaretlenmesi *önerilir*.

4.2.7 Özne Dizin Nitelikleri (Subject Directory Attributes) Eklentisi

Bu eklentinin kullanılmaması *önerilir.*

4.2.8 Nitelikli Sertifika İbareleri (Qualified Certificate Statements)

RFC 3739 [5] 3.2.6'da tanımlanan *qcStatements* eklentisi nitelikli sertifika ibareleri için kullanılacaktır. Bu eklentinin nesne belirteci değeri RFC 3739 [5] 'da tanımlanmıştır. Oluşturulacak sertifikalarda aşağıda tanımlanan üç nitelikli sertifika ibaresi de **bulunmalıdır**. 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 (ETSI EN 319 412-5) 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 Bilgi Teknolojileri ve İletişim Kurumu Nitelikli Elektronik Mühür Sertifika İbaresi

Bilgi Teknolojileri ve İletişim Kurumu tarafından belirlenen nesne belirteci 2.16.792.1.61.0.1.5070.2.1 { joint-iso-itu-t(2) ülke(16) tr(792) yürütme(1) tk(61.0.1) nes-profili(5070) nitelikli-emuhur-ibaresi (2) emuhuruygunluğu (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 mühür sertifikasıdır."

4.2.8.3 Para Limiti İbaresi

Bu eklentinin kullanılmaması gerekir.

4.2.8.4 Kullanım Kısıtı

Nitelikli elektronik mühür sertifikaları, Elektronik Mühre İlişkin Usul Ve Esaslar Hakkında Yönetmeliğin [2] 7'nci maddesini üçüncü fıkrası uyarınca, güvenli elektronik imza oluşturmak amacıyla kullanılamaz. Bu kısıtın Kullanım Kısıtı olarak sertifikaya yazılması **zorunludur**. Kısıtı tanımlayan ibare olarak Bilgi Teknolojileri ve İletişim Kurumu tarafından belirlenen nesne belirteci 2.16.792.1.61.0.1.5070.2.2 { joint-iso-itu-t(2) ülke(16) tr(792) yürütme(1) tk(61.0.1) nes-profili(5070) nitelikli-emuhur-ibaresi (2) emuhur-kullanım-kısıtı (2)} kullanılarak oluşturulacak bir ibare bulunmak **zorundadır**. Bu ibare değer olarak *UTF8String* tipinde bir ASN1 yapısı içerebilir. Görsel olarak, bu sertifikanın güvenli elektronik imza oluşturmak için kullanılamayacağı, değerde yazılacaktır. Aşağıdaki yazının değer olarak kullanılması *önerilmektedir*.

"Bu sertifika, güvenli elektronik imza oluşturmak amacıyla kullanılamaz."

4.2.9 SİL Dağıtım Noktası (CRL Distribution Points) Eklentisi

Sertifikayla ilgili yayımlanacak SİL'e ulaşmak için gerekli bilgiyi içerir. Bu eklentinin yayımlanan nitelikli sertifikalarda bulunması **gerekmektedir**. [7]'de belirtildiği gibi, SİL ve sertifika yayımlayan 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

ESHS bilgi ve servislerine ulaşmak için kullanılır. Bu profile uygun olarak yayımlanan nitelikli sertifikalarda bu eklentinin bulunması **gerekmektedir.** Farklı erişim bilgilerinin olması halinde bu bilgiler liste halinde bu eklentide yer alır. Bu listede erişim metodu *id-ad-ocsp* olarak belirtilmiş en az bir tane erişim bilgisi **bulunmalıdır.** Ayrıca erişim metodu olarak *id-ad-caIssuers* olarak belirtilmiş en az bir tane ESHS sertifikasına erişim bilgisi **bulunmalıdır**. Böylece sertifikayı işleyen istemcilerin ESHS ile ilgili bilgilere erişimi kolaylaştırılmış olacaktır. Bu erişim bilgisinde LDAP ya da HTTP adresinden en az biri **bulunmalıdır.**

Kritik olarak **işaretlenmemelidir**.

5. Nitelikli Elektronik Sertifika Şartları ile Uyum

Aşağıdaki tablo, Elektronik İmza Kanunu [1] kapsamında hazırlanan Elektronik Mühre İlişkin Usul Ve Esaslar Hakkında Yönetmeliğin [2] 9'uncu maddesinde tanımlanan nitelikli elektronik mühür sertifikasında bulunması zorunlu bilgilerin bu profil kullanılarak nasıl karşılandığını göstermektedir.

Nitelikli Elektronik Mühür Sertifika Tanımı	Bu profile göre istenen şartın nasıl sağlanacağı
a) Otomatik işlemeye uygun bir biçimde, sertifikanın "nitelikli elektronik mühür sertifikası" olarak verildiğine 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) ESHS'nin kimlik bilgileri ve kurulduğu ülke adı	Bu dokümanda 4.1.3 Yayımcı (Issuer) Alanı ile.
c) Elektronik mühür sahibinin teşhis edilebileceği resmî kayıtlarda belirtilen unvanı ve MERSİS numarası veya DETSİS numarası veya Vergi Kimlik Numarası veya Ticaret Sicil Numarası veya başvuru sahibinin bağlı bulunduğu resmî sicile tescil edilen veya ilgili mevzuat ile belirlenen tekil kayıt numarası gibi kimlik bilgileri	Bu dokümanda 4.1.4 Özne (Subject) Alanı ile.
d) Elektronik mühür oluşturma verisine karşılık gelen mühür 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) ESHS için benzersiz olması gereken sertifika seri numarası	X.509 [7] ve RFC 5280 [6] 'de geçen sertifika seri numarası (Serial number) ile.
g) ESHS'nin elektronik imzası veya nitelikli elektronik mührü	X.509 [7] ve RFC 5280 [6] 'de tanımlandığı gibi sertifika imzalanır.
h) Elektronik imza veya nitelikli elektronik mührü destekleyen sertifika bilgisinin sunulduğu yeri	4.2.10 Hizmet Sağlayıcı Bilgi Erişimi Eklentisi ile.
Sertifikanın geçerlilik durumunu sorgulamak için kullanılabilecek hizmetlerin yeri	4.2.9 SİL Dağıtım Noktası Eklentisi ve 4.2.10 Hizmet Sağlayıcı Bilgi Erişimi Eklentisi ile.

6. Sertifika İptal Listesi (SİL) Profili

Her ESHS, verdiği sertifikalarla ilgili iptal bilgisini içeren sertifika iptal listesi **yayımlamalıdır**. ESHS'nin sertifika ve SİL yayımlayan 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 yayımlanan 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 [4] 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 Yayımlama Tarihi (This Update)

SİL'in yayımlandığı tarihi gösterir. RFC 5280 [6] 'de belirtildiği gibi 2049 yılına kadar *UTCTime* **kullanılmalı** ve zaman GMT(Zulu) olarak **kodlanmalıdır**. Detaylar için [6] 4.1.2.5 geçerlidir.

6.1.5 Sonraki Yayımlama Tarihi (Next Update)

Bir sonraki SİL'in yayımlanacağı en geç tarihi gösterir. ESHS'ler bu tarihten önce mutlaka yeni SİL yayımlamak **zorundadırlar**. Sonraki Yayımlama Tarihi, daha önce yayımlanmış tüm SİL'lerin sonraki yayımlama tarihlerinden sonra **olmalıdır**.

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

RFC 5280 [6] 'de belirtildiği gibi 2049 yılına kadar *UTCTime* **kullanılmalı** ve zaman GMT(Zulu) olarak **kodlanmalıdır**. Detaylar için [6] 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 yayımladığı SİL'ler için düzenli olarak **artmalıdır**. Böylece yayımlanan iki SİL'den hangisinin daha önce yayımlandığı kesin olarak bilinebilir.

Bu eklenti kritik olarak **işaretlenmemelidir**.

6.2.3 Hizmet Sağlayıcı Bilgi Erişimi (Authority Information Access) Eklentisi

Bu eklenti ESHS bilgi ve servislerine ulaşmak için **kullanılır**. Bu eklentinin yayımlanan SİL'lerde bulunması ***önerilir.*** Bu profile uyan SİL'lerde, erişim metodu olarak sadece id-ad-caIssuers **kullanılmalıdır.** Böylece SİL'i işleyen istemcilerin hizmet sağlayıcıyla ilgili bilgilere erişimi kolaylaştırılmış olacaktır.

Kritik olarak **işaretlenmemelidir**

6.3 SİL Eleman Eklentiler

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 6960 [8] 'da tanımlandığı gibi **olmalıdır**. Bu profile uyan ESHS'lerin OCSP sunucuları http üzerinden gelen isteklere cevap **verebilmelidir**. Bu profile uyan OCSP sunucuları sertifikaların gerçek zamanlı durumunu bilmek **zorundadır**.

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 Kabul edilebilir 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 [4] 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 ve bu elemanın uzunluğunu ifade eder.

8.1 Örnek Nitelikli Elektronik Sertifika Kodlaması

```
 0 1510: SEQUENCE {
 4 1387:   SEQUENCE {
 8    3:     [0] {
10    1:       INTEGER 2
     :       }
13    3:     INTEGER 485838
```

```
 18  10:    SEQUENCE {
 20   8:      OBJECT IDENTIFIER '1 2 840 10045 4 3 3'
      :    }
 30 115:    SEQUENCE {
 32  11:      SET {
 34   9:        SEQUENCE {
 36   3:          OBJECT IDENTIFIER countryName (2 5 4 6)
 41   2:          PrintableString 'TR'
      :        }
      :      }
 45  15:      SET {
 47  13:        SEQUENCE {
 49   3:          OBJECT IDENTIFIER localityName (2 5 4 7)
 54   6:          UTF8String 'Ankara'
      :        }
      :      }
 62  24:      SET {
 64  22:        SEQUENCE {
 66   3:          OBJECT IDENTIFIER organizationName (2 5 4 10)
 71  15:          UTF8String 'ESHS Resmi Adı'
      :        }
      :      }
 88  57:      SET {
 90  55:        SEQUENCE {
 92   3:          OBJECT IDENTIFIER commonName (2 5 4 3)
 97  48:          UTF8String
      :            'Test Elektronik Sertifika Hizmet Sağlayıcısı'
      :        }
      :      }
      :    }
147  30:    SEQUENCE {
149  13:      UTCTime 23/01/2023 18:56:45 GMT
164  13:      UTCTime 22/01/2026 18:56:45 GMT
      :    }
179 114:    SEQUENCE {
181  19:      SET {
183  17:        SEQUENCE {
185   3:          OBJECT IDENTIFIER organizationIdentifier (2 5 4 97)
190  10:          UTF8String '1234567890'
      :        }
      :      }
202  19:      SET {
204  17:        SEQUENCE {
206   3:          OBJECT IDENTIFIER serialNumber (2 5 4 5)
211  10:          PrintableString '1234567890'
      :        }
      :      }
223  11:      SET {
```

```
225   9:       SEQUENCE {
227   3:         OBJECT IDENTIFIER countryName (2 5 4 6)
232   2:         PrintableString 'TR'
      :       }
      :     }
236  57:     SET {
238  55:       SEQUENCE {
240   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
245  48:         UTF8String
      :           'BU ALANA TÜZEL KİŞİNİN TAM ADI YAZILACAKTIR'
      :       }
      :     }
      :   }
295 290:   SEQUENCE {
299  13:     SEQUENCE {
301   9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
312   0:       NULL
      :     }
314 271:     BIT STRING, encapsulates {
319 266:       SEQUENCE {
323 257:         INTEGER
      :           00 DD C4 04 A3 F0 AD 44 7E CE E3 1D CA 75 4E 46
      :           D6 96 80 76 76 D1 56 43 02 34 08 6B 3D 7B D3 24
      :           21 05 AA 6E 7C C5 3E 01 D2 51 6F FB A8 5A 0F 0D
      :           C1 1C D1 9C 47 A2 DA 86 B2 01 E8 F7 A4 AC 13 A4
      :           F2 E5 C0 47 5B 62 1D 0F F6 61 57 2F C7 C8 DC 23
      :           72 F4 5F 8C 25 D1 BC 01 49 3C 49 05 BA 22 FC FD
      :           B8 78 BB 4F 6B 4D 09 F2 87 D6 6F 83 27 FA B9 35
      :           A4 50 1F E5 17 E9 D0 B6 23 ED 20 69 53 22 C1 FB
      :                 [ Another 129 bytes skipped ]
584   3:         INTEGER 65537
      :       }
      :     }
      :   }
589 802:   [3] {
593 798:     SEQUENCE {
597  31:       SEQUENCE {
599   3:         OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
604  24:         OCTET STRING, encapsulates {
606  22:           SEQUENCE {
608  20:             [0]
      :               1F 1B 86 E1 EE 66 67 C0 DF 5C A5 1B 85 66 1C 09
      :               5E 1A FD 62
      :             }
      :           }
      :         }
630  29:       SEQUENCE {
632   3:         OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
```

```
637  22:         OCTET STRING, encapsulates {
639  20:           OCTET STRING
     :             99 DD 1D 5A 23 91 37 AB 3F A3 90 E7 CB FF F1 E5
     :             D6 75 E9 FD
     :           }
     :         }
661  14:       SEQUENCE {
663   3:         OBJECT IDENTIFIER keyUsage (2 5 29 15)
668   1:         BOOLEAN TRUE
671   4:         OCTET STRING, encapsulates {
673   2:           BIT STRING 6 unused bits
     :             '11'B
     :           }
     :         }
677 297:       SEQUENCE {
681   3:         OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
686 288:         OCTET STRING, encapsulates {
690 284:           SEQUENCE {
694 280:             SEQUENCE {
698  10:               OBJECT IDENTIFIER '2 16 792 3 0 999 1 1 2'
710 264:               SEQUENCE {
714  47:                 SEQUENCE {
716   8:                   OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
726  35:                   IA5String 'http://www.testsm.net.tr/TESTSM_SUE'
     :                 }
763 212:                 SEQUENCE {
766   8:                   OBJECT IDENTIFIER unotice (1 3 6 1 5 5 7 2 2)
776 199:                   SEQUENCE {
779 196:                     BMPString
     :                 'Bu sertifika, 5070 sayılı Elektronik İmza Kan'
     :                 'ununa göre nitelikli elektronik mühür sertifikasıdır.'
     :                   }
     :                 }
     :               }
     :             }
     :           }
     :         }
978   9:       SEQUENCE {
980   3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
985   2:         OCTET STRING, encapsulates {
987   0:           SEQUENCE {}
     :           }
     :         }
989  55:       SEQUENCE {
991   3:         OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
996  48:         OCTET STRING, encapsulates {
998  46:           SEQUENCE {
```

```
1000   44:           SEQUENCE {
1002   42:             [0] {
1004   40:               [0] {
1006   38:                 [6] 'http://www.testsm.net.tr/TESTSMSIL.crl'
       :               }
       :             }
       :           }
       :         }
       :       }
1046  103:     SEQUENCE {
1048    8:       OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
1058   91:       OCTET STRING, encapsulates {
1060   89:         SEQUENCE {
1062   47:           SEQUENCE {
1064    8:             OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1074   35:             [6] 'http://www.testsm.net.tr/TESTSM.crt'
       :           }
1111   38:           SEQUENCE {
1113    8:             OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
1123   26:             [6] 'http://ocsp.testsm.net.tr/'
       :           }
       :         }
       :       }
1151  241:     SEQUENCE {
1154    8:       OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
1164  228:       OCTET STRING, encapsulates {
1167  225:         SEQUENCE {
1170    8:           SEQUENCE {
1172    6:             OBJECT IDENTIFIER '0 4 0 1862 1 1'
       :           }
1180  121:           SEQUENCE {
1182   11:             OBJECT IDENTIFIER '2 16 792 1 61 0 1 5070 2 1'
1195  106:             UTF8String
       :               'Bu sertifika, 5070 sayılı Elektronik İmza Kan'
       :               'ununa göre nitelikli elektronik mühür sertifi'
       :               'kasıdır.'
       :             }
1303   90:           SEQUENCE {
1305   11:             OBJECT IDENTIFIER '2 16 792 1 61 0 1 5070 2 2'
1318   75:             UTF8String
       :               'Bu sertifika, güvenli elektronik imza oluşturm'
       :               'ak amacıyla kullanılamaz.'
       :           }
       :         }
       :       }
```

```
      :       }
      :     }
      :   }
1395   10:   SEQUENCE {
1397    8:     OBJECT IDENTIFIER '1 2 840 10045 4 3 3'
      :   }
1407  105:   BIT STRING, encapsulates {
1410  102:     SEQUENCE {
1412   49:       INTEGER
      :         00 81 3A 7A 4A 34 66 90 AE 0A 35 79 7D 29 87 41
      :         16 13 E8 8A 94 7D BD CB 3E 5A 64 D4 22 FE 59 96
      :         38 31 6C A3 73 C9 17 A7 7F 18 31 D7 16 3A 6A 1B
      :         DC
1463   49:       INTEGER
      :         00 A0 2A 71 26 A4 A6 98 B5 DA A0 89 6D 46 A8 A0
      :         0E 0A D6 0A 9F A3 FC 1E 10 45 AD 62 EC 80 A3 2C
      :         CD 66 9C 56 8E 38 D3 97 E2 21 6B 01 14 11 6A AC
      :         D9
      :     }
      :   }
      : }
```

8.2 Örnek SİL Kodlaması

```
  0  371: SEQUENCE {
  4  250:   SEQUENCE {
  7    1:     INTEGER 1
 10   10:     SEQUENCE {
 12    8:       OBJECT IDENTIFIER '1 2 840 10045 4 3 3'
      :     }
 22  115:     SEQUENCE {
 24   11:       SET {
 26    9:         SEQUENCE {
 28    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 33    2:           PrintableString 'TR'
      :         }
      :       }
 37   15:       SET {
 39   13:         SEQUENCE {
 41    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
 46    6:           UTF8String 'Ankara'
      :         }
      :       }
 54   24:       SET {
 56   22:         SEQUENCE {
 58    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 63   15:           UTF8String 'ESHS Resmi Adı'
      :         }
      :       }
```

```
 80  57:      SET {
 82  55:        SEQUENCE {
 84   3:          OBJECT IDENTIFIER commonName (2 5 4 3)
 89  48:          UTF8String
      :            'Test Elektronik Sertifika Hizmet Sağlayıcısı'
      :          }
      :        }
      :      }
139  13:    UTCTime 11/01/2023 12:45:00 GMT
154  13:    UTCTime 12/01/2023 12:45:00 GMT
169  37:    SEQUENCE {
171  35:      SEQUENCE {
173   4:        INTEGER 790337815
179  13:        UTCTime 11/01/2023 07:45:00 GMT
194  12:        SEQUENCE {
196  10:          SEQUENCE {
198   3:            OBJECT IDENTIFIER cRLReason (2 5 29 21)
203   3:            OCTET STRING, encapsulates {
205   1:              ENUMERATED 1
      :            }
      :          }
      :        }
      :      }
      :    }
208  47:    [0] {
210  45:      SEQUENCE {
212  31:        SEQUENCE {
214   3:          OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
219  24:          OCTET STRING, encapsulates {
221  22:            SEQUENCE {
223  20:              [0]
      :                1F 1B 86 E1 EE 66 67 C0 DF 5C A5 1B 85 66 1C 09
      :                5E 1A FD 62
      :              }
      :            }
      :          }
245  10:        SEQUENCE {
247   3:          OBJECT IDENTIFIER cRLNumber (2 5 29 20)
252   3:          OCTET STRING, encapsulates {
254   1:            INTEGER 45
      :            }
      :          }
      :        }
      :      }
      :    }
257  10:  SEQUENCE {
259   8:    OBJECT IDENTIFIER '1 2 840 10045 4 3 3'
      :    }
```

```
269  104:   BIT STRING, encapsulates {
272  101:     SEQUENCE {
274   48:       INTEGER
      :         34 BA 6B 89 B2 8D E7 45 70 9B 60 4E D6 37 14 93
      :         65 6F 0F 8F 71 81 AB A4 C5 1B 63 D8 2D 41 36 D8
      :         E8 EA 4E 89 C7 CB 38 46 8F D7 DC 67 56 4C CE CC
324   49:       INTEGER
      :         00 D1 BF F2 62 65 5A 2B D4 F4 B4 4E 78 85 90 AD
      :         07 A5 2A E0 47 49 29 05 A7 14 21 69 6B D1 65 89
      :         95 61 15 03 7A 51 BA 4F A4 D3 B6 A6 D9 71 52 54
      :         FE
      :       }
      :     }
      :   }
```

9. Kaynakça

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

[2] 14 Eylül 2022 tarih ve 31953 sayılı Resmi Gazete'de yayımlanan Elektronik Mühre İlişkin Usul Ve Esaslar Hakkında Yönetmelik

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

[4] 6 Ocak 2005 tarih ve 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

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

[6] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

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

[8] RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP