PADES TEST SUİT TASARLANMASI VE ADOBE READER'IN İMZA MEKANİZMALARININ TEST EDİLMESİ

ERHAN TURAN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

NİSAN 2015
ANKARA

Fen Bilimleri Enstitü onayı

Prof. Dr. Osman EROĞUL

Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

Doç. Dr. Erdoğan DOĞDU

Anabilim Dalı Başkanı

ERHAN TURAN tarafından hazırlanan PAdES TEST SUİT TASARLANMASI VE ADOBE READER'IN İMZA MEKANİZMASININ TEST EDİLMESİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Prof. Dr. Ali Aydın SELÇUK	Dr. Tamer ERGUN
Birinci Tez Danışmanı	İkinci Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Prof. Dr. Kemal BIÇAKCI

Üye : Prof. Dr. Ali Aydın SELÇUK

Üye : Doç. Dr. M. Fatih DEMİRCİ

Üye : Doç. Dr. Bülent TAVLI

Üye : Dr. Tamer ERGUN

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Erhan TURAN

Üniversitesi	**:**	**TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü	**:**	**Fen Bilimleri**
Anabilim Dalı	**:**	**Bilgisayar Mühendisliği**
Tez Danışmanları	**:**	**Prof. Dr. Kemal BIÇAKCI** **Dr. Tamer ERGUN**
Tez Türü ve Tarihi	**:**	**Yüksek Lisans – Nisan 2015**

Erhan TURAN

PADES TEST SUİT TASARLANMASI VE ADOBE READER'IN İMZA MEKANİZMALARININ TEST EDİLMESİ

ÖZET

Dünyada milyarlarca kullanıcısı olan Adobe Reader PDF Advanced Electronic Signature (PAdES) formatında imzalı dosyalar oluşturup doğrulayabilmektedir. Bu kadar yaygın olarak kullanılan bu uygulamanın imza oluşturma ve doğrulama kısımlarının geniş bir suit ile test edilmesi, uygulamanın güvenilirliğinin ve standartlara uygunluğunun detaylı olarak incelenmesi adına çok önemlidir. Yaptığımız bu çalışmada, içerisinde çok geniş bir PKI yapısını barındıran bir test suit oluşturduk ve Adobe Reader'ın (v11.0.10.32) imza oluşturma ve doğrulama kısımlarını test ettik.

Anahtar Kelimeler: Adobe, PAdES, Test, Adobe Reader, PDF İmza, Açık Anahtar Altyapısı.

University	:	**TOBB University of Economics and Technology**
Institute	:	**Institute of Natural and Applied Sciences**
Science Programme	:	**Computer Engineering**
Supervisors	:	**Prof. Ali Aydın Selçuk** **Tamer ERGUN, Phd.**
Degree Awarded and Date	:	**M.Sc. – April 2015**

Erhan TURAN

DESIGNING PADES TEST SUITE AND TESTING ADOBE READER SIGNATURE MECHANISMS

ABSTRACT

Adobe Reader, which has billions of users world wide is able to create and verify signatures conforming to Pdf Advanced Electronic Signatures (PAdES) standard. It is crucial to test such a common application's signature creation and verification mechanisms in terms of examining reliability and compliance with standards by a comprehensive test suite. In this work, we developed a test suite which includes extensive structures and we validate the signature creation and verification parts of Adobe Reader (v11.0.10.32).

Keywords: Adobe, PAdES, Test, Adobe Reader, PDF Signature, public key infrastructure.

TEŞEKKÜR

Bütün eğitim-öğretim hayatım boyunca daima bana destek veren babam Osman TURAN'a, annem Dilber TURAN'a, abim Erman TURAN'a, hayatımın her safhasında bana yol arkadaşı olan nişanlım Özge'ye, iş hayatım ve yüksek lisansım boyunca bana yol gösteren ve abilik yapan Dr. Tamer ERGUN'a, elektronik imza alanında bildiğim birçok şeyi bana öğretmiş olan Ferda TOPCAN'a, tez yazımında bana destek olan bütün arkadaşlarıma, yüksek lisansım boyunca bana bir çok şey katan TOBB ETÜ hocalarıma, araştırma bursumu sağlayan TOBB ETÜ'e ve çalışmalarımı sürdürdüğüm TÜBİTAK KamuSM ailesine teşekkür ederim. Tez çalışmalarım boyunca bana yol gösteren, her konuda örnek aldığım kişi olan danışman hocam Sayın Prof. Dr. Ali Aydın SELÇUK'a ayrıca teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLERİN LİSTESİ

ÇİZELGELERİN LİSTESİ

KISALTMALAR

Kısaltma	Açıklama
AAA	Açık Anahtar Altyapısı
BES	Basic Electronic Signature
BTK	Bilişim Teknolojileri Kurumu
CA	Certificate Authorithy
CAdES	CMS Advanced Electronic Signature
CMS	Cryptographic Message Syntax
DSS	Document Security Store
EBYS	Elektronik Belge Yönetim Sistemi
EPES	Explicit Policy Electronic Signatures
ESHS	Elektronik Sertifika Hizmet Sağlayıcı
ETSI	European Telecommunication Standards Institue
ISO	International Organization for Standardization
KSM	Kamu Sertifikasyon Merkezi
LT	Long Term
LTA	Long Term Archive
LTV	Long Term Validation
NES	Nitelikli Elektronik Sertifika
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAdES	PDF Advanced Electronic Signature
PDF	Portable Document Format
PDF-A	Portable Document Format Level A
PKI	Public key infrastructure
PFX	Personal Information Exchange
QC	Qualified Certificate
RFC	Request for Comments
SİL	Sertifika İptal Listesi
XAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language

SEMBOL LİSTESİ

Sembol	Açıklama
$>$	Büyüktür
$<$	Küçüktür
t	Zaman

1. GİRİŞ

Günümüzde internet kullanımının artması ve işlemlerin internet üzerinden çok daha hızlı gerçekleştirilebilmesiyle birlikte yazılım tabanlı uygulamaların kullanımı her alanda artmıştır. Elektronik Belge Yönetim Sistemleri (EBYS), Elektronik Ticaret Sistemleri, Elektronik Bankacılık ve Elektronik Devlet uygulamaları yükselişte olan uygulamalardandır. Bu uygulamalarla hemen her şeyin elektronik ortamdan kolay ve hızlı bir biçimde gerçekleştirilebiliyor olması sistemlerde kullanılan güvenliğin de çok güçlü olması zorunluluğunu doğurmuştur. Oluşabilecek sahtekârlıkların ve saldırıların önüne geçmek için basit kimlik doğrulama metotlarından daha güvenilir metotlara ihtiyaç duyulmuştur. Güvenli iletişimin yeterince sağlanmadığı sistemlerde milyonlarca dolarlık zararlara sebebiyet veren durumlar oluşabilmektedir. Açık anahtar altyapısı (Public key infrastructre) ile kişinin kimliğini doğrulayan, yaptığı işlemi reddetmesini önleyen, verideki bütünlüğü koruyan, verinin gizli bir şekilde iletilmesini sağlayabilen sistemler sağlanabilmektedir. Açık anahtar altyapısının (AAA) uygulama alanları oldukça geniştir. En çok kullanıldığı alanlardan biri de elektronik imzadır.

Kişinin imzaladığı mesajın bütünlüğünün korunması imzaladığı verinin yasalar önünde geçerli olarak sayılması, kişinin güvenilir bir şekilde kimlik doğrulama işleminin yapılması ve kişinin ileride bu veriyi kendisinin imzaladığını reddedememesi için elektronik imza kullanılmaktadır. Elektronik imza, açık anahtar altyapısı üzerine kurulmuştur. Açık anahtar kriptografide olduğu gibi, elektronik imzada da; açık anahtar (public key) ve özel anahtar (private key) olmak üzere kişide bir anahtar çifti bulunmaktadır. Bu anahtar çiftlerinden açık anahtar herkesle paylaşılırken özel anahtar kişinin kendisinde saklanmaktadır ve kimse ile paylaşılmamaktadır. Özel anahtar kullanılarak kişi imza işlemini gerçekleştirir, açık anahtarıyla da imza doğrulama işlemi yapılır. Açık anahtarın alıcıya güvenli bir şekilde iletilmesi ve imzacının kimlik doğrulama işleminin güvenilir bir şekilde yapılması gerekmektedir. Açık anahtarın sahibinin kimliğini ispatlayan, imzacının ilgili açık anahtara sahip olduğunu güvence altına alan veri elektronik sertifikadır. İçerisinde kişinin kimlik bilgileri ve açık anahtar bilgileri bulunan elektronik sertifikalar; sertifika otoritelerinin (certificate authority) kendi anahtarları ile

imzalanırlar. Son kullanıcıların elektronik sertifikalarından başlayarak, sertifika otoritelerinin kök sertifikalarına kadar elektronik imza ile sağlanan bir güven zinciri bulunmaktadır. Bu güven zinciri kendi içerisinde bir Public Key Infrastructure (PKI) ağacı ihtiva eder. Uygulamalar mertebesinde elektronik imzanın güvenilir bir şekilde oluşturulduğundan ve doğrulandığından emin olmak adına PKI ağacındaki oluşabilecek açıklıkların kapsamlı olarak incelenmesi gerekmektedir. Test Suit Çalışması adı altında yapılan çalışmada bir PKI modeli kurarak bu açıklıkların neredeyse tümünü yakalaması amaçlanmıştır. [1]

Belirtilen [1] PKI modelini esas alarak yeni bir suit oluşturduk ve PDF Advanced Electronic Signature standartına [2] uygun imza oluşturan Adobe Reader'a; uyguladık. Adobe Reader'a imza oluşturma ve imza doğrulama testlerini uygulama amacımız, Adobe Reader'ın ilgili hataları doğru bir şekilde yakalayıp yakalamadığını tespit etmektir. Bu tez sonucunda karşılaşılan olumlu ve olumsuz sonuçlar ışığında, Adobe Reader'ın imza oluşturma ve imza doğrulama kısımlarının standartlara tam uygun hale gelmesini ve tespit edilen hatalı kısımların düzeltilmesini hedefliyoruz.

1.1 Benzer Çalışmalar

1.1.1 Tasarım

Test Suit Çalışması [1] ile bir PKI modeli kurulmuştur. Bu model ile son kullanıcı sertifikalarında, alt kök sertifikalarında, kök sertifikalarında, zaman damgasında, Online Certificate Statues Protocol (OCSP) de ve Sertifika İptal Listelerinde (SİL) [3] oluşabilecek bütün hatalar kurgulanmış sertifika yolu boyunca tek bir hata olacak şekilde senaryolar tanımlanmış ve gerçekleştirilmiştir. Bu çalışmadan yararlanarak çalışmamız kapsamında yeni senaryolar eklenerek bütün son kullanıcı sertifikaları, alt kök sertifikaları, kök sertifikaları, ocsp sunucuları, zaman damgası sunucuları, SİL'ler tarafımızdan oluşturulmuştur. Her bir durumda sadece bir tane hatayı içerecek şekilde kurgulanmış sertifika yapıları oluşturulmuştur. Bu yapılar PAdES için oluşturacağımız imza oluşturma testlerine temel olmuştur. CMS Advanced Electronic Signature (CAdES) [4] ve XML Advanced Electronic Signature (XAdES) [5] için de PAdES için de, imza oluşturmak için kullanılacak PKI yapısı benzer bir PKI yapısıdır. Aynı yapı içerisinde PKI ihtiva eden her yere uygulanabilir. Fakat imza doğrulama testleri

için her imza formatına özel imzalı dosyaların oluşturulması gerekmektedir.

1.1.2 İmza Oluşturma

Benzer çalışmalardan, NIST'in (National Institute of Standards and Technology) [6] imza oluşturma testleri yapmak üzere oluşturduğu bir set bulumaktadır. Fakat bu çalışmada OCSP üzerine hiç bir test yapılmamıştır. OCSP sertifikalarında ve OCSP cevaplarında oluşabilecek hatalı senaryolar hiç ele alınmamıştır. Ayrıca NIST sadece alt kök tarafından oluşturulmuş SİL'lerle ilgili senaryoları incelemiştir. Biz ise kök tarafından yayınlanmış SİL'leri de inceledik. Dolayısıyla imza oluşturma kısmında NIST'in suitinden daha farklı bir suit hazırlayarak sertifika zincir doğrulama senaryolarını olabildiğince ele aldık.

1.1.3 İmza Doğrulama

İmza doğrulama adına yapılan çalışmalar arasında ETSI (European Telecommunication Standards Institue) plug testleri [7] bulunmaktadır. Fakat ETSI Plug Test'lerinde ağırlıklı olarak imza formatlarının doğruluğu üzerine testler yapılmaktadır. Bizim çalışmamızda ise imza formatlarının doğruluğu adına çok daha fazla senaryo incelenmekte ve ayrıca sertifika doğrulama senaryoları da daha geniş bir biçimde ele alınmaktadır.

2. TANIMLAMALAR

Bu bölümde; Test Suit kapsamında yapılan çalışmalarımızda kurduğumuz PKI modelinde kullandığımız yapıların tanımlamaları yapılacaktır.

Kriptografik imzalama sırasında öncelikle bir özet (hash) [8–12] fonksiyonuna ihtiyaç duyulmaktadır. Asimetrik anahtar kriptografi kullanılarak mesajın tamamının bir özet fonksiyonu kullanılmadan imzalanması halinde verinin boyutuyla doğru orantılı olarak imzalama işlemi çok uzun sürebilmektedir. Bu sebeple imzalama öncesinde bir özet [13] fonksiyonu kullanılır. Özet fonksiyonu sonucunda sabit uzunlukta özet değeri (message digest) ortaya çıkar ve sadece bu veri imzalanır. Özet fonksiyonunun sağladığı çarpışma (collision resistance), preimaj (preimage resistance) ve tek yönlülük (one way) özellikleri sayesinde de verinin sanki tamamı imzalanmışçasına elektronik imzadaki bütünlük ilkesi korunurken; verinin tamamının imzalanmasında yaşanabilecek yavaşlık sorunu da ortadan kaldırılmış olunur [12]. Her ne kadar imzalama işlemi; bir verinin özet değerinin özel anahtar ile encrypt edilmesi, doğrulama işlemi de; imzalama işlemi sonucunda oluşan mesajın decrypt edilerek orjinal mesajdaki hash ile karşılaştırılması şeklinde ifade edilse de, bu işlemler gerçek uygulama alanında bu kadar basit değildir. Sadece mesajın imzalanması güvenli bir yapı için çok yetersiz kalmaktadır. Güvenlik; bir zincir olarak düşünülürse, "zincirin sağlamlığını en zayıf halka belirler." ilkesi elektronik imza için de geçerlidir. Bu sebeple imzalı yapının doğrulanabilmesi için gerekli olan bütün yapıların imzalı olması gerekmektedir. Elektronik imzada kullanılan diğer imzalı yapılar: Sertifikalar, iptal bilgileri ve zaman damgalarıdır.

2.1 Sertifika

İmzalanan dokümanla birlikte imzacı, imzaladığı verinin alıcı tarafından decrypt edilerek doğrulanabilmesi adına; açık anahtarını da imzası ile birlikte, alıcıya güvenli bir şekilde iletmelidir. Aksi takdirde araya giren bir saldırgan mesajı değiştirerek kendi özel anahtarıyla, değiştirdiği mesajı imzalayıp kendi açık

anahtarını imzacının açık anahtarıymuş gibi iletebilir. [14] Bu tip saldırıların oluşmasını engellemek adına açık anahtarın kime ait olduğunu ispatlayan bir yapıya ihtiyaç duyulmaktadır. Bu yapı yine kendi içerisinde imzalı olan X509 elektronik sertifika [3, 15] ile sağlanmaktadır.

Elektronik sertifika kişinin açık anahtarını, kişisel bilgilerini ve sertifikanın geçerlilik kontrolü için gerekli olan bilgileri içeren yapıdır. Son kullanıcıların elektronik sertifikaları güvenilir bir sertifika otoritesinin Alt Kökü (SubCA) tarafından imzalanmaktadır.

Alt kök yapısında da yine son kullanıcı sertifikasında olduğu gibi özel anahtar ve açık anahtar olmak üzere bir anahtar çifti bulunmaktadır. Alt kökün de oluşturduğu imzaların doğrulanabilmesi için imzaladığı dokümanla birlikte doğrulama yapan tarafa güvenli bir şekilde açık anahtarını iletmesi gerekmektedir. Bu güvenli yol yine alt kökün açık anahtarının, alt kökün kimlik bilgilerinin ve geçerlilik kontrolü yapılması için gerekli bilgilerinin bulunduğu imzalı bir yapı olan elektronik sertifika ile sağlanmaktadır. Alt kökün sertifikası da kök adı verilen yapının private keyi tarafından imzalanır.

Kök yapısının açık anahtarı, kimlik bilgileri ve geçerlilik süresi yine elektronik sertifikasında bulunur. Kökün elektronik sertifikası ise yine kökün kendi özel anahtarı tarafından imzalanır. Yani kök kendi kendini imzalamış (self signed) bir yapıdadır. Böylelikle son kullanıcı sertifikasından başlayarak kök sertifikasına kadar bir güven zinciri kurulmuş olunur. Bu zincirin tamamlanabilmesi için sonunda bu güven zincirinin en tepesinde olan sertifika makamına kayıtsız şartsız güvenilmesi gerekir. Bu sertifika makamları dünya üzerinde güvenilir olarak kabul edilen sertifika makamlarıdır. Bu makamların güvenilir olarak kabul edilen sertifikaları da kök sertifikalardır.

Nitelikli Sertifika (Qualified Certificate) imzanın yasalar önünde delil sayılabilmesi için gerekli alanları içeren bir sertifikadır. [16–19] İmzalı evrakların herhangi bir itilaf durumunda delil olarak kullanılabilmesi için de imza paketinin ve imzada kullanılan yapıların standartlarda belirtilen şekilde oluşturulması gerekmektedir. Standartlara uygun oluşurulan imzalı yapıda ayrıca imzalama için kullanılan sertifikanın da nitelikli bir elektronik sertifika olması gerekmektedir. [20–23] Bu ilkelerden birinin dahi sağlanmaması ve/veya imzanın standartlara uygun üretilmemesi durumda imza yasalar önünde geçersiz sayılıcaktır.

İmzanın ve sertifikaların doğrulanması için kullanılan yine kendi içerisinde bir PKI hiyerarşisi içeren yapılar bulunmaktadır. Sertifika doğrulama işlemi yapılırken sertifikanın geçerlilik tarihi ile ilgili kontroller sertifikanın içerisinde yazan geçerlilik başlangıcı ve geçerlilik sonu kısımlarından bakılarak çevrim dışı (offline) olarak kontrol edilebilir. Fakat sertifikanın iptal durumu her an değişebilecek bir durumdur. İmza oluşturma ve imza doğrulama anında sertifikanın iptal olup olmadığı ile ilgili bir sorgulama yapılması gerekmektedir. Sertifikanın iptal işlemlerini yapan ve sertifikanın iptal bilgilerinin yayınlanmasından sorumlu makam Elektronik Sertifika Hizmet Sağlayıcılarıdır (ESHS) [24]. Sertifikanın iptal bilgilerini ESHS'ler Sertifika iptal listesi (SİL) veya Online Certificate Status Protocol (OCSP) ile sağlayabilirler.

2.2 Sertifika İptal Bilgileri

Sertifika ile ilgili iptal kontrolleri sertifika iptal bilgileri aracılığı ile yapılır. Sertifika iptal bilgileri de bütün yapılar gibi imzalı yapıdadır. Sertifika iptal bilgisi için kullanılan SİL ve OCSP yapıları güvenilir makamlar tarafından imzalanırlar. İptal bilgisi kullanılırken; iptal bilgisi üzerinde bulunan imzalar da, aynı dokümanın üzerindeki imzalar gibi doğrulanarak kabul edilirler.

Sertifika İptal Listesi Request for Comments'de (RFC) [3] tanımlanmış içerisinde iptal olmuş sertifikaların seri numaralarını barındıran imzalı bir yapıdır. SİL'ler ESHS'ler tarafından imzalanarak yayınlanmaktadır. İmzalı olarak yayınlanmasının amacı bütünlüğü korumak, ilgili saldırganın iptal olmuş bir sertifkayı SİL'den çıkararak iptal olmamış gibi göstermesini önlemektir. İlgili SİL iptal kontrolü yapılan sertifikanın yayıncısı (issuer) tarafından yapılmalıdır. Yani SİL sertifikanın issuer'u tarafından imzalanmaktadır.

SİL elektronik imza oluşturulması esnasında bir çok yerde kullanılmaktadır. SİL'in bazı avantajlarının olmasının yanında dez avantajları da bulunmaktadır. SİL'ler belli periyotlarda yayınlanır. SİL'in ömrünü içerisinde bulunan this update ve next update alanları belirler.

This Update alanı ile SİL'in ne zaman yayınlandığını, next update alanıyla da de SİL'in ne zamana kadar geçerli bir biçimde kullanılabileceği, yani yeni SİL'in ne zaman yayınlanacağı ifade edilir.

Elektronik imza ile bir dokümanın imzalanması saniyeler içerisinde gerçekleştirilebilir. Fakat unutulmamalıdır ki elektronik imzaya sahip olan kişi imza atma gücüne de sahip olur. Eğer kişinin elektronik imzası kötü amaçlı bir kişinin kontrolüne geçer ve isteği dışında bir doküman imzalanırsa; kişi sertifikasını iptal ettirse dahi iptal durumu SİL'e yansımamış olabilir. Sertifika otoritelerinin SİL'leri yayınlama süreleri farklılık göstermektedir. Bu periyot göz önünde bulundurulduğunda, SİL kullanılarak yapılan bir doğrulama işleminde iptal olmuş sertifika geçerli olarak değerlendirilebilir. Bu da iptal olmuş bir sertifika ile imzalama işlemi yapan saldırganın imza sahibine zarar vermesine yol çar.

Grace Period bu tip durumları ortadan kaldırmak adına geliştirilmiştir. Hali hazırda yayında olan SİL'in hemen kullanılmasını önlemek ve yayında olan SİL ile işlem yapmak yerine doğrulama için yeni çıkacak SİL'in beklenmesini sağlamak adına kullanılır. İmzalama yapıldığı anda yayında olan SİL yerine imzalama zamanından sonra grace period kadar beklenir ve yayınlanan yeni SİL'ler kullanılır. Yani kullanılabilecek SİL'ler için "this update $>$ imza zamanı $+$ grace period" olmalıdır.

Sertifikalar sadece iptal edilmezler. Sertifikalar askıya da alınabilirler. Benzer bir tehlike askıya alınma durumu için de geçerlidir. Sertifikalar sadece belli zamanlar arasında kullanım dışına alınıp, sonrasında tekrardan askıdan indirilebilirler. Bu sebeple imzalanan dosya doğrulanırken imza zamanındaki durumuna göre kontrol edilmelidir. İmza zamanından çok çok sonraki SİL ile kontrol işlemi yapıldığında, imza zamanında askıda olan bir sertifika ile oluşturulmuş imza geçersiz sayılması gerekirken geçerli sayılabilir.

Last Revocation Period imza zamanından maksimum t kadar süre sonraki SİL'in kullanmasını sağlayan bir güvenlik parametresidir. İmza zamanına göre çok ileri tarihteki SİL'lerin kullanılmasını önler. İmza yapılan dönemde askıda olan sertifikalara, askıdan indirildikten sonraki bir SİL kullanılarak geçerli cevabının dönülmesinin Last Revocation Period ile önüne geçilir.

Bir imzalı dosyanın doğrulanması için gerekli olan SİL'in geçerli sayılabilmesi için idealde grace period kadar beklenilmesi gerektiğini söylemiştik. Fakat hızın çok önemli olduğu günümüzde bekleme gerektiren sistemler pekiyi karşılanmamaktadır. Bu sebeple SİL kullanımında oluşan, grace period kadar sonraki ve last revocation'dan önceki SİL'lerin kullanılma zorunlulukları, operasyonel olarak sıkıntılar doğurmaktadır. Bu da SİL kullanımı için büyük bir dezavantaj

oluşturmaktadır. Ayrıca kullanıcıların sertifikaları iptal oldukça, SİL dosyasının günden güne boyutu artmaktadır. Bu da imza doğrulama esnasında zamanla her seferinde daha büyük boyutta bir SİL'in indirilmesine sebep vermektedir.

CA sertifikalarının iptal olma ihtimalleri çok düşük olduğu için ESHS kontrolünde olan alt kök sertifikası, kök sertifikası, zaman damgası ve OCSP sertifikalarının kontrolünün SİL'den yapılması bir sorun ihtiva etmemektedir. Ayrıca iptal olma ihtimallerinin çok düşük olması sebebi ile genellikle liste boş olmakta ve boyutu da artmamaktadır.

SİL'in avantajlarından bahsetmek gerekirse tek bir SİL ile aynı alt kök tarafından yayınlanmış bütün sertifikalar için iptal kontrolü yapılabilir. Bu da uygun SİL indirildikten sonra aynı alt kök tarafından sertifikalandırılmış bütün kullanıcıların aynı SİL'den yararlanabilmesini sağlamaktadır. Diğer avantajıysa SİL'in bir sefer kaydedilerek, online olunmaya gerek kalmaksızın tekrar tekrar kullanılabilemesidir. Networksel sorunların yaşandığı sistemlerde bir B planı olarak SİL'in kaydedilerek kullanılması operasyonel sürecin aksamasını önleyecektir.

Online Certificate Status Protocol sertifika iptal kontrollerinin yapılması için geliştirilmiş olan bir protokoldür RFC de tanımlanmıştır. [25] OCSP'de, SİL'de olduğu gibi bir liste indirilmez. İptal kontrolü yapmak için standartlara uygun bir OCSP isteği (request) üretilir. Bu OCSP isteği tek bir sertifikanın durumunu sorgulamak için üretilir. OCSP isteği sonrasında sertifikanın geçerlilik durumunu belirten OCSP cevabı standartta belirtildiği üzere sorgu yapılan sertifikanın yayıncısı veya yayıncısı tarafından delege edilmiş bir OCSP sertifikası tarafından imzalanır ve iptal sonucu dönülür. OCSP sunucusu anlık olarak yanıt döndüğü için sertifikanın güncel durumu CA tarafından bildirilmiş olunur. OCSP kullanıldığında, SİL kullanılırken beklenen grace period kadar beklenilmemiş olur.

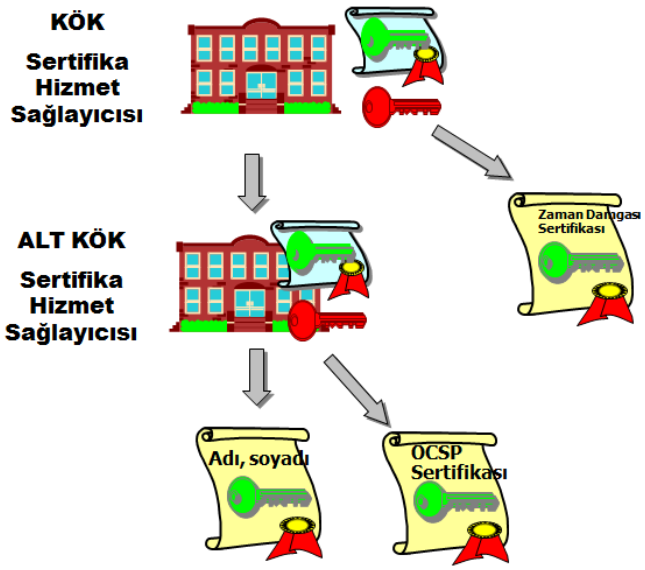
CertID alanı, OCSP isteği ve OCSP cevabı yapılarında bulunan bir alandır. Sorgulama yapılan ve cevap dönülen sertifikanın seri numarasını içerir. Ayrıca sertifikanın yayıncısının adının (issuer name alanının) ve yayıncısının açık anahtarınının (issuser key name) hashleri içerir. Ayrıca hash alırken kullanılan algoritmanın tanımlayıcısı da bir diğer alan olarak bulunmaktadır. Sequence yapısını bulabilirsiniz. [25] Sertifika ile ilgili request gönderilirken ve cevap alınırken hangi sertifika ile ilgili işlem yapıldığı CertID alanı ile kontrol edilir. Bu alanda "issuerNameHash" ve "issuerKeyHash" alanlarının bulunmasının sebebi, aynı seri numarasına sahip bir son kullanıcı sertifikası için farklı bir yayıncıdan

alınan response'un sorgu yapılan response yerine konulmasını önlemektir.

OCSP'nin dezavantajı sürekli online olunması gerekliliğidir. Ayrıca SİL'de olduğu gibi online olunamadığı durumlarda kaydedilen eski cevaplar kullanılamaz. OCSP cevabının, sorgulanan sertifikanın yayıncısı tarafından ya da yayıncının delege ettiği bir OCSP sunucusu tarafından imzalanabileceğinden bahsetmiştik. Her sertifika gibi OCSP sertifikasının da iptal olma ihtimali bulunmaktadır. Bu sebeple OCSP sertifikasının da iptal kontrolünün yapılması istenebilir.

OCSP Revocation NoCheck alanı OCSP sertifikası içerisinde bulunabilen bir alandır. Bu alan OCSP sertifikaların içerisinde bulunmuyor ise OCSP sertifikaları için de iptal kontrolü yapılmalıdır. OCSP sertifikasının iptal kontrolü tekrar bir OCSP sorgusu ile yapılamaz. CA'ler tarafından, OCSP'nin sorgusu tekrar OCSP'den yapılacak şekilde bir yapı kurulursa, sorun yaşayacak ve sonsuz bir sorgu döngüsüne girilmiş olunacaktır. OCSP sertifikasının iptal kontrolü sadece SİL ile yapılabilir. Herhangi bir sertifikanın SİL'ini yayınlayan ve imzalayan, makamın kendi yayıncısıdır. Şekil 2.1 örnek bir CA hiyerarşisi görmekteyiz. OCSP ile Nitelikli elektronik sertifikayı (NES) yayınlayan aynı makamlar olduğu için OCSP için yapılan iptal kontrolü esnasında indirilen SİL aynı zamanda iptal sorgulaması yapılan son kullanıcı sertifika için de geçerli bir SİL'dir. Sorgu mekanizması sırasında son kullanıcı sertifikası için SİL yerine, OCSP ile sorgu yapıldığı durumlarda, OCSP'nin iptal durumuna bakmak için yine ilk etapta tercih edilmeyen SİL'in indirildiği görülmektedir. O halde ilk etapta son kullanıcı sertifikasının iptal kontrolü yapılırken; OCSP'i tercih etmek yerine sertifikanın iptali için SİL kullanmanın adımları daha kısaltığını düşünülebilinir. Fakat SİL'de anlatılan dezavantajlara dönülecek olursa, iptalin SİL'e hemen yansımadığı durumların oluşabildiği hatırlanacaktır. Son kullanıcı için OCSP'den sorgulama yapıldığı durumda, geçerlilik durumu ne ise ona yönelik güncel cevap alınır. OCSP sertifikasınınsa iptal olma ihtimali neredeyse hiç bulunmamaktadır. Bu sebeple çok da güncel olmayan SİL'in kullanılmasında bir sakınca bulunmamaktadır. OCSP için yayınlanan SİL ile son kullanıcı için yayınlanan SİL'in aynı SİL olması ve bu SİL'in, OCSP'nin iptal olma gibi düşük bir ihtimal yüzünden her seferinde indirilmememesi adına OCSP revocation no check alanı isteğe bağlı olarak OCSP sertifikalarına konulmaktadır. Bu sayede OCSP için SİL'in indirilmesi adımının önüne geçilmiştir.

Gerek OCSP için gerekse SİL için yaptığımız tanımlamalarda imza atılma zamanın öneminden bahsettik. İmza zamanı; imzalanan dosyanın doğrulanabilmesi



Şekil 2.1: Örnek Sertifika Otoritesi Hiyerarşisi

adına çok önemlidir.

Zaman Damgası herhangi bir verinin damga alınan tarihten önce var olduğunu ispatlar. RFC [26]'de detaylı olarak tanımlanmış olan zaman damgası; kendi içerisinde imzalı bir yapı ihtiva eder. Kişi zaman damgası istediği verinin hash'ini alır. Sonrasında içerisine bu hash'i de koyduğu zaman damgası isteğini (timestamp request) oluşturur ve zaman damgası sunucusuna bu isteği iletir. Zaman damgası sunucusu kendisine gelen özeti ve kendi güvenilir saatinden aldığı zamanı birleştirerek zaman damgası cevabını oluşturur. Bu cevap yapısını kendi özel anahtarı ile imzalar. Zaman damgası da ESHS'lerin kökleri tarafından imzalanmış bir sertifikaya sahiptirler ve Şekil 2.1 görüldüğü üzere hiyerarşide yerlerini alt köklerle aynı seviyede alırlar.

Zaman Damgası herhangi bir veri için alınabildiği gibi elektronik imza yapısı için de alınmaktadır. Elektronik imza standartlarında [4, 5, 27, 28] zaman damgasının, imzanın hangi kısımlarına alındığı tanımlanmıştır. Zaman damgası imza saatini güvence altına almaktadır. İmzalı bir yapı olduğu için kötü amaçlı kişiler tarafından zaman damgası cevabı içerisindeki saatle oynanarak imza zamanı değiştirilemez. Değiştirilmesi halinde elektronik imzanın sağladığı bütünlük ilkesi gereğince, zaman damgasında bulunan imza yapısı bozulmuş olur ve saati ile değiştirilmiş olan zaman damgası cevabının (token) imzası doğrulanamaz.

Zaman damgasının herhangi bir veri için alınabileceği gibi, elektronik imzalı yapı için de alınabileceğinden bahsetmiştik. Zaman damgasının PAdES standatında bahsedilen çeşitlerini görelim.

Document Time Stamp (Doküman zaman damgası) ETSI tarafından yayınlanan PAdES standartında [2, 28] belirtildiği üzere var olan dokümanı ve iptal bilgilerini koruma maksadıyla kullanılmaktadır. İmzanın zaman damgası alınan tarihten önce varolduğunu ispatlamak amacıyla kullanılır.

Content Time Stamp (İçerik zaman damgası) ETSI tarafından yayınlanan CAdES standartında tam olarak tanımlanmış; PAdES standartında da aynen kullanılmıştır. İmzanın içerisinde bulunan içeriğe (content) alınan bir zaman damgası çeşitidir. İlgili content'in imzalanan zamandan daha öncesinde de var olduğunu ispatlar.

Archieve Time Stamp (Arşiv Zaman Damgası) ETSI tarafından yayınlanan CAdES standartında signer info ve bütün signed data alanlarına alındığı tanımlanmıştır. PAdES standartına göre ise doküman zaman damgasının iptal bilgilerin de imzalı pakete dâhil edilmesinden sonra bütün yapıya tekrar zaman damgası alınması ile arşiv zaman damgası oluşmuş olur. İmzalanan dokumanla birlikte ilk alınan zaman damgası ve iptal bilgilerini de koruma altına almaktadır. İlk zaman damgasında kullanılan algoritmaların zayıflaması geçersiz olarak kabul edilmesi ya da doküman zaman damgası alırken imzalama işlemini yapan zaman damgasının sertifikasının süresinin dolması arşiv zaman damgası alınmasını gerektiren sebeplerdir.

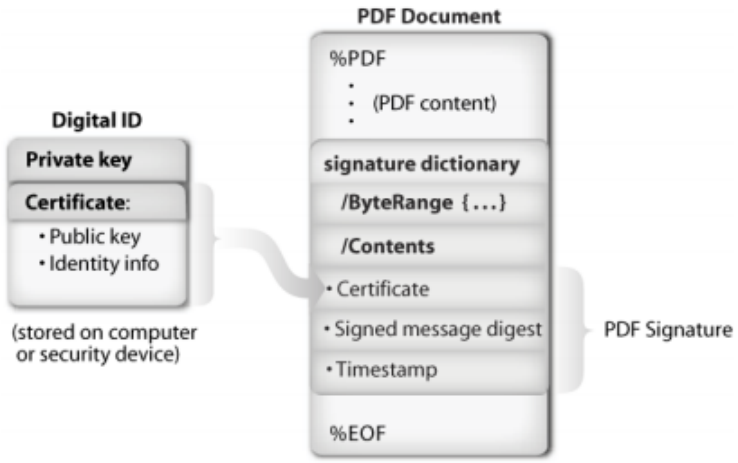
2.3 PAdES İmza

PDF (Portable Document Format) dokümanların ortamdan bağımsız olarak güvenilir bir şekilde görüntülenebilmesine ve oluşturulabilmesine olanak sağlayan bir formattır. [29] ISO (International Organization for Standardization) 32000-1'de PDF'lerin imzacının kimliğinin doğrulanması ve dokümanın bütünlüğünün korunması adına Cryptographic Message Syntax (CMS) imza [30] ile birlikte, CAdES standartında [4] ve XAdES imza ile XAdES standartında [5,31] belirtilen bazı gelişmiş imza özellikleri dâhil edilmeden kullanılabileceği belirtilmiştir. CAdES imzada dokümanın hash'i ve signed attributelar birleştirilerek topluca bir hash alınır ve bu hash imzalanır. PAdES'de ise imza dokumanın içerisine

gömüleceği için PDF signature kısmı hariç, geri kalan bütün alanlar imzalanır. Bu imzalama işlemi CAdES imzada tanımlandığı üzere yapılır ve sonrasında oluşan CAdES yapıdaki imza PDF in içerisinde ayrılmış olan alana gömülür.

İmza oluşturulması sırasında istenildiği takdirde imzayı doğrulayacak kişinin görmesi adına, görünecek imza figürü de eklenebilir. [32]

İmza Sözlüğü (Signature Dictionary) PDF yapısı içerisinde ayrılmış bir alandır. Bu alana imzalama sonucunda oluşmuş olan imza, doküman zaman damgası, iptal verileri, arşiv zaman damgası Şekil 2.2 'de görüldüğü üzere konmaktadır. [33]



Şekil 2.2: PAdES İmza Sözlüğü (Signature Dictionary)

PDF-A ISO standartlarında [34] tanımlanmış, bir PDF dokümanın uzun yıllarca güvenilir olarak saklanmasını sağlamak amacıyla oluşturulmuş bir PDF formatıdır. PDF-A; PDF içerisine verinin dinamik olarak değişmesine sebep olabilecek (java script gibi) script'lerin yazılmasını önlemekte ve bu tip dinamik oluşumları sınırlamaktadır. Elektronik imza ile imzalanacak içeriğin görüntüleyiciden görüntüleyiciye fark göstermesi ve içerisinde dinamik veriler içermesi bütünlük ilkesini tehlikeye sokacak bir durum ortaya çıkarmaktadır. Bu sebeple PAdES standartında, PDF formatındaki dokumanların imzalanmadan önce PDF-A ya çevrilmesi önerilmektedir. [33]

Elektronik imzanın oluşturulma zamanını belirlemek için zaman damgasının kullanıldığını, iptal kontrolleri için iptal bilgilerinin kullanıldığı ve ilk zaman damgası ve iptal bilgilerini kapsayan arşiv zaman damgasının kullanıldığından

bahsetmiştik. İşte imza paketine bu verilerin dâhil edilme durumlarına göre imza tipleri oluşmaktadır. PAdES ile ilgili imza tiplerine detaylı olarak buradan erişebilirsiniz. [2] [28]

2.3.1 PAdES İmza Tipleri

PAdES-Basic Electronic Signature (BES) Profili (B-Type) en temel imza yapısıdır. PAdES BES'de; PDF içerisinde bulunan Signature Dictionary içerisine CMS [4] olarak oluşturulan imza yerleştirilir. CMS imza oluşturulurken zorunlu signed attributelar imzalanır. Zorunlu signed attributelar'a ek olarak da tercihe göre de optional signed attribute'lar konabilir. [2, 4]

PAdES-Explicit Policy-based Electronic Signature (EPES) Profili'nin PAdES BES profilinden farkı; imzalama aşamasında imzalama ve imza doğrulama aşamalarında nasıl bir politika kullanılacağını belirten signature policy identifier'ın da imzaya dâhil edilmesidir. BES imza ile aynı seviyede bir imzadır. [2, 4, 35–37]

PAdES Long Term Validation (LTV) Profili imzanın uzun dönemli doğrulanabilmesi adına; PDF'deki Signature Dictionary alanına doküman zaman damgasının alınarak eklenmesi ve sertifikayı ve sertifika doğrulama sırasında kullanılan bütün ağacı doğrulayabilmek adına; iptal bilgilerinin ve kullanılan sertifikaların (alt kök sertifikası, kök sertifikası, OCSP sertifikası) eklenmesi ile oluşmuş, gelişmiş paket yapısıdır. İmzanın doğrulanması için gerekli olan bütün veriler Document Security Store (DSS) alanı içerisine konulmuş olur. LT-Type imzalı tipi ve LTA-Type imza tipi LTV imza yapısındadır. İçerisinde iptal bilgileri ve sertifika bilgileri bulunan imza tipi LT-Type imzadır. LT-Type imzalı yapıya, arşiv zaman damgası alınmasıyla birlikte LTA-Type imza oluşturulur. [2, 28]

3. ADOBE READER TEST ÇALIŞMASI

Elektronik imza temelde bütünlük, kimlik doğrulama ve inkâr edememezlik olmak üzere üç tip güvenlik bileşenine sahiptir. Bu güvenlik bileşenleri, inşa edilen PKI mimarisiyle güvence altına alınmaya çalışılsa da güvenliğin seviyesini belirleyen, uygulamaların sahip olduğu güvenlik seviyesidir. Elektronik imza uygulamalarının güvenliği ancak kendi çalışma mekanizmasının ne kadar düzgün bir şekilde uygulamaya dönüştürüldüğü ile ölçülebilir.

Türkiye'de 5070 sayılı kanunla [16] elektronik imza ıslak imza ile aynı hükümlülüğe getirilmiştir. Bu durum, elektronik imza uygulamalarının yaygınlaşmasını sağladığı gibi, güvensiz kullanılmasına da yol açabilir. Bu durum, büyük zararlara sebep olabilmektedir. Bu nedenle kişilerin kullandığı uygulamaların elektronik imza oluşturma ve doğrulama kısımlarının derinlemesine testen geçirilmesini de bir zorunluk haline gelmiştir. Aksi takdirde kişiler farkında olmadan büyük zararlar görebilirler. Bu şekilde kötü sonuç doğurabilecek durumların önüne geçilmesi, hatalı-geçersiz imzalı dosyaların oluşturulmasının önlenmesi ve geçersiz bir imzalı dosyanın, geçerli olarak değerlendirilmesinin önlenmesi adına elektronik imza uygulamaların test edilmesi büyük önem taşımaktadır. Firmalar imza doğrulama uygulamalarından emin olamazlarsa geçersiz bir imzalı dosyayı doğrulayıp çeşitli saldırılara maruz kalabilirler. İmza oluşturma uygulamaları düzgün çalışmıyorsa farkında olmadan geçersiz imzalı dosyalar oluşturabilirler. Bu tip kötü kullanıma açık senaryoların oluşmaması adına, güvenlik ilkesiyle kurulmuş elektronik imza uygulamalarının standartlara uygun bir şekilde implement edilmesi (uyarlanması) ve detaylı bir şekilde test edilmesi gerekmektedir.

Elektronik imza uygulamalarını test etmek adına; imza oluşturma ve imza doğrulama mekanizmalarında oluşabilecek hatalı durumların neredeyse tamamını ele alan bir model kullandık [1]. Bu modelde imza oluşturma ve imza doğrulama kısımlarında kullanmak üzere CA hiyerarşileri, OCSP sunucuları, SİL servisleri, zaman damgası sunucuları ve son kullanıcı sertifikaları oluşturduk. İmzalı dosyaları oluşturabilmek için de PAdES imza oluşturma uygulaması kodladık ve bu uygulamayı kullarak imzalı dosyalar setini oluşturduk. İmza oluşturma kısmında karşılaşabilecek senaryoları kendi içlerinde bölümlere ayırdık ve bu

hatalı durumlara sahip yapıları gerçekleştirdik. Bu yapıları anlatmak adına örnekle açıklamak istiyorum. Senaryomunuzun, alt kökün sertifikasının imzasının bozuk olması durumu olduğunu düşünelim. Alt kök sertifikasının imzasının bozuk olma senaryosunu sağlamak adına geçerli bir kök yarattık ve bu kökün imzaladığı alt kök sertifikasının imzasını bozduk. İmzası bozuk olan alt kökten, tamamen hatasız bir son kullanıcı sertifikası ürettik. Bu son kullanıcı sertifikasının iptal kontrolünün yapıldığı bütün yapıları hatasız bir şekilde oluşturduk. Çalışan OCSP sunucuları ve gelen OCSP cevapları, SİL servisleri ve SİL cevaplarının doğru şekilde çalışmasını sağladık. Böylece bu yapıdaki tek hatalı durumun, "alt kökün sertifikasının bozuk olma durumu" olduğunu güvence altına aldık. Bahsettiğimiz üzere, tek bir senaryo için alt kökün imzasının bozuk olması dışında tamamen doğru çalışan büyük bir yapı kurmuş olduk. İmza oluşturma uygulamalarının bu hatalı durumu yakalayıp yakalamadığını anlamak adına; oluşturduğumuz ilgili yapıda bulunan son kullanıcı sertifikası ile imza oluşturma testi yaptık. İmza oluşturma uygulamasının; son kullanıcı sertifikası ve bütün yapıyı doğruladıktan sonra, imza oluşturmaya izin vermesi beklenmektedir. Bu senaryoda son kullanıcı sertifikasının imzası doğrulanacak, iptal kontrolü yapılacak ve sonrasında alt kök sertifikası için yine aynı kontroller yapılacaktır. Tek hatalı durum; "alt kök sertifikasının imzasının bozuk olma durumu" olduğu için uygulamadan beklenen bu hatayı yakalaması ve imza oluşturmaya izin vermemesidir. İmza oluşturmaya izin vermemesinin yanında, imza oluşturma sırasında yakalanan durumu da kullanıcıya düzgün ifade etmesi önemlidir.

Tek bir hatalı durumun oluşturulması için yapılan çalışmalardan kısaca bahsettik, bu örnekten de anlaşıldığı üzere, imza oluşturma kısımları test edilirken uygulamaya bir son kullanıcı anahtarı ve sertifikası girdi (input) olarak verilmiş ve işlem sonucunda bu sertifika ile aynı zincirde bulunan ve bu sertifikanın yayıcısı olan alt kökteki hatanın, yakalanması amaçlanmıştır.

Bütün senaryoları gerçellemek adına; her bir durum için son kullanıcı sertifikalarından oluşan bir yapı oluşturduk. Bütün senaryolar için, oluşturduğumuz son kullancı sertifikalarıyla imza oluşturulmaya çalışıldığında; son kullanıcı sertifikasından başlayarak köke kadar giden zincirde, ilgili hatanın bulunduğu kısımda bu hatanın yakalanması gerekmektedir. Örnek verdiğimiz alt kökün sertifikasının imzasının bozuk olma senaryosunun, imza oluşturma tarafında yakalanması gerektiği gibi imza doğrulama tarafında da aynı şekilde yakalanması gerekmektedir.

İmza oluşturma testleri yapılırken; ilgili senaryonun test edilmesi için, bir son kullanıcı sertifikasının uygulamanın imza oluşturma mekanizmasına takıldığı ve ilgili hatanın yakalanmasıyla imza oluşturulmamasının beklendiğinden bahsetmiştik. Aynı şekilde imza doğrulama uygulamalarının aynı yapı ile oluşturulmuş imzalı dosyayı doğrulamaması ve hatayı düzgün bir şekilde kullanıcıya bildirmesi beklenmektedir. Hatalı senaryoların imza doğrulama mekanizmaları tarafından kontrol edilip edilmediğini test etmek amacıyla, yapısında tekil bir hataya sahip imzalı dosyalar tarafımızdan geliştirilen Bölüm 4.4 belirtilen PAdES imza oluşturma uygulaması kullanılarak oluşturulmuştur.

Yapılan testlerde kullanılan metotolojiyi anlatmak adına imza oluşturma ve imza doğrulama testlerinde yaptığımız çalışmalardan bahsettik. Aynı şekilde bütün senaryolar için gerek sistemsel, gerek yazılımsal bileşenler tek tek tarafımızdan gerçellenmiştir. İmza oluşturma mekanizmasında kullanılan suit PAdES e özel bir suit değildir. Bu suit açıkladığımız üzere içerisinde son kullanıcı sertifikalarından başlayarak, köke kadar ilerleyen ve iptal kontrolleri yapılması için içerisinde SİL ve OCSP sunucuları barındıran bir CA yapısındadır. Bu yapıda ilgili hataları kendisinde ya da bulunduğu zincirdeki bir halkada barındıran son kullanıcı sertifikaları bulunmaktadır. Bu sertifikalar kullanılarak PAdES uygulamaların imza oluşturma mekanizmalarının test edilmesinin yanında; XAdES, CAdES imza oluşturma uygulamalarının da imza oluşturma mekanizmaları test edilebilir.

Hatalı durumların son kullanıcıya, alt köke, iptal bilgisine bağlı olabileceğine yüzeysel bir şekilde değinmiştik. Son kullanıcı sertifikasından başlanarak bir zincirdeki her bir halkanın doğrulandığını ve test senaryolarımızda bu zincirlerin birinde spesifik bir hata olduğundan da bahsetmiştik. Hatalar bu zincir üzerindeki yapılarda olabildiği gibi zaman damgalarında da olabilmektedir. Zaman damgalarının bir verinin damgalanan tarihten önce varolduğu teyit altına aldığından bahsetmiştik. Zaman damgalarının elektronik imzada kullanılma amacı; oluşturulmuş olan imzalı dosyanın yine aynı şekilde ilgili tarihten önce oluşturulduğunu garanti altına almaktır. Bu sayede yapılacak olan geçerlilik ve iptal kontrolleri; zaman damgasının alındığı tarihteki durum baz alınarak yapılabilir. Zaman damgasının kullanımını kısaca hatırlattıktan sonra test suit açısından önemine de kısaca değinelim. Zaman damgası da imzalı bir yapıdadır. Bu sebeple zaman damgasının yapısının da düzgün bir şekilde kontrol edilmesi çok önemlidir. Test suit'de zaman damgalarının da sahip olabileceği hatalar tarafımızdan düşünülmüş ve bu hatalara sahip zaman damgası sunucuları kurulmuştur. İmza

oluşturma testlerinde bahsettiğimiz CA hiyerarşisinde zaman damgası sunucuları da bulunmaktadır. Test edilecek olan hatalı durumu içeren zaman damgası sunucusu adresine gidilmesi, dönen cevapların uygulama tarafından değerlendirilmesi ve ilgili hatanın yakalanması beklenmektedir. İmza doğrulama testlerindeyse imzalı dosyaların uygulamanın imza doğrulama mekanizmasına doğrulatılarak, mekanizmaların ilgili hatayı yakalaması beklenmektedir. Bu bölümde test suit oluştururken izlediğimiz metotoloji ve örnek bir senaryoyu nasıl sağladığımıza değindik. Önümüzdeki bölümde senaryoları irdeleyeceğiz.

3.1 İmza Oluşturma Senaryoları

Bu bölümde imza oluşturma testlerinde kullandığımız senaryoları ve kullandığımız modeli inceleyeceğiz. Daha öncesinde de bahsettiğimiz üzere son kullanıcı sertifikasından başlayarak kök sertifikasına kadar giden bir zincir bulunmaktadır. Bu zincirde alt kök sertifikası, kök sertifikası, OCSP sertifikası, OCSP cevabı , SİL cevabı gibi yapılarda spesifik hatalar bulunabilir. İşte bu bölümde bu hataları başlıklar altında detaylandıracağız.

3.1.1 Son Kullanıcı Senaryoları

Son kullanıcı sertifikalarından başlayarak köke uzanan bir zincirden bahsetmiştik. Bu bölümde bu zincirin ilk elemanı olan son kullanıcı sertifikaları kaynaklı hatalı senaryolardan bahsedeceğiz. Bu senaryoları nasıl oluşturduğumuzu anlatacağız ve Reader'a uygulayarak sonuçları paylaşacağız.

3.1.1.1 Sertifika İmza Kontrolü

Açık anahtar altyapısında özel anahtar ve açık anahtar olmak üzere iki tip anahtar olduğundan bahsetmiştik. Elektronik imzada özel anahtar kullanılarak imzalanan dokümanın, doğrulama işleminin açık anahtarla yapıldığını anlatmıştık. Karşı tarafa imzalanan doküman ile birlikte imzanın doğrulanabilmesi adına açık anahtarın da iletilmesinin zorunlu olduğunu ve bu açık anahtarın araya giren saldırganlar tarafından değiştirilmemesi adına, güvenli bir şekilde iletilmesi gerektiğini detaylı bir biçimde aktarmıştık. Açık anahtarın imza ile birlikte

alıcıya güvenli bir biçimde iletilmesinin elektronik sertifika ile sağlanabileceğinin altını çizmiştik. Elektronik sertifika; içerisinde açık anahtarın yanında kime ait olduğunu içeren bir çok alanı (field) barındıran imzalı bir yapıdır. Elektronik sertifika, kendisini yayınlayan yayıncı tarafından imzalanır. Son kullanıcının sertifikası kendisini oluşturan alt kökün özel anahtarıyla imzalanır. Alt kök sertifikası da, kök tarafından imzalanır. Kök sertifikaysa anlattığımız üzere kendi özel anahtarıyla kendi sertifikasını imzalamış (self signed) bir sertifikadır. Kısaca sertifika ve sertifika zincirini hatırlatmamızın ardından, sertifikanın imzasının kontrolünün neden çok önemli olduğunu irdeleyebiliriz. Sertifikanın bütünlük, kimlik doğrulama prensiplerinin korunması adına, imzalanması son derece önemlidir. İmzası bozuk bir sertifika; araya girilen bir kişi tarafından herhangi bir alanı değiştirilmiş bir sertifika olabilir. Bu detaylar göz önünde bulundurulduğunda, sertifikanın ve zincirinde bulunan bütün sertifikaların ve imzalı yapıların imzasının doğrulanması mutlak suretle gereklidir. Eğer son kullanıcı sertifikasının ya da zincirindeki bir sertifikanın imzasının bozuk olma durumu mevcutsa ve imza oluşturma uygulaması tarafından imza oluşturulmasına izin verilirse, kullanıcıya bilgi verilmeden geçersiz bir imzalı dosya oluşturulmuş olunur. İmzası geçersiz şekilde imzalı dosya oluşturulması durumu kötü kullanıma açık durumlar oluşturabilir. Bu durumdan daha da tehlikeli olan durum, eğer imzası bozuk olan bir sertifika ile oluşturulmuş bir imzalı dosyanın doğrulanmaması gerekirken uygulama tarafından doğrulanması durumudur. Bu büyük bir yıkıma sebebiyet verebilir. Saldırganların, başkaları adına, oluşturdukları imzalı dosyaları değiştirerek kimlik dolandırıcılığı yapmasının yolu açılmış olunur. Bu sebeple gerek son kullanıcı sertifikaları gerekse alt kök sertifikaları ve diğer yapılar için imza kontrolü dikkatlice yapılmalıdır. Bu kontrolün son kullanıcı sertifikalarında yapılıp yapılmadığını anlamak adına imzası bozuk olan bir son kullanıcı sertifikası oluşturduk ve Adobe Reader'ın imza oluşturma kısmında bu son kullanıcı sertifikasını kullanarak imza oluşturma testi yaptık. Sonuç olarak Adobe Reader'ın imza oluşturma testleri sırasında hatalı bir şekilde imzası bozuk son kullanıcı sertifikası ile imza oluşturulmasına izin verdiğini fark ettik.

3.1.1.2 Sertifika Geçerlilik Kontrolleri

Sertifika yapısında çeşitli alanlar olduğundan bahsetmiştik. [3] Bu alanlardan biri de sertifikanın başlangıç tarihidir. Sertifikanın başlangıç tarihi sertifikanın kullanılmaya başlandığı tarihi belirtir. Sertifikalar geçerlilik başlangıç tarihinden serti-

fika bitiş tarihine kadar kullanılabilirler. Bu tarihlerden sonra kullanılamazlar. Bu şekilde bir zaman kısıtının bulunmasının temel sebebi, anahtarların güvenliğinin belirli bir süreden sonra tehlikeye girebilmesinden kaynaklanmaktadır. Sertifika için biçilen süre, kötü amaçlı kişilerin sürekli olarak anahtar çiftlerini kırmaya çalıştıklarını ve bunu da büyük bir donanım ile yaptıklarını öngörerek hesaplanır. Anahtarların çok güçlü donanımlar ile ne kadar sürede kırılabileceği belirlenmiş ve bu sürelerden sonra anahtar çiftlerinin ve dolayısıyla açık anahtarı koruma altına alan sertifikanın yenilenmesinin gerektiği belirtilmiştir.

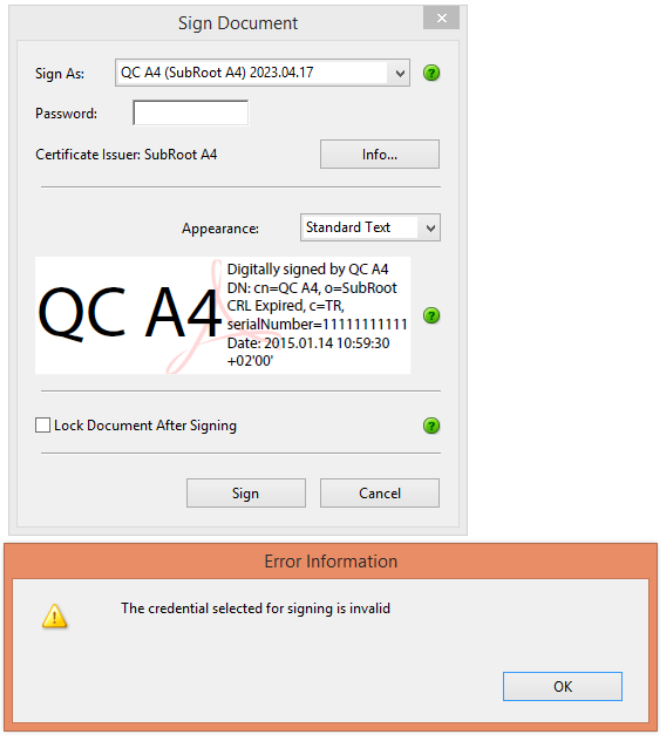
Uygulamaların süresi dolmuş sertifikalar kullanılarak imza oluşturulmasına izin vermemesi beklenir. Bu senaryomuzda süresi dolmuş bir son kullanıcı sertifikası kullanarak Adobe Reader'ın imza oluşturma kısmını test ettik.

Sertifika geçerlilik kontrolü offline olarak yapılan bir kontroldür. Sertifikanın içerisinde imzalı bölümde güvence altına alınmış olarak muhafaza edilen geçerlilik başlangıcı (valid from) ve geçerlilik bitişi (valid to) arasındaki bir tarihte imzalama işlemi yapılıyorsa ve başka bir hatalı durum yoksa uygulamanın imza oluşturmaya izin vermesi beklenir. İmza oluşturma mekanizması imza oluşturulan tarihin geçerlilik tarihleri içerisinde bulunup bulunmadığını tespit etmek için sistem saatinden veya zaman damgasından yararlanabilir. Oluşturduğumuz son kullanıcı sertifikası ile Reader'a yaptığımız testlerde, son kullanıcı sertifikası geçerli olmayan durumlar Reader tarafından yakalanmıştır. Fakat kullanıcıya Şekil 3.1 deki gibi durumu açıklamayan ve net olmayan bir hata mesajı vermiştir.

3.1.1.3 Sertifika niteliklilik kontrolleri

Nitelikli sertifikanın tanımlaması yapmıştık. 5070 sayılı kanuna göre kişinin nitelikli sertifikası ile oluşturduğu imzalar ıslak imza ile aynı yasal geçerliliğe sahiptir demiştik. Türkiye'de nitelikli sertifikaların sağlaması gereken kriterler belirtilmiştir. [16, 18, 19, 21, 38] Tarafımızdan Adobe Reader'ın uluslar arası standartlarda belirtilen niteliklilik kontrollerini yapıp yapmadığını test etmek adına; kriterlerde belirlenen durumlardan her bir son kullanıcı sertifikası için, yalnızca bir tanesini sağlamayan niteliksiz son kullanıcı sertifikaları oluşturduk.

Bu senaryolardan ilki anahtar kullanımı alanında (key usage); inkar edilememezlik (non repudation) prensibinin, bulunmadığı son kullanıcı sertifikasının oluşturulmasıdır. Nitelikli sertifikanın sağlaması gereken temel şartlardan olan, inkar



Şekil 3.1: Reader'ın İmza Oluşturma Sırasında Verdiği Standart Hata

edememezlik özelliğinin bulunmadığı son kullanıcı sertifikasını oluşturduk.

İkinci olarak ETSI QC Statment ID (0.4.0.1862.1.1) alanının olmadığı son kullanıcı sertifikasını oluşturduk. ETSI QC Statment ID'si nitelikli sertifikaların sahip olması gereken zorunlu bir alandır ve ID kontrolü, niteliklilik kontolleri sırasında bakılması gereken bir kontroldür. [19] Türkiye'de niteliklilik ile ilgili şartları tanımlayan kuruluş Bilişim Teknolojileri Kurumu'dur (BTK). BTK nitelikli sertifikaların QC Statment bölümünde belirlediği OId (Object Identifier)'nin ve kullanıcı notunun bulunmasını zorunlu tutmuştur. Türkiye'de 5070 sayılı kanunda belirtilen hükümlülükleri sağlayan imzalı dosyaların oluşturulabilmesi adına bu iki alanın bulunması da mutlak suretle gereklidir. Türkiye'de bulunan uygulamaların sertifikanın nitelikli olarak değerlendirilip değerlendirilmeyeceğine karar vermesi esnasında bu alanları da kontrol etmesi beklenmektedir. Adobe Reader Türkiye için geliştirilmiş bir uygulama değildir. B sebeple bu alanların default'da kontrol edilmesini elbette beklememekteyiz. Bu sertifikaları oluşturmamızdaki amaç; Adobe Reader'ın yanında daha farklı imza oluşturma uygulamalarının test edilmesi sırasında bu son kullanıcı sertifikaların kullanılabilmesidir. BTK nın belirlediği ve QC statement kısmında bulunması gereken OID (2.16.792.1.2.1.1.5070.7.1.1) bulunmayan bir son kullancı sertifikası ve BTK nın Kullanıcı notu olan "Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır." notunu bulundurmayan bir son kullanıcı sertifikası oluşturarak bu iki durumu da ayrı yarı inceleme imkanı sağlamış olduk.

Sertifika Politikası Kullanıcı Notu (Certificate Policy User Notice) sertifikanın hangi amaçla üretildiğini belirten bir politikadır. 5070 sayılı E-imza kanununa göre sertifikanın nitelikli sayılabilmesi için BTK tarafından belirtilmiş olan sertifika politikası object id (2.16.792.1.2.1.1.5.7.1.1). bulunmak zorundadır. Bu senaryomuzda yine Adobe Reader ın bu kontrolü yapmasını beklemiyoruz ancak ürettiğimiz test suit ile farklı uygulamaların test edilmesi durumunda bu durumun test edilebilir bir durum olarak setimizde bulunması adına bu senaryoya sahip sertifikaları ürettik.

3.1.1.4 Sertifika İptal Konrolleri

Kişinin açık anahtarını ve kendisine aitlik bilgilerini içerisinde bulunduran ve sertifikalardan bahsetmiştik. Sertifikanın içerisinde açık anahtar dışında X509 standartında belirlenen alanların bulunduğundan bahsetmiştik. Sertifikanın geçerliliği

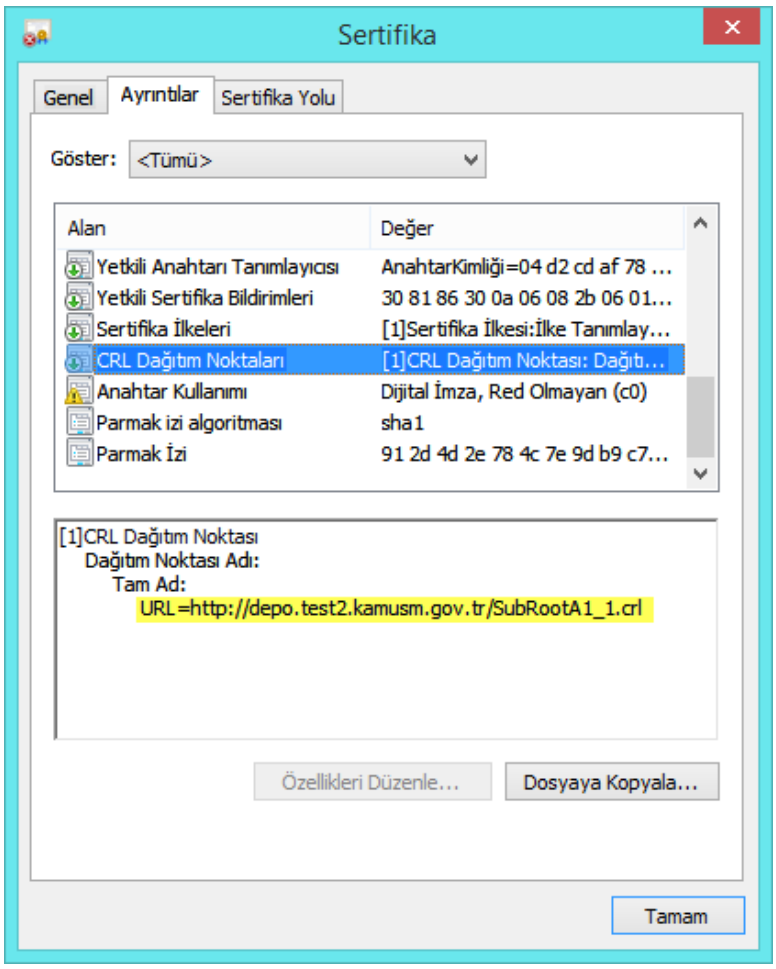
için bir başlangıç ve bitiş tarihi bulunduğunu ve bu tarihler arasında bir zamanda sertifikayla imza oluşturulabileceğini aktarmıştık. Kişilerin (ıslak imzaları yerine geçen) elektronik imzalarının, iptal edilmesini gerektirecek durumlar oluşabilir. Aynı kredi kartlarında olduğu gibi kişilerin elektronik imzalarını kaybetmeleri durumunda elektronik imzanın iptal edilmesi, oluşabilecek kötü niyetli kullanım önüne geçilmesi adına son derece önemlidir. Kişiler sertifikalarını iptal ettirmek için elektronik imzasını aldığı Elektronik Sertifika Hizmet Sağlayıcı'lara (ESHS) başvurabilirler. Elektronik Sertifika Hizmet Sağlayıcıları kişilerin sertifikalarını iptal etmek ve iptalleri yayınlamak zorundadırlar.

Sertifikaların iptalinin iki farklı şekilde yapılabileceğinden bahsetmiştik. Bu metodlardan ilkinin sertifika iptal listesinin indirilmesi ve bu listeler içerisinden iptal durumununun kontrol edilmesi olduğunu belirtmiştik. Sertifika iptal listelerinin dezavantajının; belirli aralıklarla yayınlanan bir liste olması, iptal durumunun anlık olarak sorgulanamaması olduğundan, avantajınınsa; aynı alt kök tarafından yayınlanan bütün sertifikalar için aynı SİL kullanıldığından aynı alt kök tarafından yayınlanmış kullanıcılarının listeyi bir kez indirmek koşulu ile aynı sertifika iptal listesinden iptal kontrolü yapabilmesi olduğundan bahsetmiştik. Uygulamaların sertifikanın iptalini sorgulamak için bir Uniform Resource Locator'a (URL) ihtiyaç duyduğunu ve bu adresi sertifikaların içerisinde imzalı bir şekilde korumaya alınmış olan SİL Dağıtım Noktalarından (CRL Distribution Point) alabildiklerini ifade etmiştik.

Diğer metodunsa OCSP'den sorgulama metodu olduğunu belirtmiştik. OCSP'den sorgulamanın anlık olarak yapıldığını ve sorgulama yapılırken seri numarası sorulan sertifika için spesifik bir sorgu yapısı oluşturulduğunu, bu sorguya istinaden sorgusu yapılan sertifikaya özgü anlık bir cevabın dönüldüğünü detaylarıyla ele almıştık. OCSP'nin avantajlarının; anlık ve güncel cevabın dönülüyor olması, SİL'e göre boyutunun küçük olması, dezavantajlarınınsa kullanıcılara ve ESHS ye her an online olma zorunluluğu getirmesi, SİL'de olduğu gibi bir liste dönmediği için, yalnızca bir kullanıcının iptal bilgisi için kullanılabiliyor olması olduğunu aktarmıştık. Uygulamalrın OCSP'den iptal kontrolü yapması için yine sertifika içerisinde yetkili bilgi erişimi (authorithy information access) kısmında bulunan OCSP adresi kullanıldığını aktarmıştık.

Bir sertifikada hem OCSP hem de SİL adresi bulunabileceği gibi, yalnızca OCSP adresi veya SİL adresi bulunabilir. Bu sebeple uygulamaların hem OCSP hem de SİL'ler ile çalışabilmesi gerekmektedir. Testlerimizde yalnızca SİL'den hizmet

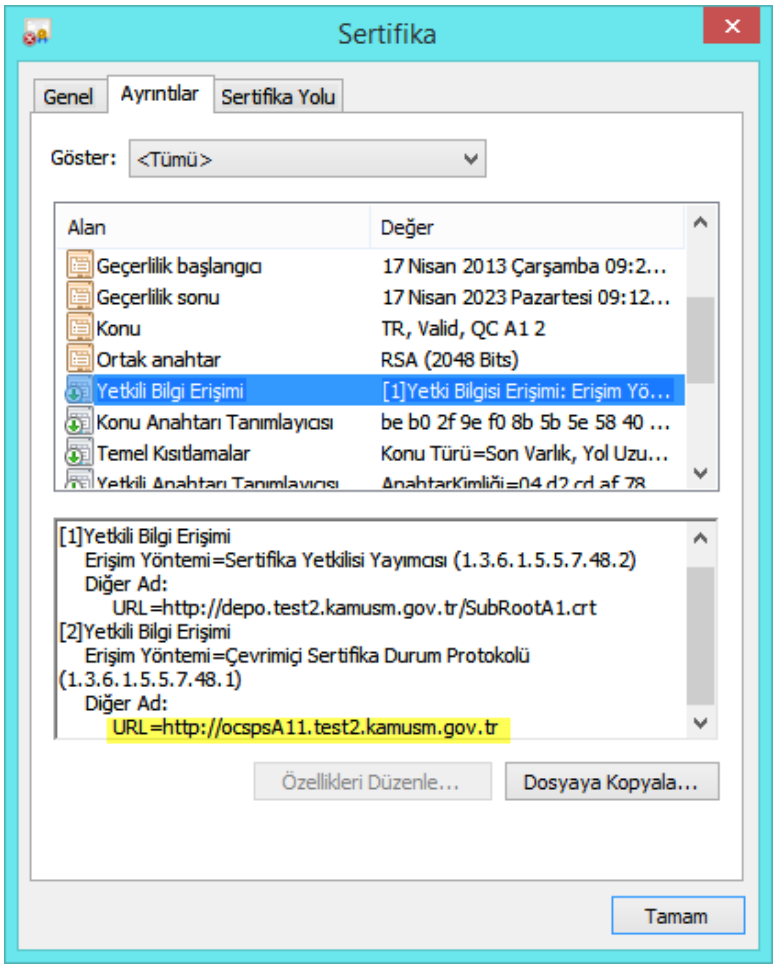
alan ve yalnızca OCSP'den hizmet alan birer sertifika üreterek uygulamanın SİL'ler ve OCSP'ler ile düzgün bir biçimde çalışıp çalışamadıklarını kontrol ettik. Seneryolarımızın birinde sertifikanın içerisinde Şekil 3.2 de görüldüğü gibi yalnızca içerisinde SİL adresi bulunmakta, diğerindeyse Şekil 3.3 de görüldüğü gibi yalnızca OCSP adresi bulunmaktadır. Bu iki sertifika ile de Adobe Reader'ın imza oluşturması beklenmektedir.



Şekil 3.2: İçerisinde SİL Adresi Bulunan Sertifika

İçerisinde yalnızca SİL Dağıtım Noktası adresi barındıran sertifika ile imza oluşturma testlerinde Adobe Reader beklenilen şekilde SİL listesini indirerek imza oluşturma işlemini başarı ile tamamladı.

OCSP sorgusu yapılırken oluşturulan OCSP request içerisinde bir CertID alanı bulunmaktadır. CertID alanı detayları görülebilir. [25,39] CertID alanı içerisinde hash alınırken hangi algoritmanın kullanılacağını belirten bir Algorithm Identifier Sequence'i bulunmaktadır. Standartta gösterildiği üzere CertID alanı içerisinde



Şekil 3.3: İçerisinde OCSP Adresi Bulunan Sertifika

sertifikanın "issuerNameHash" , "issuerKeyHash" ve "serial number" kısımları bulunmaktadır. Algorithm Identifer'da belirtilen hash algoritmasına göre burada belirtilen hash değerleri hesaplanarak özetlerin (digest) üretilmesi beklenir. Oluşturulan OCSP isteğine cevap olarak da dönen OCSP cevabında aynı CertID bulunmaktadır. Adobe Reader'ın oluşturduğu OCSP sorgularında kullandığı algoritmanın SHA1 olduğunu farkettik. İmza oluşturma kısmında Reader tarafından, OCSP sorgusu yapılırken CertID nin hash algoritmasının ayarlanabileceği bir opsiyon sağlanmamaktadır. Fakat yine de Reader, OCSP'li senaryomuzu başarı ile geçti. SHA1 algoritmasının güvenini günden güne yitirdiği ve Türkiye'de güvensiz bir algoritma ilan edilmesi durumları göz önünde bulundurulduğunda Reader'ın SHA1 dışında bir algoritmanın seçilmesine izin vermiyor olması bir eksikliktir. Güvensiz ilan edilen algoritmalar iptal cevapları, sertifikalar, zaman damgaları başta olmak üzere imzalama işleminde görev alan hiç bir yapıda kullanılmamalıdır. Güvensiz olan algoritma ile oluşturulmuş bir hash değeri ile aynı hash değerine sahip farklı bir içerik oluşturulabilir tehlikesi bulunmaktadır ve PKI yapısında kullanılan ve içeriğinde hash değeri içeren bütün yapıların güvenilir olmayan hash algoritmalarından arındırılmalıdır. OCSP'de elektronik imzada iptalin durumunu gösteren bir yapıdır. Bu sebeple OCSP sorgularının ve cevaplarının güvensiz olan bir algoritma ile yapılmaması gerekmektedir. ESHS'lerin Türkiye'de verdikleri bütün hizmetleri SHA1 den arındırmaları gerektiği bildirilmiştir. [13, 40] Adobe Reader OCSP sorgularını yalnızca SHA1 algoritması ile gerçekleştirdiği için Türkiye'deki ESHS'lerden cevap alamaması muhtemeldir.

3.1.1.4.1 SİL'de İptal Olmuş Sertifika Sertifika kontrollerinin uygulamalar tarafından hem SİL'den hem de OCSP'den yapılabilmesi gerektiğini belirtmiştik. Bir sertifikanın SİL'de iptal olma durumunun ve OCSP'de iptal olma durumunun uygulama tarafından düzgün bir şekilde değerlendirilip değerlendirilmediğini tespit etmek adına, içerisinde yalnızca SİL adresi bulunan ve SİL'de iptal durumda olan bir sertifika ürettik. Adobe Reader'dan beklediğimiz sertifika içerisindeki SİL adresinden SİL'i indirmesi ve sertifikanın iptal olduğunu görerek iptal olduğu ile ilgili mesajı kullanıcıya düzgün bir şekilde vermesidir. Adobe Reader oluşturduğumuz son kullanıcı sertifikasının iptal olma durumunu düzgün bir biçimde yakalamış ve imza oluşturulmasına izin vermemiş, fakat yine Şekil 3.1 daki mesajı vermiştir.

3.1.1.4.2 OCSP'de İptal Olmuş Sertifika SİL'de iptal olma durumuna benzer bir durum olarak da içerisinde yalnızca OCSP adresi bulunan durumu oluşturduk. Bu sertifika ile imza oluşturma testlerimiz sırasında Adobe Reader'ın sertifika için OCSP sorgusu yaparak gelen OCSP cevabındaki iptal olma durumunu incelediğini ve imza oluşturulmasına izin vermediği tarafımızdan görüldü. Fakat Şekil 3.1 gösterildiği üzere Adobe Reader açıklayıcı bir hata mesajı dönmemektedir.

3.1.2 Yayıncı Sertifikası Kontrolleri

Bir önceki bölümde son kullanıcı sertifikalarında oluşabilecek hataları başlıklar altında açıklamıştık. Sertifikaları detaylı bir biçimde incelemiş ve son kullanıcı sertifikalarınında bir alt kök tarafından imzalandığını aktarmıştık. Aynı şekilde alt köklerin de sertifikalarının bulunduğuna değinmiştik. Bu bölümde son kullanıcı sertifikalarını yayınlayan alt köklerde oluşabilecek senaryoları inceleyeceğiz.

Alt köklerde oluşabilecek senaryoları incelerken yine alt kök hariç bütün yapıları doğru çalışacak bir şekilde oluşturduk ve hatanın yalnızca alt kökte olmasını sağladık. Böylelikle uygulamaların alt kökte oluşabilecek hatalı durumları yakalayıp yakalayamadığını görmüş olduk. Alt kökte oluşabilecek her bir hatayı gerçelleyebilmek adına geçerli bir kökten ilgili senaryodaki hatayı barındıran bir alt kök sertifikası ürettik ve bu sertifikadan hatasız bir son kullanıcı sertifikası ürettik. Ürettiğimiz son kullanıcı sertifikasını kullanarak uygulamaların imza oluşturma mekanizmalarını test ettik. Burada uygulamalardan beklenen son kullanıcı sertifikasından başlayarak bütün ağaçtaki yapıların düzgün ve geçerli olup olmadığını kontrol etmesidir. İlgili hatalar alt kökte olduğu için; uygulama, alt kök kontrollerini yaparken alt kökteki hatayı tespit etmeli ve imza oluşturmadan uygulamadan çıkmalıdır. İlgili durumu karşılayacak şekilde hatalı mesaj dönmesi de önemlidir. Adobe Reader'ın imza oluşturma testleri sırasında alt kökler ile ilgili kontrolleri kapsamlı ve düzgün bir şekilde yapıp yapmadığının tespit edilmesi adına bu bölümde yaptığımız çalışmalar da son derece önemlidir. Bazı uygulamalarda son kullanıcı sertifikalarında işlemler doğru bir biçimde yapılmış olsa dahi yayıncı sertifikaları ile ilgili kontroller düzgün bir biçimde yapılmıyor olabilir.

Yine son kullanıcı sertifikalarında yaptığımız gibi yayıncı sertifikalarında oluşabilecek durumları başlıklar altında inceleyeceğiz.

3.1.2.1 Sertifika İmza Kontrolü

Sertifikanın imzasının bozulması, sertifikanın bütünlüğünün bozulduğu, sertifikanın değiştirildiği yada zarar gördüğü anlamına gelmektedir. Araya giren saldırganın kendi açık anahtarını sertifikadaki açık anahtar ile değiştirdiği düşünülebilir. [14] Sertifikanın imza kontrolü imza oluşturma ve imza doğrulama uygulamaları tarafından mutlaka düzgün bir şekilde yapılmalıdır. İmza oluşturma mekanizmasında bu şekilde bir duruma izin verilmesi halinde, doğrulanamayan imzalı dosyaların oluşması kaçınılmazdır. İmza oluşturulmasına izin verilmesiyle imza oluşturmaya bağlı süreçler aksayabilir, kişiler düzgün bir biçimde imzalı dosya oluşturduklarını düşünürken geçersiz imzalı dosyaları sistemlere sürebilirler. Her ne kadar bu durum imza doğrulama uygulamalarının düzgün çalışması ile açığa çıkacak olsa da, süreçleri çeşitli risklere sokabilecek durumlar oluşturabilir. Bu gibi sebeplerden ötürü uygulamaların imza oluşturma kısımlarında; imzası bozuk alt kök sertifikası tarafından verilmiş son kullanıcı sertifikasıyla, imza oluşturulmasına izin vermemesini ve kullanıcıya hatayı düzgün bir biçimde dönmesini bekleriz.

Adobe Reader'da imzası bozuk bir alt kök sertifikasından verilmiş son kullanıcı sertifikası ile imza oluşturma testlerimiz sonucunda imza oluşturulmasına izin vermiştir.

3.1.2.2 Sertifika Geçerlilik kontrolleri

Sertifikaların içerisinde sertifika geçerlilik başlangıcının ve sertifika bitiş tarihinin olduğundan bahsetmiştik. Son kullanıcı sertifikalarında olduğu gibi yayıncı sertifikalarının da bir başlangıç ve bitiş tarihi bulunmaktadır. Uygulamalar imza oluşturma sırasında sertifikaların geçerlilik süresi ile ilgili kontrollerini geçerlilik başlangıcı ve geçerlilik bitişi tarihlerini baz alarak kontrol etmektedirler. Bu kontrolün alt kökler mertebesinde yapılıp yapılmadığını anlamak adına geçerli bir kökten süresi dolmuş bir alt kök sertifikası ürettik. Bu alt kök sertifikası tarafından yine geçerli bir son kullanıcı sertifikası oluşturduk. Yine ilgili sertifika zincirinde bulunan tek hatalı durumun yalnızca ilgili senaryo olmasını sağladık. Beklenilen sonuç imza oluşturma sırasında uygulamaların imza oluşturmaması ve sertifikanın geçerlilik süresinin dolduğu ile ilgili olarak hatayı kullanıcıya bildirmesidir.

Adobe Reader'a yaptığımız test sonucunda ilgili sertifikanın geçerlilik dışında olması durumunda imza oluşturulmasına izin vermediğini tespit ettik. İmza atılma basamığına gelmeden offline olarak sertifikayı kontrol ederek imza oluşturma sırasında kullanılmasına izin vermemektedir.

3.1.2.3 Sertifika İptal Kontrolü

Sertifikaların bitiş tarihleri gelmeden iptal olmasını gerektiren durumların oluşabileceğinden bahsetmiştik. Aynı kredi kartları gibi son kullanıcı sertifikalarının da (ESHS tarafından kendilerine kullanıcı tarafından bildirilmesi ve iptalinin istenmesi durumunda) iptal edilebildiğinden bahsetmiştik. İptal olma durumları son kullanıcı sertifikaları bazında sıkça olabilmektedir. Fakat yayıncı sertifikaları ESHS kontrollerinde olduğu için iptallerini gerektiren durum özel anahtarlarının kontrolünün bir şekilde ESHS dışında birilerine geçmesi, özel anahtarın güvenliğini yitirmesi, kırılmasıyla olabilir. Başka bir iptal gerektiren durumsa ESHS'lerin bir şekilde temel kısıtlamalar (basic constraints) alanında, CA yazan sertifikayı son kullanıcı sertifikası olarak vermesi olabilir. Bu tip bir durumda; son kullanıcısı sertifikası olması beklenen sertifika, bir yayıncı sertifikası olarak üretilmiş ve kişiye yayıncı yetkisi verilmiştir ve sertifikasının acilen iptal edilmesi gerekmektedir.

Alt kök sertifikasının iptalini gerektiren durumların oluşması son derece nadir görülen bir durum olsa da dünya üzerinde bu tip durumlar oluşmuştur. Bu sebeple iptal olmuş bir alt kök tarafından oluşturulmuş son kullanıcı sertifikası ile imza oluşturulmaya çalışıldığında uygulamaların imza oluşturulmasını önlemesi ve kullanıcılara ilgili hatayı düzgün şekilde dönmesi beklenmektedir.

İptal kontrollerinin SİL'den veya OCSP'den yapılabileceğinden bahsetmiştik. Alt kök sertifikasının iptal olma durumunu incelemek adına;geçerli bir kökten, birinin içerisinde yalnızca SİL adresi bulunan diğerindeyse, OCSP adresi bulunan iki adet alt kök sertifikası ürettik. Bu sertifikaların her birinden birer geçerli son kullanıcı sertifikası oluşturduk. Uygulamalardan beklentimiz ürettiğimiz son kullanıcı sertifikaları ile imza oluşturmaya çalıştığımızda imza oluşturma işlemini gerçekleştirmemesi ve iptal olma ile ilgili hatayı kullanıcıya iletmesidir.

Adobe Reader'a bu iki son kullanıcı sertifikası ile yaptığımız testler sonucunda Reader'ın imza oluşturmadığını gördük. Fakat hata mesajı açık bir şekilde verilmemektedir. Yine Şekil 3.1 deki gibi durumu açıklamayan, standart bir hata

mesajı verilmektedir.

3.1.3 İptal Değerleri Kontrolleri

Önceki bölümlerde son kullanıcı sertifikaları ve yayıncı sertifikaları kaynaklı olabilecek hatalı seneryoları incelemiştik. Bu bölümdeyse sertifikaların iptal kontrolleri yapılırken karşılaşılabilecek hatalı durumlardan bahsedeceğiz. Sertfikanın iptal olma durumuyla sertifikanın iptal kontrolleri kaynaklı hatalı durumlar bir birine karıştırılmamalıdır. Bu bölümdeyse son kullanıcı sertifikaları ve yayıncı sertifikaları için iptal kontroleri yapılırken iptal kontrolerinde karşılaşılabilecek hatalı senaryoları anlatacağız.

Önceki bölümde, OCSP ve SİL'de oluşabilecek durumları oluşturarak ayrı ayrı inceledik. Yine ilgili hatalı senaryonun SİL tarafında veya OCSP tarafında olma durumlarına göre, kontrolün yapılma metodunu (SİL kaynaklı bir hatalı senaryo test edilecekse) SİL'e, (OCSP kaynaklı bir senaryo incelenecekse) OCSP'e zorladık. Bunu yine ilgili duruma göre içerisine SİL adresi koymayarak veya OCSP adresi koymayarak sağladık. İçerisine SİL adresi koymadığımız sertifika OCSP'den'kontrol edilmeye zorlanmış, tersi bir şekilde OCSP adresi koymadığımız sertifika da SİL'den kontrol edilmeye zorlanmış oldu. Aşağıdaki bölümlerde sırasıyla SİL kaynaklı oluşabilecek senaryolar ve OCSP kaynaklı oluşabilecek senaryolar incelenmektedir.

3.1.3.1 Son kullanıcı İptal Değerleri Senaryoları

3.1.3.1.1 SİL Kaynaklı Senaryolar Sertifikaların iptal kontrollerinin SİL'den yapılabileceğinden ve SİL'in iptal olan sertifikaların tutulduğu bir liste olduğundan bahsetmiştik. Bir SİL'in iptal kontrolünde kullanılabilmesi için de bazı kontrollerin yapılması gerekmektedir. Bu kontrolleri sağlamayan SİL'ler kullanılmamalıdır. SİL'in süresinin dolması veya imzasının bozuk olması durumunda kullanılamaması gerekmektedir.

Süresi Dolmuş SİL: SİL'lerin içerisinde this update ve next update tarihleri bulunmaktadır. Bir SİL'in kullanılabilmesi için kontrolün yapıldığı zamanın next update tarihinden ileride olması gerekmektedir. Next update zamanı imza doğrulama zamanından geride olan SİL'ler süresi dolmuş (expired) olarak

belirtilmektedir. Süresi dolmuş SİL'lerse iptal kontrolü için kullanılamazlar. Bu senaryoda oluşturduğumuz sertifikanın SİL dağıtım noktası alanından indirilen SİL; süresi dolmuş, geçersiz bir SİL'dir. Adobe Reader'ın imza oluşturma testleri sırasında süresi dolmuş SİL'i kabul etmemesini ve imza oluşturmaya izin vermemesi beklenir. Ayrıca ilgili hatayı düzgün bir biçimde de ifade etmesi önemlidir. Reader testlerimizde imza oluşturulmasına izin vermediği görüldü fakat yine Şekil 3.1 gibi standart ve durumu ifade etmeyen bir hata mesajı vermiştir.

İmzası Bozuk SİL : Güvenliği bir zincire benzetirsek güvenliğin gücü en zayıf halkanın gücü kadardır. Bu sebeple sertifikaların güvenceye alındığı bu yapıda sertifikaların iptal olup olmadığının kontrolü imzasız bir şekilde yapılırsa, iptal cevapları değiştirilebilir ve iptal olmuş sertifikalar iptal olmamış gibi gösterilebilir. Bu sebeple bu güven zincirinde bulunan bütün trafik imzalı bir biçimde olmaktadır. SİL'ler de Şekil 3.1 de gösterildiği üzere sorgunun yapıldığı sertifikanın yayıncısı tarafından imzalanmaktadır. Eğer saldırganlar tarafından araya girilip SİL listesi değiştirilirse, bu değişiklik SİL listesinin imzasının bozulmasına sebebiyet verecektir. [14] Bu sebeple SİL'de bulunan imzanın kontrol edilmesi son derece önemlidir.

Bu senaryoda oluşturduğumuz sertifika için dönen SİL'in imzası bozuktur. Adobe Reader ile bu sertifika ile imza oluşturulmaya çalışıldığında beklenildiği gibi imza oluşturma işlemimi tamamlanmamıştır. Fakat Şekil 3.1'de gösterildiği üzere yine durumu tam olarak ifade edemeyen standart bir hata dönülmüştür.

3.1.3.1.2 OCSP Kaynaklı Senaryolar

Sertifikaların iptal kontrolünün yapıldığı bir diğer iptal kontrol metodu da OCSP'dir. OCSP sorgusunun bir sertifika için yapıldığının ve cevabında sorgulanan sertifika için verildiğini aktarmıştık. OCSP'lerin SİL'lere göre avantaj ve dez avantajlarını ele almıştık. SİL'lerin iptali sorgulanan sertifikanın yayıncısı tarafından imzalandığından, OCSP'lerinse; hem yayıncısı, hem de yayıncısı tarafından imzalanarak yetkilendirilmiş bir OCSP sertifikası tarafından imzalanabildiğini anlatmıştık. Bu bölümde OCSP cevabının süresinin dolması, imzasının bozulmasının yanında OCSP cevabını imzalayan OCSP sertifikasının süresinin dolma, imzasının bozulma ve iptal olma durumlarını da içeren senaryoları inceleyeceğiz.

Süresi Dolmuş OCSP Cevabı: OCSP'i anlatırken OCSP'de SİL'deki gibi bir this update bir bir next update bir de ilaveten "produce at" bulunduğundan

bahsetmiştik. "Produce at" alanının bulunamasının sebebinin OCSP'de online olarak anlık sorgu yapılması ve cevabın anlık üretilmesi olduğunu belirtmiştik. OCSP de bulunan "this update" ile "produce at" tarihleri aynı olması isteğin ilgili anda üretildiğini belirtir ve "next update'in" de "null" olması da her istek için yeni bir OCSP cevabı üretileceğini belirtir. İmza oluşturma sırasında imza anınından daha eski tarihli bir OCSP cevabı kullanılmaya kalkılırsa uygulama buna izin vermez. Yani "produce at" sertifikanın doğrulanma tarihinden daha gerideyse kullanılamaz. Bu senaryomuzda imza oluşturma testleri sırasında kullandığımız OCSP cevabı imza oluşturulduğu andan daha geride oluşturulmuş (süresi dolmuş) bir OCSP cevabıdır. Bu testimizde Adobe Reader'ın süresi dolmuş OCSP cevabı kullanılan durumda imza oluşturamamasını ve kullanıcıya durumu ifade edecek şekilde bir mesaj vermesini bekliyoruz. Yaptığımız test sonucunda Reader'ın bu senaryoda imza oluşturulmasına izin vermediği fakat yine standart bir hata vererek kullanıcaya tam olarak bilgilendirme dönmediğini tespit ettik.

İmzası Bozuk OCSP Cevabı: OCSP cevaplarının da SİL gibi imzalı bir yapıda olduğunu belirtmiştik. Cevapların imzalı olmasının önemine vurgu yapmıştık. Bu senaryomuzda OCSP tarafından imzalanan OCSP cevabının imzası bozulmuştur. Yani cevabın içeriği artık koruma altında değildir. Değiştirilmiş ya da bambaşka bir özel anahtarla imzalanmış olabilir. Yine diğer senaryolarda olduğu gibi bu durumu da test etmek adına duruma özgü bir sertifika hiyerarşisi kurduk. Geçerli bir kökten verilmiş alt kök, bu alt kök tarafından oluşturulmuş geçerli bir son kullanıcı sertifikası oluşturduk. Hatalı senaryoyu sağlaması adına cevabın imzasını bozuk oluşturan bir OCSP sunucusu kurduk. Yine uygulamanın imza oluşturma mekanizmasına input olarak son kullanıcı sertifkasını verdik ve son kullanıcı sertifikası ile imza oluşturmaya çalıştık. Beklediğimiz sonuç OCSP cevabının imzası bozuk olduğu için; Adobe Reader'ın imza oluşturma sırasında hatayı yakalaması ve imza oluştrumaya izin vermemesidir. Reader test sonucunda beklediğimiz üzere imza oluşturulmasına izin vermemiştir. Ancak kullanıcıya durumu ifade eden bir mesaj vermemiş ve Şekil 3.1 gibi standart bir hata mesajı dönmüştür.

Süresi Dolmuş OCSP Sertifikası: OCSP cevabında oluşabilcek senaryoları gerçelledik ve Adobe Reader'ı bu senaryolar ile test ettik. Şimdiyse OCSP sertifikalarında oluşabilcek hatalar üzerinde duracağız. OCSP cevaplarının; iptal sorgusu yapılan sertifikanın yayıncısı veya sertifikanın yayıncısı tarafından verilmiş bir OCSP sunucusu tarafından oluşturulabileceğinden bahsetmiştik. Hali

hazırda OCSP cevabı kullanılan sistemlerde, OCSP cevapları direk olarak alt köklere imzalatılmazlar. Alt köklerin bu şekilde direk online sistemlere bağlı olması son derece sakıncalıdır. Yapılabilecek bir atak ile OCSP cevabı yerine bir alt kök sertfikası imzalatılabilir. Bu sebeple, alt kök tarafından sadece OCSP cevabı imzalamak için yetkilendirilmiş bir OCSP sunucusu tarafından cevaplar imzalanmaktadır. OCSP sertifikasının da bir geçerlilik başlangıç ve bitiş süresi bulunmaktadır. Bu senaryomızda OCSP sertifikasının süresinin dolma durumunu inceledik. Uygulamaların bu testi yapabilmesi adına, bu durumu sağlayacak geçerli bir son kullanıcı sertifikası oluşturduk ve bu son kullanıcı sertifikasının cevabının verildiği OCSP sunucusuna süresi dolmuş bir sertifika ürettik. Bu son kullanıcı sertifikası ile Adobe Reader'ın imza oluşturuma mekanizmasını test ettik. Beklenilen durum Reader'ın, son kullanıcı sertifikasının iptalini sorgulayan OCSP sertifikanın süresi dolduğu için iptal kontrolünü tamamlayamaması ve imza oluşturmaya izin vermemesidir. Testlerimiz sonucunda Adobe Reader beklediğimiz gibi imza oluşturmaya izin vermemiştir. Fakat kullanıcya durumu izah eden bir mesaj vermek yerine Şekil 3.1 de gösterildiği gibi standart bir mesaj vermiştir.

İmzası Bozuk OCSP Sertifikası: OCSP sertifikasının yayıncısı ile iptaili sorgulanan sertifikanın yayıncısının aynı olduğunu belirtmiştik. OCSP sertifikası, OCSP cevabının imzasının doğrulanabilmesi için, kullanılmaktadır ve OCSP cevabına güvenilmesi için OCSP sertifikasının da doğrulanması gerekmektedir. Saldırganlar tarafından OCSP sertifikasının da içeriği değiştirilebilir. Bu şekilde bir değişiklikte sertifikanın bütünlüğü bozulacak ve dolayısıyla OCSP sertifikasının imzası bozulacaktır. Bu senaryoyu oluşturmak adına yine geçerli bir kök, alt kök, son kullanıcı sertifikalarının yanında imzası bozuk bir OCSP sertifikası oluşturduk. Uygulamanın imza oluşturma mekanizmasından beklenilen, son kullanıcı sertifikasının iptal kontrolü sırasında OCSP sertifikasının imzasının bozuk olduğunu yakalaması ve imza oluşturulmasına izin vermemesidir. Uygulamanın yakaladığı hatayı kullanıcıya açıklayıcı bir biçimde ifade etmesi de önemlidir. Reader imza oluşturma testleri sonucunda beklenildiği üzere imza oluşturulmasına izin vermemiştir, Fakat yine kullanıcya durumu ifade eden bir mesaj vermek yerine Şekil 3.1 deki gibi standart bir hata dönmüştür.

OCSP Sertifikası İptal Olmuş: Testlerimiz sırasında kullandığımız bütün senaryolarda, yalnızca bir hatalı durumun olduğundan bahsetmiştik. İnceleyeceğimiz senaryodaysa hatalı durum yalnızca OCSP sertifikasının iptal olma

durumudur. Bu durumu oluşturmak adına geçerli bir alt kök sertifikası ve bu alt kök sertifikasından oluşturulmuş geçerli bir son kullanıcı sertifikası kullanılmıştır. Bölüm 1 de anlatıldığı üzere OCSP sertifikası son kullanıcı sertifikasıyla aynı yayıncı tarafından verilmiştir. OCSP sertifikasının iptalinin SİL üzerinden yapılmaktadır. OCSP sertifikasının SİL'i son kullanıcı sertifikasının SİL'i ile aynıdır ve aynı alt kök tarafından yayınlanmıştır. Bu senaryomuzda Reader ile imza oluşturmaya çalıştığımızda; Reader'ın, son kullanıcı sertifikasında yalnızca OCSP adresi bulunduğu için iptal kontrolünü OCSP ile yapılmaktadır. Sonrasında OCSP sertifikasında No Revocation Check alanı bulunmadığından dolayı, OCSP sertifikası için de iptal kontrolü yapmasını ve OCSP sertifikasının iptali yakalamasını bekliyoruz. Testlerimiz sırasında Adobe Reader'ın son kullanıcı sertifikası için OCSP kullandığını; sonrasında OCSP sertifikasının iptal kontrolü için SİL'i indirdiğini ve (indirdiği SİL son kullanıcı sertifikası için kullanılabilir bir SİL olduğu için) bu SİL'i son kullanıcı sertifikasını doğrulamak için kullandığını farkettik. Unutulmamalıdır ki amaç son kullanıcı sertifikasının iptal kontrolünün yapılmasıdır ve son kullanıcı sertifikası için kontrol hem SİL'den hem de OCSP'den yapılabilmektedir. Bu testte son kullanıcı sertifikası için iptal kontrolü metodu olarak OCSP'ye zorlasakda, (OCSP sertifikasının iptali için kullanılan SİL son kullanıcı sertifikası için yanınlanan SİL olduğu için) son kullanıcı sertifikası SİL kullanılarak doğrulanmıştır. Bu hatalı bir durum değildir. Bu sebeple Reader imza oluşturmasına rağmen bu senaryomuzdan da geçmiştir.

OCSP Cevabında Sorgulanan Sertifikadan Farklı Sertifika Olma Durumu: OCSP cevabında bir CertID alanı bulunduğundan ve bu alan sayesinde, OCSP cevabının hangi sertifika için verildiğinin anlaşılabildiğinden bahsetmiştik. Bu senaryomuzda kurduğumuz OCSP sunucusu sorgu yapılan sertifika için cevap dönmemekte, (hangi sertifika için sorgu yapılırsa yapılsın sorgu yapılan sertifikadan bağımısız olarak) farklı bir sertifika için cevap dönmektedir. Yani dönen OCSP cevabındaki iptal olmadı bilgisi, sorgu yapılan sertifika için verilmemektedir. Bu durum uygulamalar tarafından kesinlikle kontrol edilmesi gereken bir durumdur. Aksi takdirde iptal olmuş bir sertifika ile sorgu yapıldığında, iptal olmamış bir başka sertifika için hazırlanmış cevap kullanılarak iptal durumunun değiştirilmesi sağlanabilir.

İmza oluşturma testinde Reader, OCSP cevabının içinde sorgulanan sertifikadan farklı bir sertifika için cevap dönülmesi durumunda; beklenildiği üzere imza oluşturulmasına izin vermemiştir. Fakat yine Şekil 3.1 deki gibi standart bir hata

dönerek hatayı tam olarak vermemiştir.

3.1.3.2 Yayıncı İptal Değerleri Senaryoları

Son kullanıcı sertifikalarının iptal kontrolleri için kullanılan SİL ve OCSP'lerde oluşabilecek hataları incelemiştik. Aynı hatalı durumlar yayıncı sertifikasının iptal kontrolleri için de geçerlidir. Bu bölümde, yalnızca yayıncı sertifikalarının iptal kontrollerinde hatalı senaryolar olacak şekilde sertifika hiyerarşisi oluşturduk. Geçerli bir kökten, iptal değerinde farklı bir hataya sahip alt kökler ve bu alt köklerden birer son kullanıcı sertifikası ürettik. Bu testlerimizde kullandığımız son kullanıcı sertifikalarının imzası, geçerliliği ve iptali ile ilgili hiçbir hata bulunmamaktadır. Son kullanıcı halkası olarak doğrulama yapılabilmektedir. Zincirde son kullanıcı sertifikasından sonra bulunan alt kök sertifikaları için iptal kontrolü yapılmaya çalışıldığındaysa hatalı durumla karşılaşılmaktadır. Son kullanıcı sertifikalarındaki durumların bir uyarlaması olduğu için çok detaylandırmadan ilgili bölümlerin üstünden yayıncı sertifikaları için yeniden geçeceğiz. Yine SİL'de ve OCSP'de oluşacak hataları oluşturup Adobe Reader'ın bu senaryolarda nasıl sonuçlar verdiğini paylaşacağız.

3.1.3.2.1 SİL Kaynaklı Senaryolar Yayıncı sertifikaları için de, son kullanıcı sertifiklarında olduğu gibi iptal kontrolleri yapılır. Bir yayıncı sertifikasının iptal olma durumu çokça rastlanan bir durum değildir. Bu sebeple anlık sorgu yapmanın çok da anlamı bulunmamaktadır. Genellikle yayıncı sertifikalar için OCSP kullanılmamakta bunun yerine yalnızca SİL kullanılmaktadır. Bu bölümde yayıncı sertifikalarının iptalleri için kullanılan SİL'lerde oluşabilecek geçersiz durumları inceleyeceğiz.

Süresi Dolmuş SİL: Son kullanıcılar için SİL kaynaklı senaryoları incelerken durumu detaylı olarak ele almıştık. Son kullanıcı için yayınlanmış SİL'dekine benzer bir şekilde süresi dolmuş SİL'e sahip bir alt kök sertifikası ürettik. Alt kökün yalnızca SİL'den iptal kontrolü yapmansını sağladık. Testlerimizde Reader'ın alt kökün iptal kontrolünü yapması sırasında, süresi dolmuş SİL'i kabul etmemesini ve imza oluşturulmasına izin vermemesini bekledik. Reader testlerimizde beklediğimiz üzere hatayı yakalamış ve imza oluşturulmasına izin vermemiştir. Fakat yine hatayı ifade eden bir mesaj vermek yerine Şekil 3.1 de görüldüğü üzere standart bir hata mesajı dönüştür.

İmzası Bozuk SİL: Yayıncı sertifikası için kullanılan SİL'in üzerindeki imzanın bozuk olma durumunu incelemek adına; yine sertifikalarımızı oluşturduk. İlgili hatalı duruma bizi ulaştıracak olan son kullanıcı sertifikasıyla Adobe Reader'ın imza oluşturma mekanizmasını test ettik. Adobe Reader beklenildiği üzere yayıncı sertifikasının iptali için indirdiği SİL'in imzasının bozuk olduğunu yakaladı ve imza oluşturulmasına izin vermedi. Fakat kullanıcıya durumu ifade eden açklayıcı bir mesaj vermek yerine Şekil 3.1 de görüldüğü üzere standart bir mesaj verdi.

3.1.3.2.2 OCSP Kaynaklı Senaryolar

Bu bölümde yayıncı sertifikası için yalnızca OCSP'den sorgulama yapılması sağlanacak ve OCSP cevapları, OCSP sertifikasında oluşacak hatalı senaryoların uygulama tarafından yakalanıp yakalanmadığı irdelecektir.

OCSP Cevabının Süresi Dolmuş: OCSP cevabının süresinin dolma senaryosunda yine durumu sağlayacak şekilde sertifika hiyerarşisi kurulmuş; ilgili OCSP sunucusu hazırlanmıştır. Beklenen durum Adobe Reader'ın yayıncı sertifikası için iptal sorgusu yaptığı anda, gelen OCSP cevabının süresinin dolduğunu yakalaması ve imza oluşturulmasına izin vermemesidir. Bununla birlikte durumu ifade edecek şekilde hata mesajı dönerek kullanıcılarını bilgilendirmesi önemlidir. Reader testlerimizde beklediğimiz gibi iptal kontrolünü yapamadığı için imza oluşturılmasına izin vermemiştir. Fakat yine kullanıcıya Şekil 3.1 de görüldüğü gibi durumu ifade etmeyen standart bir mesaj dönmüştür.

OCSP Sertifikasının İmzası Bozuk: Yayıncı sertifikasının iptal kontrolü yapıldığı OCSP sertifikasının imzasının bozuk olma durumunu incelemek adına ilgili duruma sahip sertifika hiyerarşisini oluşturduk ve Adobe Reader'ı ilgili hataya eriştirecek son kullanıcı sertifikasıyla imza oluşturmaya çalışarak test ettik. İlgili senaryoda beklediğimiz durum alt kök sertifikasının iptal kontrolü yapıldığı sırada, OCSP cevabını veren OCSP sunucusunun sertifikasının imzasının bozuk olduğunun anlaşılması ve imza oluşturulmasına izin verilmemesidir. Yaptığımız test sonucunda Reader'ın ilgili durumu yakaladığı, imza oluşturulmasuna izin vermediği görülmüştür. Fakat yine Şekil 3.1 de görüldüğü üzere durumu açıklayan bir mesaj vermekten uzak , standart bir mesaj dönmüştür.

OCSP Sertifikası İptal Olmuş: OCSP sertifikasının iptal olma durumunda farklı bir akış olduğundan bir önceki bölümde bahsetmiştik. OCSP sertifikasının iptal kontrolünün SİL ile yapıldığından ve bu SİL'in, ilgili sorgulamanın yapıldığı

sertifika için de kullanılabilecek bir SİL olduğundan bahsetmiştik. Bu senaryoda da, OCSP'nin iptalinin sorgulanması esnasında dönen SİL, iptali sorgulanan sertifika için de kullanılabilir bir SİL olduğu için OCSP sertifikasının iptal kontrolü es geçilmiştir. İndirilen bu SİL ile yayıncı sertifikasının iptal kontrolü yapılmıştır. OCSP sertifikasının iptal olması durumu yayıncı sertifikasının iptalinin sorgulanmasını önlememiştir ve yayıncı sertifikasının iptali OCSP için indirilen SİL ile yapılmıştır. Son kullanıcı sertifikaları için irdelediğimiz senaryoda belirtiğimiz gibi, Adobe Reader'ın bu akışı hatalı bir akış değildir. Sonuç olarak; son kullanıcı sertifikasının iptali kontrol edildiği için, imzanın bu şekilde oluşturulması hatalı değildir. İmza oluşturulmasına rağmen bu akışın mantıklı bir akışdır. Reader bu testimizden geçmiştir.

3.1.4 Zaman Damgası Doğrulama Senaryoları

Zaman damgasının, elektronik imzada son derece önemli bir rol üstlendiğinden bahsetmiştik. Sertifika geçerliyken oluşturulmuş bir imzanın sertifika geçerliliğini yitirdikten sonra da doğrulanabilmesi adına; zaman damgasının, kilit bir rol üstlendiğini belirtmiştik. İmzanın ilgili tarihten önce varolduğunu ispatlayan zaman damgasının da uygulamalar tarafından düzgün bir biçimde değerlendirilmesi son derece önemlidir.

Önceki bölümlerde son kullancı sertifikaları kaynaklı senaryoları, yayıncı kaynaklı senaryoları, son kullanıcı ve yayıncı için iptal bilgisi kaynaklı senaryoları incelemiştik. Bu bölümdeyse zaman damgasında oluşabilecek senaryoları inceleyeceğiz.

3.1.4.1 İmzası Bozuk Zaman Damgası

Zaman damgası cevabının da imzalı bir yapıya sahip olduğunu anlatmıştık. Zaman damgasının imzası, zaman damgası içerisindeki özet değerini ve damgalanma zamanını güvence altına almaktadır. Uygulamalar tarafından zaman damgasının imzasının kontrol edilmesi son derece önemlidir. Zaman damgasının imzasının bozuk olma durumunu incelemek için kök, alt kök , son kullanıcı sertifikası ve iptal bilgileri geçerli bir sertifika hiyeararşisi ile imzası bozuk cevaplar veren bir zaman damgası yapısı oluşturduk. Hatalı senaryonun yalnızca zaman damgası kaynaklı olmasını sağlamak istediğimiz için, zaman damgası ile ilgili bütün senaryolarda geçerli olarak ürettiğimiz hiyerarşiyi kullandık. Adobe Reader ile geçersiz bir

zaman damgası ile imza oluşturmaya çalıştığımızda Reader'ın beklediğimiz gibi imza oluşturmadığını gördük.

3.1.4.2 Süresi Dolmuş Zaman Damgası Sertifikası

Zaman damgalarının da (geçerli bir kök tarafından yayınlanmış) sertifikalarının bulunduğundan ve sertifikalarının da zaman damgası cevabına konduğundan bahsetmiştik. Bu senaryoda yine tek hata zaman damgasının geçerlilik zamanında olacak şekilde yapımızı kurduk. Adobe Reader'a imza oluşturma testi yaptık. Reader'ın beklediğimiz gibi imza oluşturmadığını gördük.

3.1.4.3 İmzası Bozuk Zaman Damgası Sertifikası

Zaman Damgası sertifikasının imzasının bozuk olması durumunu incelemek adına sertifikasının imzası bozuk olan bir zaman damgası sunucusu oluşturduk ve belirlediğimiz adresten hizmet vermesini sağladık. Yaptığımız testde; Adobe Reader'ın, imzası bozuk zaman damgası sertifikası kullanılarak imza oluşturulmasına izin vermediğini tespit ettik.

3.1.4.4 İptal Olmuş Zaman Damgası Sertifikası

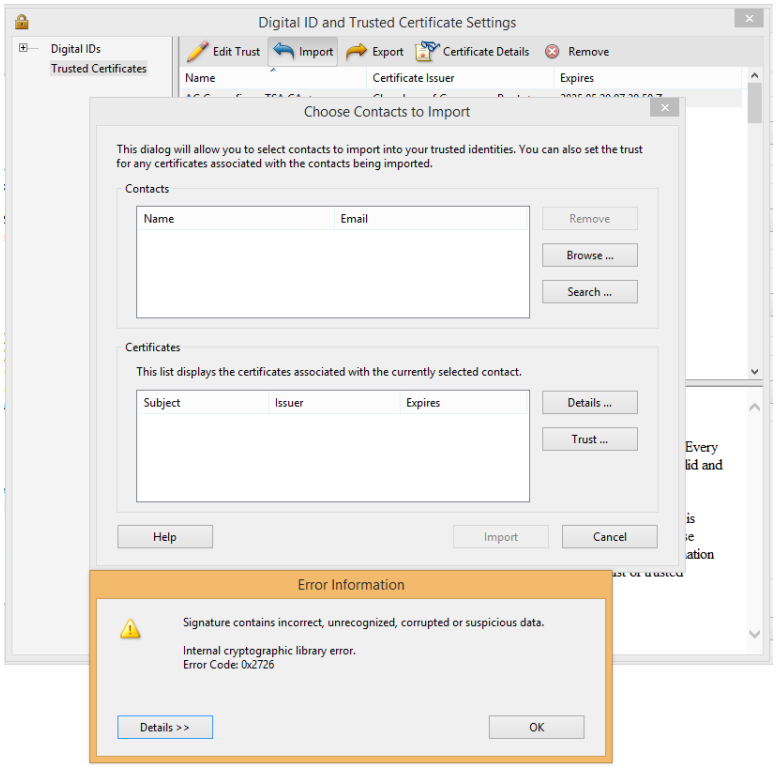
Zaman damgası sertifikasının iptal olma durumu da uygulamalar tarafından kontrol edilmesi gereken bir durumdur. Bu durumu incelemek adına bir zaman damgası sunucusu oluşturduk ve ürettiğimiz SİL'e zaman damgasının iptal bilgisini ekledik. İmza oluşturma testleri sırasında bu iptalin Reader tarafından yakalanmasını ve imza oluştrulmasına izin vermemesini bekliyoruz. Testimiz sonucunda gördüğümüz üzere Reader beklenildiği üzere imza oluşturmamaktadır.

3.1.4.5 Zaman Damgası Yayıncı ve İptal Bilgisi Senaryoları

Hatalı durumlar zaman damgasından kaynaklı olabileceği gibi, zaman damgasının yayıncısının sertifikası ve iptal bilgisi kaynaklı da olabilir.

3.1.4.6 Zaman Damgası Sertifikası İmzası Bozuk Kök Tarafından Üretilmiş

Zaman damgası sertifikasının imzası bozuk kök tarafından imzalanma durumunu incelemek adına imzası bozuk kökü sisteme güvenilir kök olarak eklemeye çalıştığımızda Şekil 3.4 de gösterildiği üzere imzası bozuk Root B nin sisteme eklenmesine Reader izin vermemiştir. Bu sebeple kökün bozuk olma durumunu Reader ile test edemedik.



Şekil 3.4: İmzası Bozuk Kökün Güvenilir Olarak Tanıtılmasında Verilen Hata

3.1.4.7 Zaman Damgası Sertifikası Süresi Dolmuş SİL'e Referans Veriyor

Zaman damgası sertifikasının süresinin dolma durumu Reader tarafından tespit edilmiştir. Reader beklenildiği üzere zaman damgası alma işlemini gerçekleştirmemiştir.

3.1.4.8 Zaman Damgası Sertifikası İmzası Bozuk SİL'e Referans Veriyor

Zaman damgası sertifikasının imzası bozuk SİL'e referans verme durumu Reader tarafından yakalnmıştır. Reader beklenildiği üzere zaman damgası alma işlemini gerçekleştirmemiştir.

3.2 İmza Doğrulama Senaryoları

Bir önceki bölümde imza oluşturma mekanizması için geliştirdiğimiz suiti ve testlerimizi anlatmıştık. Bu bölümdeyse imza doğrulama mekanizmaları için geliştirdiğimiz yapıdan ve testlerden bahsedeceğiz. İmza oluşturma ve imza doğrulama mekanizmalarının düzgün çalışmasının neden önemli olduğunu aktarmıştık. İmza oluşturma, imza doğrulama mekanizmalarında oluşabilecek güvenlik açıklıklarının büyük problemler doğurabileceklerinden bahsetmiştik. Bu sebeple imza oluştuma ve imza doğrulama suitlerimizi mümkün olduğunca bütün senaryoları içerecek şekilde kurguladığımızdan bahsetmiştik.

İmza oluşturma testlerinde kullanmak üzere bir çok son kullanıcı sertifikası, yayıncı sertifikası, SİL servisi, OCSP servisi, SİL, OCSP sertifikası, zaman damgası servisi, zaman damgası sertifikası oluşturduğumuzdan bahsetmiştik. Bu yapıları oluştururken her bir senaryoda tek ve eşsiz bir hata olacak şekilde modelimizi kurduğumuzu belirtmiştik. Bu yapıların bir önceki bölümde anlatılan kısımlarında durumlara göre hatalı senaryolar bulunmaktaydı. İmza oluşturma uygulamasını ilgili hatalı senaryoyu sağlayacak şekilde test etmiştik. Son kullanıcı sertifikası ile imza oluşturulup oluşturulmayacağının değerlendirmesi adına; son kullanıcı sertifikasından çıkılarak kök sertifikalara kadar yapılan çeşitli kontrollerde, ilgili hatanın yakalanıp imza oluşturulmasına izin verilmemesi gerektiğinden bahsetmiştik.

İmza doğrulama testlerini yapmak için de yazdığımız PAdES imza oluşturma programının yanında yine yukarıda oluşturduğumuz yapıları kullandık. İmza doğrulama mekanizmalarını test etmek için içerisinde tek bir hatalı durum olacak şekilde imzalı dosyalar oluşturduk. Bu imzalı dosyaları PAdES Baseline Profile'a uygun bir biçimde B-Type, LT-Type ve LTA-Type olarak üç ayrı imza tipi için ayrı suitler halinde oluşturduk. [2] İmza tiplerini Bölüm 2.1.1'de anlatmıştık.

Burada üç imza tipinde ayrı ayrı suitler oluşturma sebebimiz uygulamaların imza doğrulama mekanizmaların imza tipine özel hatalar verebilecek olmasıdır. İmza tiplerinden hatırlanacağı üzere imzada tipler geliştikçe yapıya modül modül bazı eklentiler gelmektedir, bir sonraki imza tipi aslında bir önceki imza tipini içeren daha gelişmiş bir halidir. Yani bizim imza doğrulama senaryolarında oluşturduğumuz B-Type imzalı dosyalarda bulunan senaryoların aynı LT-Type imza dosyaları için de geçerlidir. LT-Type imzalı dosyalar için olan senaryolar da LTA-Type için geçerlidir. LTA-Type'da ek olarak kendine özgü arşiv zaman damgası kaynaklı yeni senaryoları bulunmaktadır. Uygulamalar B-Type için imza doğrulama kısmında farklı bir hata mesajı verirken LT-Type da aynı senaryoda farklı bir hata mesajı verebilmektedir. Bu hatalı durumları anlatırken B-Type için senaryolar anlatılacak ve B-Type için olan senaryolar LT-Type ve LTA Type'da da oluşturulduğu için bu imza tipleri için alınan sonuçlarda paylaşılacaktır. Aynı şekilde LT-Type için olan hatalı durumlar anlatılırken de aslında aynı hatalı senaryolar LTA-Type için de oluşturulduğu için bu senaryoların 2 tip imzalı dosyadaki sonuçları paylaşılacaktır. Yalnızca LTA-Type a özgü olan senaryolardaysa LTA-Type için olan sonuçları paylaşılacaktır. İmza tiplerinin nasıl geliştikçe bir önceki imza tipini kapsadığını ve gelişmiş imza tipinin bir önceki imza tipindeki senaryoları içerdiğini imzalı dosya isimlerinin ve hatalarının bulunduğu Bölüm 4.3 inceleyebilirsiniz.

İmzalı dosyalarda son kullanıcı sertifikası, yayıncı sertifikası ve iptal değerleri bazlı hatalı senaryolar olabileceği gibi oluşturulmuş olan imza yapısına özgü senaryolar da olabilmektedir. İmza oluşturma ve imza doğrulama testlerinde bulunan: Son kullanıcı sertifikası, yayıncı sertifikası, iptal değerleri kaynaklı senaryolar aynı olsa da, uygulamanın imza oluşturma testlerinde yakaladığı bir senaryoyu imza doğrulama senaryosunda yakalamaması mümkündür. Tersi olarak da imza oluşturma testlerinde yakalamadığı bir senaryoyu imza doğrulama testlerinde yakalayabilmektedir. Ayrıca belirttiğim üzere imza doğrulama testleri için senaryolar her ne kadar aynı olsa da, yapılan işler bakımından imza oluşturma tarafından çok farklıdır. İmza doğrulama testlerinin yapılabilmesi için ilgili senaryoya sahip imzalı dosyaların oluşturulması gerekmektedir.

İmza doğrulama kısmında, imza oluşturma kısmında bahsettiğimiz senaryolara tekrar kısaca değinip sonrasında da Adobe Reader'ın imza doğrulama mekanizmasının test sonuçlarını paylaşacağız.

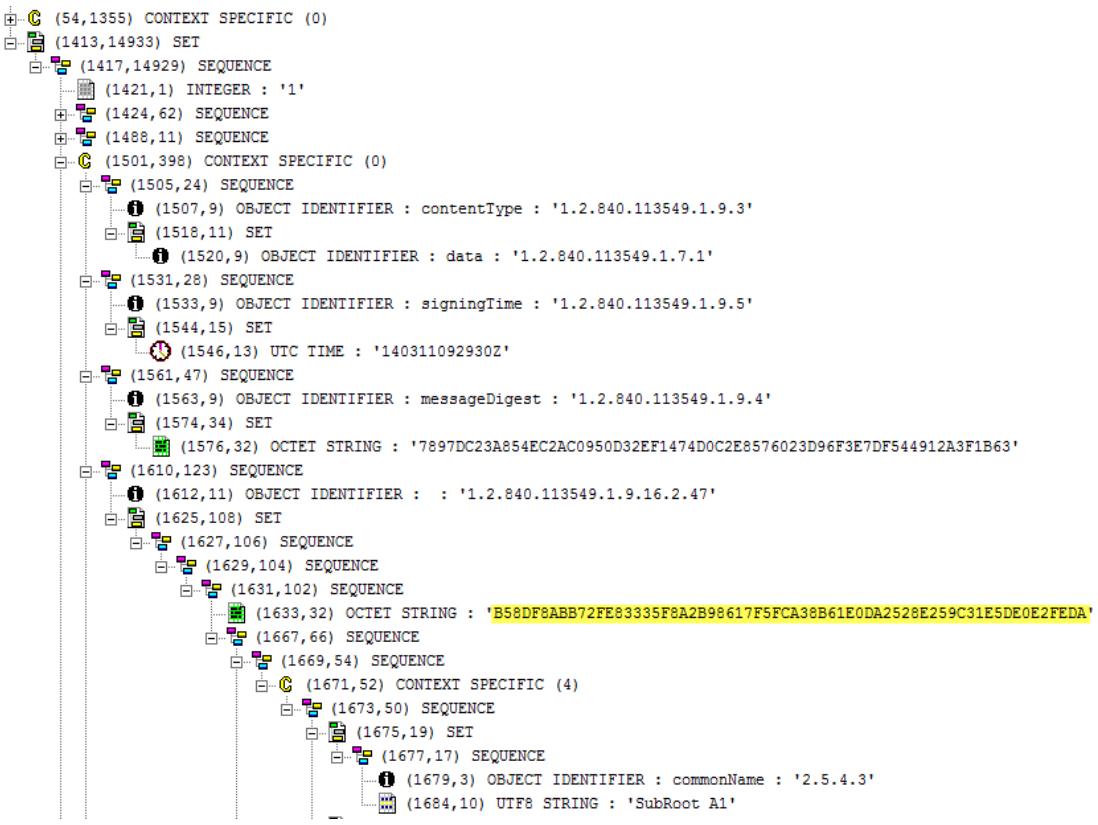
3.2.1 İmza Kaynaklı Senaryolar

Elektronik imzada, genellikle yalnızca hash değerinin imzalandığı düşünülmektedir. İmzalama işlemi bu şekilde bilinse de imzalama yalnızca dokümanın hash değerine yapılmamaktadır. İmzalama işlemi signed attributes denen alanlar birleştirildikten sonra bu alanların hash değerine yapılmaktadır. PAdES de zorunlu olan Signed Attributelar ESS-Signing Certificate, Message Digest, Content Type ve m Entry alanı içerisinde bulunan Signing Time dır. PAdES de message digest hesaplanırken Signature için ayrılmış alan dışında PDF in tamamı dahil edilmektedir. [33] Bu kısımda ilgili Signed Attributelarda ve imzada bozukluk olma durumlarını inceleyeceğiz.

3.2.1.1 ESS-Signing-Certificate İçeriği Bozuk

ESS-Signing-Certificate imzacı sertifikasının hash değerini içeren zorunlu bir signed attribute'dur. ESS-Signing-Certificate in imzaya dahil edilmesinin sebebi şudur: PKCS10 isteği ile açık anahtarın ESHS'ye iletildiği durumda (aynı/farklı) ESHS tarafından aynı açık anahtara sahip iki ayrı sertifika üretilebilir. [41] İmzaya eğer ESS-Signing-Certificate dahil edilmez imzayı bu iki imzacıdan hangisinin imzaladığı tespit edilemezdi ve bir imzacının oluşturduğu imza, diğer imzacı tarafından oluşturulmuş gibi gösterilebilir.

Senaryomuzda imzalı dosyamızın ESS-Signing-Certificate içeriği bozulmuştur. Test için kullacağımız imzalı dosyayı oluşturabilmek için Bölüm 3.5'deki gibi CMS yapının içerisine girilmiş ve CAdES yapı PDF'e gömülmeden ESS-Signing-Certificate içeriği tarafımızdan bozulmuştur, sonrasında imzalanacak özet değeri yeni ESS-Signing-Certificate göz önünde bulundurularak yeniden hesaplanmış ve kriptografik imza yeniden oluşturulmuştur. Yeni kriptografik imza, eski imza üzerine set edilmiştir. Böylelikle tek hatanın ESS-Signing-Certificate da olması sağlanmıştır. Çift hata (ESS-Signing-Certificate'ın bozulmasından kaynaklı imzanın da bozulması) oluşmasına izin verilmemiştir. Doğrulama mekanizmasından beklenen durum ESS-Signing-Certificate bozuk olduğu için, imzacı sertifikasının hash'iyle ESS-Signing-Certificate'in tutmaması ve imzanın doğrulanmamasıdır. Reader B-Type, LT-Type ve LTA-Type için hatayı yakalamış ve testi başarılı bir biçimde geçmiştir.

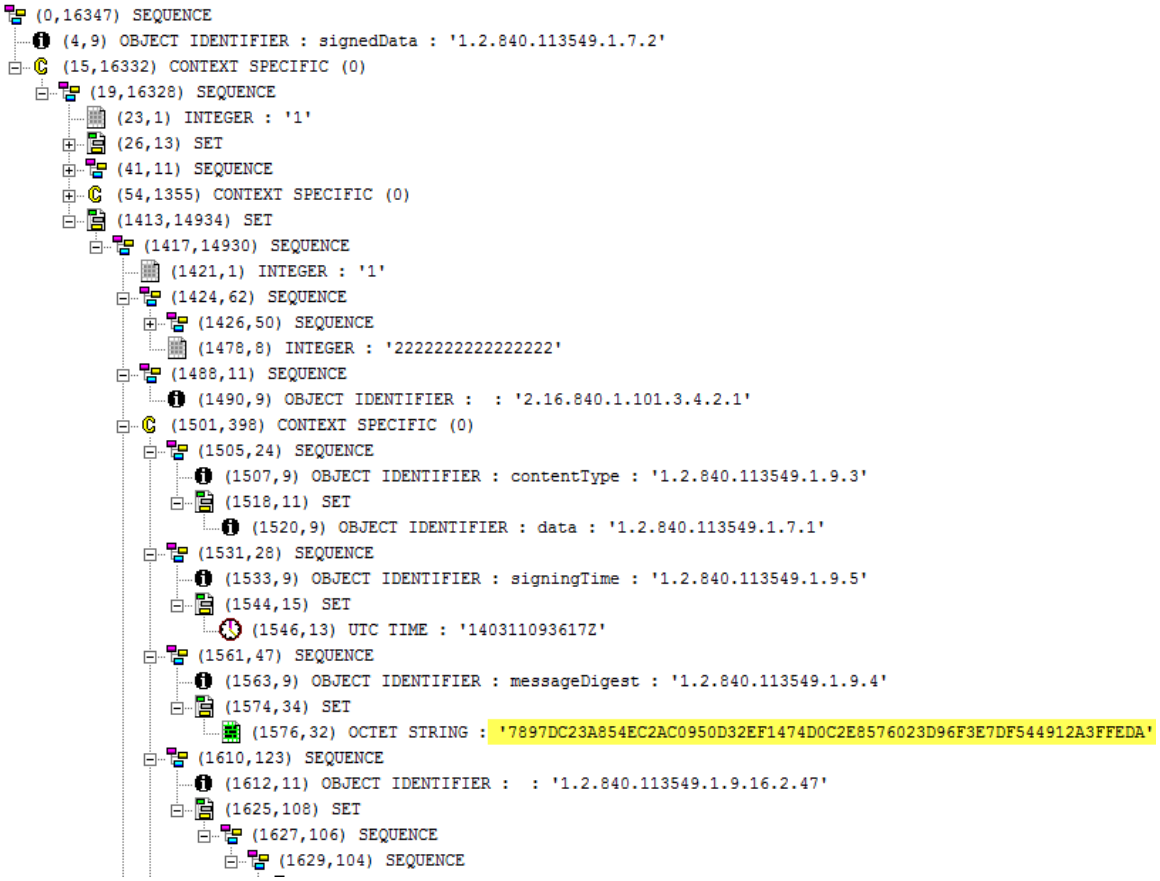


Şekil 3.5: CMS Yapıdaki ESS-Signing-Certificate Alanın ASN Görüntüsü

3.2.1.2 Message-Digest İmza Özelliği Bozulmuş

Message-Digest imzalanan içeriğin özet değeridir, senaryomuzda imzalı dosyamızın Message-Digest i bozulmuştur. İlgili imzalı dosyayı oluşturma esnasında CAdES imza değeri PDF'e gömülmeden araya girerek CAdES içerisinde bulunan Şekil 3.6 görüldüğü gibi Message-Digest'i bozarak, kriptografik imzayı yeni Message-Digest'e göre yeniden hesaplattık. Böylelikle yalnızca Message-Digest'in hatalı olma durumunu gerçekleştirmiş olduk.

Testimiz sırasında imza doğrulama mekanizmasından beklenilen durum Message-Digest i bozuk olduğu için imzanın doğrulanmasıdır. Reader testi başarılı bir biçimde B-Type, LT-Type ve LTA-Type için geçmiştir.



Şekil 3.6: CMS Yapıdaki Message-Digest Alanın ASN Görüntüsü

3.2.1.3 İmza Dosyasının İmzası Bozulmuş

Senaryomuzda imzalı dosyanın kriptografik imza değeri bozulmuştur. Testimiz için kullanacağımız imzalı dosyayı oluşturmak için PDF'in içerisine gömülmeden önce CAdES yapının içerisine ASN.1 [42–44] tool'unu kullanarak girdik ve kriptografik imza değerini bozduk.

İmzası bozuk imzalı dosya ile yaptığımız testlerde imzalı dosyanın imzasının bozuk olduğu Reader'ın imza doğrulama mekanizması tarafından yakalanmıştır ve Reader testi başarılı bir biçimde B-Type, LT-Type ve LTA-Type için geçmiştir.

3.2.2 Son Kullanıcı Sertifikası Kaynaklı Kontroller

3.2.2.1 Sertifika İmza Kontrolü

Bölüm 3.1.1.1 de bu senaryodan ve sertifika imza kontrolünün neden çok önemli olduğundan bahsetmiştik. İmza oluşturma testlerinde Reader'ın imzası bozuk bir sertifika ile kesinlikle imza oluşturmaya izin vermemesi gerekirken imza oluşturduğunu belirtmiştik.

İmza doğrulama testlerindeyse imzası bozuk sertifika ile oluşturduğumuz imzalı dosyayı Reader'a doğrulatarak imza doğrulama mekanizmasını test ettiğimizde; (beklenildiği üzere) Reader imzalı dosyayı doğrulamamıştır.

3.2.2.2 Sertifika Geçerlilik Kontrolü

Bölüm 3.1.1.2 da sertifikanın geçerlilik tarihinden ve geçerliliği bitmiş bir sertifika ile imza oluşturulmaması gerektiğinden bahsetmiştik. İmza doğrulama mekanizmasındaysa imzanın tipine göre geçerlilik zamanı değişmektedir. B-Type imzalı dosyalar doğrulandığı anki süredeki geçerliliklerine göre değerlendirilirler. LT-Type ve LTA-Type imzalı dosyalardaysa zaman damgası bulunduğu için imza oluşturulan tarih güvence altına alınmıştır ve imza oluşturulduğu tarihte değerlendirilecektir.

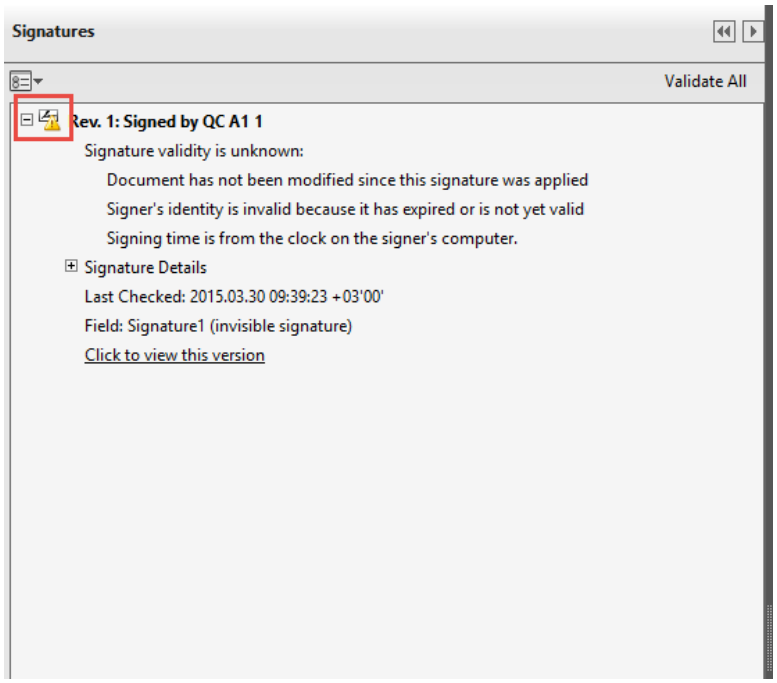
İmza doğrulama testlerinde B-Type süresi dolmuş sertifikayı doğruladığımızda imzalı dosyada herhangi bir zaman damgası bulunmadığı için doğrulama anına

göre değerlendirilecek ve doğrulanmayacaktır.

LT-Type ve LTA-Type imzalı dosyalar doğrulandığındaysa imza oluşturulma zamanına bakılacak ve imza oluşturulduğu yani zaman damgası alındığı andaki durumuna göre eğer geçerliyse geçerli olarak değerlendirilecek ve doğrulanacaktır.

Reader ile suitteki imzalı dosyalar ile yaptığımız testlerde B-Type dosyayı imzalayan sertifika geçerliliğini doldurduğu için imza beklenildiği gibi doğrulanmamıştır.

LT-Type ve LTA-Type daysa imzalı dosyalar eğer document time stamp alındığı anda sertifika geçerliyse doğrulanmış, zaman damgası alındığı zamanda sertifikanın süresi dolmuşsa doğrulanmamıştır. Fakat Şekil 3.7 de görüldüğü üzere ikon (icon) olarak invalid icon u yerine incomplete icon'u vermektedir. Süresi dolmuş bir sertifika ile oluşturulmuş imza için invalid şeklinde icon verilmelidir.



Şekil 3.7: Reader'ın Expired Sertifika İçin Uyarı İkonu Vermesi

3.2.2.3 Sertifika İptal Kontrolü

Sertifika iptal kontrolünü B-Type imzalı dosyalar ile yaptığımızda imza doğrulamasını doğrulama anına göre yapacaktır. B-Type imzalı dosyalar için kontrolün SİL'den de yapıldığı OCSP den de yapıldığı durumlarda doğrulamanın yapıldığı

anda sertifika iptal olarak görüldüğü için Reader beklenildiği gibi iptal olduğunu yakalamıştır.

LT-Type ve LTA-Type imzalı dosyalardaysa yine doküman zaman damgasının tarihine göre doğrulama yapılacaktır. OCSP ve SİL kullanılan senaryolarda eğer imza oluşturulma tarihinde sertifika iptal olmamışsa geçerli, iptal olmuşsa geçersiz olarak değerlendirilmelir. LT-Type ve LTA-Type imzalı dosyalar için geçerli ve geçersiz durumlar Reader doğru bir şekilde değerlendirilmiştir.

İmza oluşturmak için geliştiridiğimiz programla OCSP cevaplarını CertID SHA256 olarak alıp iptal değerlerine ekleyerek OCSP'li imzalı dosyalarımızı oluşturduk. İmza doğrulama testlerinde CertID'nin SHA2 olduğu imzalı dosyamızda; Reader'ın "LTV is not enabled" olarak uyarı verdiğini, yani Long Term Validation olan dosyayı beklenildiği üzere LTV olarak değerlendirmediğini farkettik. İncelediğimizde Reader'ın OCSP cevabında CertID'nin SHA2 olduğu durumlarda OCSP cevabını çözümleyemediğini gördük. CertID yapısında bir algorithm identifier bulunmaktadır, SHA1 in geçerliliğini kaybettiği günümüzde, algorithm identifier'ın daha güçlü bir algoritma olan SHA2 olarak set edildiği durumlarda uygulamalar tarafından set edilen algoritmanın kullanılabilmesi beklenmektedir. Reader'ın SHA2 olan Algorithm Identifier'a sahip OCSP cevaplarını çözümleyememesi, düzgün bir biçimde oluşturulmuş LT-Type ve LTA-Type imzalı dosyalar için iptal kontrolü yapamamasına ve imza doğrulama işlemini gerçekleştirememesine sebep olmaktadır ve bu durum düzeltilmesi gereken bir durumdur.

3.2.2.4 Sertifika Niteliklilik Kontrolleri

Bölüm 3.1.1.3'de nitelikli sertifikadan ve bir sertifikanın nitelikli sayılması için gerekli uluslar arası ve Türkiye bazlı gerekliliklerden bahsetmiştik. Bu alanların olmadığı sertifikalar ürettiğimizden bahsetmiştik. Bu sertifikalar kullanılarak yapılan imza oluşturma testlerinde Reader'ın QC kontrollerini dikkate almadığını farketmiştik. Test Suitimizin imza doğrulama kısmında kullanmak üzere bu sertifikalarla oluşturulmuş imzalı dosyalar bulunmaktadır. B-Type, LT-Type ve LTA-Type ile yaptığımız imza doğrulama testlerinde QC kontrollerinin imza doğrulama testlerinde de yapılmadığını fark ettik. Yani bir sertifika; güvenilir CA tarafından verilen bir logon sertifikası yada encryption sertifikası olursa ve imza oluşturma amacıyla kullanılırsa, oluşturulan imza Reader tarafından doğrulanacaktır ve sertifikanın imzalama sertifikası olmadığı, imzanın geçersiz

olduğu yakalanmayacaktır.

3.2.3 Yayıncı Sertifikası Kaynaklı Kontroller

3.2.3.1 Sertifika İmza Kontrolü

Sertifikanın imzasının bozuk olduğu senaryoyu imza oluşturma testlerinde de kullanmıştık, yayıncı sertifikasının bozuk olma durumu Reader tarafından yakalanmamış ve imza oluşturulmasına izin verilmişti.

İmza doğrulama kısmındaysa, Reader imzası bozuk yayıncı senaryosuna sahip B-Type imzalı dosyayı beklenildiği üzere doğrulamamaktadır. Ancak hata olarak imzanın bozuk olduğuna dair net bir hata vermek yerine ("This signer's identity is unknown because it has not been included in your list of trusted identities and none of it's parent certificates are trusted identities.") güvenilir bir zincir kurulamadığına dair daha az açıklayıcı bir hata mesajı dönmektedir. LT Type ve LTA-Type imzalı dosyaları doğrulama aşamasındaysa yine hatayı yakalamaktadır, fakat bu kez imzalı dosyalarda imzanın bozuk olduğuna dair düzgün bir hata dönmektedir.

3.2.3.2 Sertifika İptal Kontrolü

Alt kök sertifikasının iptal olma durumunu SİL ve OCSP olmak üzere iki iptal durumununda kullanıldığı senaryolarda inceledik.

B-Type imzalı dosyalarda SİL ve OCSP için Reader imzalı dosyayı beklenildiği üzere Reader, doğrulamadı fakat iptal olduğunu belirtmek yerine yine "zincir kurulamadı" ("This signer's identity is unknown because it has not been included in your list of trusted identities and none of it's parent certificates are trusted identities.") şeklinde net olmayan bir hata mesajı döndü.

LT-Type ve LTA-Type imzalı dosyalardaysa eğer iptal olma durumu imza oluşturulma zamanından sonraysa beklenildiği üzere SİL kullanılan ve OCSP kullanılan imzalı dosyaları doğruladı. Fakat yine imzalı dosyanın DSS alanında kayıtlı olan SHA2 OCSP cevabını anlayamadığı için imzalı dosyayı LTV olarak tanımadı. İmza zamanından önce sertifikanın iptal olduğu senaryolardaysa iptal

beklenildiği üzere Reader tarafından yakalandı ve iptal ile ilgili mesaj kullanıcıya verildi.

3.2.4 Son Kullanıcı İptal Değerleri Senaryoları

3.2.4.1 SİL Kaynaklı Senaryolar

1. **Süresi Dolmuş SİL**
2. **İmzası Bozuk SİL**

   Son kullanıcı sertifikasının iptal kontrolü için yukarıdaki senaryolar için SİL kullanılarak oluşturulmuş B-Type, LT-Type ve LTA-Type imzalı dosyaları Reader'a doğruladığımızda, Reader hatayı beklenildiği gibi yakalamış ve imzalı dosyayı doğrulamamıştır.

3.2.4.2 OCSP Kaynaklı Senaryolar

1. **OCSP Cevabının Süresi Dolmuş**
2. **OCSP Cevabının İmzası Bozuk**
3. **OCSP Sertifikasının Süresi Dolmuş**
4. **OCSP Sertifikasının İmzası Bozuk**

   Bölüm 3.1.3.1 de son kullanıcı sertifikası için alınan OCSP cevabı için oluşturduğumuz yukarıdaki senaryoları derinlemesine aktarmıştık. Reader'ın imza doğrulama mekanizmasına imzalı dosyaları doğrulattığımızda, beklenildiği gibi B-Type, LT-Type ve LTA-Type imzalı dosyalar için hatayı yakalamış ve imzalı dosyaları doğrulamamıştır.

5. **OCSP Sertifikası İptal Olmuş**

   İmza oluşturma testlerinde OCSP sertifikasının iptal kontrolünün yapıldığı evrede çekilen SİL'in son kullanıcı sertifikası için kullanılan SİL'le aynı olduğunu ve bu nedenle OCSP için indirilen SİL'in kullanılabileceğini belirtmiştik. Aynı şekilde imza doğrulama testlerinde de OCSP sertifikasının iptal olma durumlarının incelendiği B-Type, imzalı dosyanın doğrulanmasında yine SİL kullanılarak imzalı dosyalar doğrulanmıştır. Bu durum hatalı

bir durum değildir. Bu sebeple imzalı dosyalar doğrulansa dahi Reader testlerimizden geçmiştir.

6. **OCSP Response İçindeki Sertifika Farklı**

   OCSP response içerisinde cevabın yapısını ve mekanizmasını anlatmıştık. Oluşturduğumuz B-Type, LT-Type ve LTA-Type imzalı dosyalarda kullanılan OCSP cevabı farklı bir sertifika için verilen OCSP cevabıdır.

   İmza doğrulama testlerinde, Reader üç tip imzalı dosya için de hatayı yakalamış ve beklenildği üzere hatayı dönmüştir.

3.2.5 Yayıncı İptal Değerleri Senaryoları

Son kullanıcı sertifikaları için SİL ve OCSP senaryolarını incelemiştik. Bu bölümdeyse alt kök sertifikası için çekilen SİL ve OCSP'de problem olduğu durumları inceleyeceğiz. Bu durumları test etmek adına PAdES imza oluşturma programımızı kullanarak B-Type, LT-Type ve LTA-Type tipinde imzalı dosyalar oluşturduk. B-Type imzalı dosyalar imza tipleri bölümünde anlattığımız üzere içerisinde yine imza doğrulama için değerler içermemektedir. İlgili senaryoda kullanılan sertifikalar için cevap veren OCSP ve SİL sunucuları, ilgili senaryoya özel SİL ve OCSP cevaplarını dönmektedir. B-Type imzalı dosyalar doğrulanırken ilgili iptal değerleri kurduğumuz sunucular vasıtasıyla doğrulanma sırasında dönülmektedir. LT-Type ve LTA-Type imzalı dosyaları oluşturduğumuz sırada içerisine ilgili iptal bilgilerini de koyduk. İmza doğrulama testlerini yaparken imza tipinden bağımısız olarak aynı şekilde imza doğrulama mekanizmlarının cevap dönmesini bekliyoruz.

3.2.5.1 SİL Kaynaklı Senaryolar

1. **Süresi Dolmuş SİL**

2. **İmzası Bozuk SİL**

   Senaryolarına sahip B-Type imzalı dosyaları Reader'a doğrulattığımızda, Reader'ın beklediğimiz üzere imzalı dosyaları doğrulamadığını gördük. Fakat Reader Sertifika iptal kontrolü yapılamadığına dair bir hata vermek yerine "Güvenilir Zincir kurulamadı" şeklinde açık olmayan bir hata verdi.

LT-Type ve LTA-Type imzalı dosyalar ile yaprığımız imza doğrulama testlerinde de Reader'ın imzalı dosyaları beklenildiği üzere doğrulamadığını gördük, Reader LT-Type ve LTA-Type imzalı dosyaları doğruladığımızdaysa hatalı durumu düzgün bir biçimde kullanıcıya ilettiğini tespit ettik.

3.2.5.2 OCSP Kaynaklı Kontroller

1. **OCSP Cevabının Süresi Dolmuş**
2. **OCSP Cevabının İmzası Bozuk**
3. **OCSP Sertifikasının Geçerlilik Süresi Dolmuş**
4. **OCSP Sertifikasının İmzası Bozuk**

   Senaryolarına sahip B-Type imzalı dosyaları Reader'a doğrulattığımızda, Reader'ın beklediğimiz üzere imzalı dosyaları doğrulamadığını gördük. Fakat Reader Sertifika iptal kontrolü yapılamadığına dair bir hata vermek yerine "Güvenilir Zincir kurulamadı" şekilinde açık olmayan bir hata verdi. LT-Type ve LTA-Type imzalı dosyalar ile yaptığımız imza doğrulama testlerinde de Reader'ın imzalı dosyaları beklenildiği üzere doğrulamadığını gördük, Reader LT-Type ve LTA-Type imzalı dosyaları doğruladığımızdaysa hatalı durumu düzgün bir biçimde kullanıcıya ilettiğini tespit ettik.

5. **OCSP Sertifikasının İptal Olma Durumu**

   Senaryoya sahip imzalı dosyalar yalnızca B-Type için oluşturulmuştur. LT-Type ve LTA-Type için oluşturulmama sebebi OCSP için kullanılan SİL'in son kullanıcı için aynı SİL olmasıdır. B-Type için yaptığımız testlerde Reader OCSP sertifikası için indirdiği SİL'i son kullanıcı için kullanmış ve imzalı dosyayı doğrulamıştır. Bölüm 3.1.3.1 detaylı olarak anlattığımız üzere bu hatalı bir akış değildir. Bu sebeple Reader bu senaryo için testimizden geçmiştir.

3.2.6 Doküman Zaman Damgası Kaynaklı Durumlar

Bir önceki bölümde son kullanıcı sertifikası ve yayıncı sertifikasında oluşabilecek senaryolar incelenmiştir. Bu senaryolar B-Type, LT-Type ve LTA-Type'da oluşturulmuş ve testler her bir tip için yapılmıştır. Zaman damgası

kaynaklı durumlardaysa sadece LT-Type ve LTA-Type'da görülmesi mümkün senaryolardır. B-Type dosyalarda zaman damgası bulunmamaktadır. Bu sebeple bu bölümde testleri oluşturduğumuz LT-Type ve LTA-Type imzalı dosyalar ile yapmaya devam edeceğiz.

Bölüm 3.1.4 hatalı zaman damgaları kullanarak imzalı dosya oluşturma testlerini yapmıştık ve imza oluşturma mekanizmasını test etmiştik. Bu bölümdeyse oluşturuğumuz LT-Type ve LTA-Type imzalı dosyalarla imza doğrulama mekanizmasını test edeceğiz.

1. **İmzası Bozuk Zaman Damgasını**
2. **Süresi Dolmuş Zaman Damgası**
3. **İmzası Bozuk Zaman Damgası Sertifikası**
4. **Zaman Damgası Sertifikasının İmzası Bozuk Kök Tarafından Üretilme Durumu**

   Senaryolarına sahip LT-Type ve LTA-Type imzalı dosyaları kulllanarak Reader'ın imza doğrulama mekanizmasını test ettiğimizide Reader'ın imzalı dosyaları doğrulamadığı ve hatalı durumu düzgün bir biçimde ifade ettiğini gördük.

5. **Zaman Damgası Sertifikası İptal Olmuş**

   Senaryosuna sahip imzalı dosyaları doğruladığımızda zaman damgası sertifikası eğer imza zamanından önce iptal edilmişse imzalı dosyanın Reader tarafından doğrulanmadığını, imza oluşturulduktan sonra zaman damgası sertifikası iptal edilmişse beklenildiği üzere Reader tarfından doğrulandığını tespit ettik.

6. **Zaman Damgası Sertifikasının Süresi Dolmuş SİL'e Referans Verme Durumu**
7. **Zaman Damgası Sertifikasının İmzası Bozuk SİL'e Referans Verme Durumu**

   Senaryolarına sahip imzalı dosyaları imza doğrulama mekanizmasına doğrulattığımızda Reader'ın her iki tip imza içinde beklenildiği üzere doğrulamadığını ve hatayı düzgün bir biçimde bildirdiğini tespit ettik.

3.2.7 Arşiv Zaman Damgası Kaynaklı Durumlar

Dökuman zaman damgası kaynaklı senaryoları incelemiştik. Doküman zaman damgasında bulunan senaryolar arşiv zaman damgası için de gerçekleşebilmektedir. Bu sebeple hatalı durumlar arşiv zaman damgası kaynaklı olacak şekilde bu durumları sağlayacak LTA-Type yeni imzalı dosyaları yazdığımız imza oluşturma uygulamamızı kullanarak oluşturduk. İlgili senaryoların arşiv zaman damgasında olma durumunda da Reader'ın Bölüm 3.2.6 deki sonuçlarla aynı sonuçları verdiğini gördük. Bu sebeple bu bölümde arşiv zaman damgası için tekrardan testleri ve sonuçları paylaşmamaktayız.

3.3 Test Sonuçları Ve Değerlendirme

3.3.1 İmza Oluşturma Test Sonuçları

İmza oluşturma senaryoları ve imza doğrulama senaryoları bölümlerinde senaryoları ve Reader'ın senaryolar karşısındaki sonuçlarını, senaryoları aktardıkça paylaşmıştık. Bu bölümdeyse test sonuçlarını toplu bir şekilde paylaşıp, değerlendireceğiz. Tablo 3.1'de görüldüğü üzere Reader imzası bozuk sertifika ile imza oluşturulmasına izin vermiştir. Uygulamaların imzası bozuk sertifikalar ile imza oluşturmaya kesinlikle izin vermemesi gerekmektedir.

İmza oluşturma kısımlarında Reader'ın niteliklik kontrollerini yapmadığını gördük. Bu kontroller yalnızca nitelikli sertifikaların kullanılmasını sağlamak amacıyla yapılması gerekli kontrollerdir ve Reader nitelikli sertifikalar dışında sertifikalarla da çalışılması için bu şekilde bir kontrol koymamış olabilir. Yine de Reader'ın niteliklik kontrollerini [18, 19] yapabilecek şekilde geliştirilmesi iyi olacaktır. Reader imza oluşturma testlerinde hataya dair net bir hata dönmemiş her hatalı senaryoda imza oluşturulmadığına dair standart bir hata dönmüştür. Kullanıcıya imza oluşturmasını engelleyen durumun ne olduğuna dair net bir hata dönülmesi beklenmektedir. Tablo 3.1 da

X:Testi geçemeyen

OK: Testi başarılı bir biçimde geçen **Geçti:** Hata veren fakat net bir hata vermeyen

şeklinde ifade edilmiştir.

Çizelge 3.1: İmza Oluşturma Sonuçları

Senaryo	**Son Kullanıcı Sonucu**	**Alt Kök Sonucu**
Geçerli Sertifika SİL Kullanılmış	Geçti	Geçti
Geçerli Sertifika OCSP Kullanılmış	Geçti	Geçti
Süresi Dolmuş Sertifika	Geçti	Geçti
Niteliklik Kontrolleri (Opsiyonel)	X	X
Sertifikanın Üzerindeki ESHS İmzası Bozuk	X	X
SİL'de İptal Olmuş	Geçti	Geçti
Kontrol Edildiği SİL'in Geçerlilik Süresi Dolmuş	Geçti	Geçti
Kontrol Edildiği SİL'in Üzerindeki ESHS İmzası Bozuk	Geçti	Geçti
Kontrol Edildiği OCSP Cevabının Geçerlilik Süresi Dolmuş	Geçti	Geçti
Kontrol Edildiği OCSP Cevabı Üzerindeki ESHS İmzası Bozuk	Geçti	Geçti
Kontrol Edildiği OCSP Sertifikasnın İmzası Bozuk	Geçti	Geçti
Kontrol Edildiği OCSP Sertifikası İptal Edilmiş	Geçti	Geçti
Para Limiti "0" Olarak Eklenmiş (Opsiyonel)	X	X
Kullanım Kısıtlı Sertifika (Opsiyonel)	X	X
OCSP Sorgusu İçinde Sorgulanandan Farklı Sertifika İçin Cevap Dönen	Geçti	OK

İmza oluşturma kısmında zaman damgası ile yaptığımız testler sonucunda Reader bütün testlerden geçmiştir.

Çizelge 3.2: İmza Oluşturma Zaman Damgası Testleri

Senaryo	**ZD Sonuçları**
TSTInfo Özelliği Bozulmuş Zaman Damgası Cevabı	OK
İmzası Bozulmuş Zaman Damgası Cevabı	OK
Süresi Dolmuş Zaman Damgası Sertifikası	OK
İmzası Bozulmuş Zaman Damgası Sertifikası	OK
İptal Olmuş Zaman Damgası Sertifikası	OK
Yayıncısının Sertifikası Bozulmuş Zaman Damgası Sertifikası	OK
Süresi Dolmuş Zaman Damgası Sertifikası	OK

3.3.2 İmza Doğrulama Test Sonuçları

İmza doğrulama testlerinde Reader'dan aldığımız sonuçlar Tablo 3.3 de B-Type, LT-Type ve LTA-Type olmak üzere gösterilmektedir. İmza doğrulama testlerinde Reader bazı B-Type dosyalarda hataları tam olarak belirtmemiştir. Reader aynı hatalı durumu içeren LT-Type ve LTA-Type dosyalardaysa hataları net bir biçimde kullanıcıya bildirmektedir. Reader'ın B-Type için de hataları açık bir biçimde dönmesi beklenmektedir. Niteliklik kontrolleri ile ilgili de bir kontrol mekanizması imza doğrulama kısmında da konmamıştır. Ayrıca özel olarak ürettiğimiz ve testlerimizde uygulamalardan opsiyonel olarak kontrol etmesini beklediğimiz maddi limit ve kullanım kısıtı bulunan sertifikalarla oluşturulmuş imzalı dosyalar beklediğimiz üzere Reader tarafından denetlenmemiştir. Bu senaryolar çok istisnai senaryolardır ve uygulamalardan yapması beklenmemektedir. Çok daha özel Elektronik Belge Yönetim Sistemleri için evrakların imzalanması yapılırken maddi limit kontrolü yapacak şekilde uygulama hazırlanmışsa eğer bu PAdES uygulamalarını doğrulamak için kullanmak üzere bu dosyalar ve sertifikalar üretilmiştir. [45, 46] İmza doğrulama testlerinde Tablo 3.3 sonuçlar

X:Testi geçemeyen

OK: Testi başarılı bir biçimde geçen

Geçti: Hata veren fakat net bir hata vermeyen

şeklinde ifade edilmiştir.

Çizelge 3.3: İmza Doğrulama Sonuçları

Senaryo	**B-Type Son Kullanıcı Sonucu (SKS)**	**B-Type Alt Kök Sonucu (AKS)**	**LT Type SKS**	**LT Type AKS**	**LT Type SKS**	**LTA Type AKS**
Geçerli Sertifika SİL Kullanılmış	OK	OK	OK	OK	OK	OK
Geçerli Sertifika OCSP Kullanılmış	OK	OK	OK	OK	OK	OK
ESS-Signing Certificate İçeriği Bozulmuş	OK	OK	OK	OK	OK	OK
Message Digest İmza Özelliği Bozulmuş	OK	OK	OK	OK	OK	OK
İmza Dosyasının İmzası Bozulmuş	OK	OK	OK	OK	OK	OK
Süresi Dolmuş Sertifika	OK	-	OK	-	OK	-
Niteliklik Kontrolleri (Opsiyonel)	X	X	X	X	X	X
Sertifikanın Üzerindeki ESHS İmzası Bozuk	OK	Geçti	OK	OK	OK	OK
SİL'de İptal Olmuş	OK	Geçti	OK	OK	OK	OK
Kontrol Edildiği SİL'in Geçerlilik Süresi Dolmuş	OK	Geçti	OK	OK	OK	OK
Kontrol Edildiği SİL'in Üzerindeki ESHS İmzası Bozuk	OK	Geçti	OK	OK	OK	OK
OCSP'de İptal Olmuş	OK	OK	OK	OK	OK	OK
Kontrol Edildiği OCSP Cevabının Geçerlilik Süresi Dolmuş	OK	Geçti	OK	OK	OK	OK
Kontrol Edildiği OCSP Cevabı Üzerindeki ESHS İmzası Bozuk	OK	Geçti	OK	OK	OK	OK
Kontrol Edildiği OCSP Sertifikasnın İmzası Bozuk	OK	Geçti	OK	OK	OK	OK
Kontrol Edildiği OCSP Sertifikası İptal Edilmiş	OK	Geçti	OK	OK	OK	OK

Çizelge 3.3: İmza Doğrulama Sonuçları (Devam)

Senaryo	**B-Type Son Kullanıcı Sonucu (SKS)**	**B-Type Alt Kök Sonucu (AKS)**	**LT Type SKS**	**LT Type AKS**	**LT Type SKS**	**LTA Type AKS**
Para Limiti "0" Olarak Eklenmiş (Opsiyonel)	X	X	X	X	X	X
Kullanım Kısıtlı Sertifika (Opsiyonel)	X	X	X	X	X	X
OCSP Sorgusu İçinde Sorgulanandan Farklı Sertifika İçin Cevap Dönen	OK	OK	OK	OK	OK	OK
OCSP CertID SHA2 Olan İmzalı Dosya	-	-	X	X	X	X
ZD TSTInfo İçeriğinde MessageImprint bozuk	-	-	OK	OK	OK	OK
ZD İmzası Bozuk	-	-	OK	OK	OK	OK
ZD Geçerilik Süresi Dolmuş	-	-	OK	OK	OK	OK
ZD Sertifikası İmzası Bozuk	-	-	OK	OK	OK	OK
ZD Sertifikası İptal Olmuş	-	-	OK	OK	OK	OK
ZD Sertifikası İmzası Bozuk Kök Tarafından Üretilmiş	-	-	OK	OK	OK	OK
ZD Sertifikası Süresi Dolmuş SİL'e Referans Veriyor	-	-	OK	OK	OK	OK
ZD Sertifikası İmzası Bozuk SİL'e ReferansVeriyor	-	-	OK	OK	OK	OK

4. TASARIM

Bu bölümde "PAdES Test Suit'de" dokümanında kullanılan test paketini tanımlayacağız. Bu bölümde testlerde kullanılan kök, alt kök sertifikaları, NES'ler, OCSP'ler, SİL dosyaları ve zaman damgalarının özellikleri ilgili Tablo'larda verilmiştir. Dokümanda imza doğrulamada kullanılacak olan test amaçlı oluşturulmuş imzalı dosyaların özellikleri de tanımlanmıştır

Bu bölümde tanımlanan kök, alt kök, zaman damgası ve OCSP sertifikaları, NES Personal Information Exchange (PFX) dosyaları [15] , SİL dosyaları ve imzalı dosyalar test paketi içinde mevcuttur. Ayrıca kök, alt kök sertifikaları ve SİL dosyalarına Kamu Sertifikasyon Merkezi'nin (KSM) adreslerinden erişilebilmektedir. 10 adet Zaman Damgası (ZD) sunucusu ve 15 adet OCSP sunucusu belirtilen adreslerden sürekli hizmet vermektedir. NES, sertifika zincir yapısındaki kök/alt kök sertifikaları, OCSP ve zaman damgası sertifikaları, SİL, OCSP cevapları ve zaman damgalarında hatalı bir durum olması halinde imza doğrulamalarının uygulamada yapılamaması beklenmektedir.

Oluşturulan tüm test sertifikaları aksi belirtilmedikçe SHA-256 özet algoritması ve RSA-2048 bit şifreleme algoritması kullanılarak oluşturulmuştur. Oluşturulan imzalı dosyalarda, SİL, zaman damgası ve OCSP cevaplarında aksi belirtilmedikçe SHA-256 özetleme algoritması kullanılmıştır. [12, 47–50]

Test sistemindeki sertifikalar için oluşturulan hiyerarşik sertifika zincir yapıları da bu dokümanda verilmiştir.

4.1 Test Sistemi Hiyerarşik Sertifika Zincir Yapısı

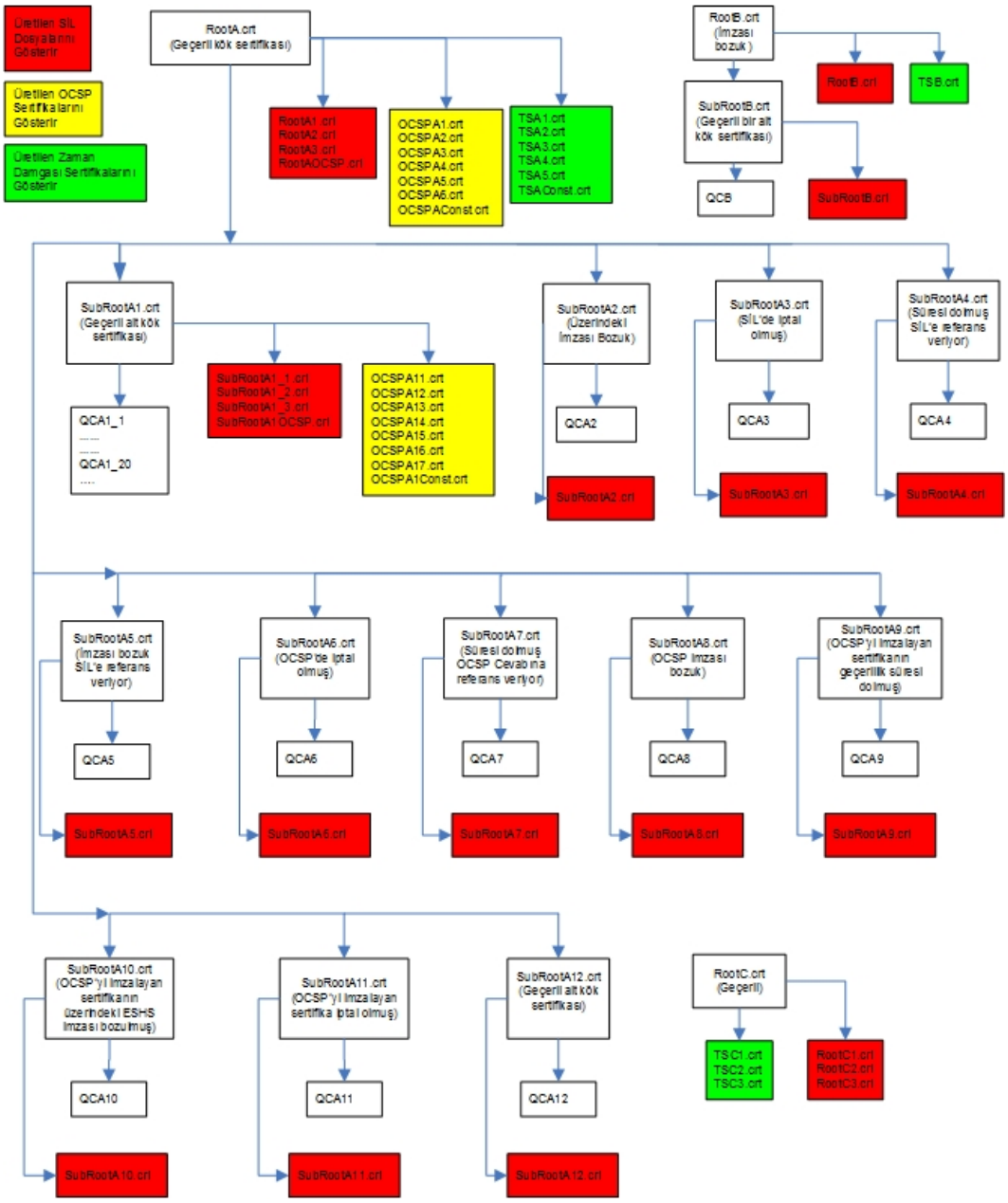
Testlerde kullanılan sertifikalar için hiyerarşik kök sertifika zincir yapısı oluşturulmuştur Şekil 4.1 Zincir yapısında tanımlanan her sertifika için bir hata durumu oluşturulmuştur. Hata durumu içermeyen geçerli sertifikalar da sistemde tanımlıdır.

Test sistemi planlanırken aşağıdaki kurallara uyulmuştur:

1. Her bir zincir yapısında sadece bir hata vardır, bir zincirde birden fazla hata bulunmasına izin verilmemektedir.
2. Kök sertifikalarının iptal ve geçerlilik süresi kontrolleri yapılmamaktadır.
3. Sertifikaların iptal kontrollerinin yapılacağı SİL'ler sertifikayı imzalayan kök/alt kök tarafından yayınlanmaktadır.
4. Sertifikaların iptal kontrollerinin yapılacağı OCSP sunucu sertifikaları, sertifikayı imzalayan kök/alt kök tarafından yayınlanmaktadır.
5. Zaman Damgası sunucu sertifikalarının iptal kontrolleri sadece SİL üzerinden yapılmaktadır.
6. OCSP sertifikalarının içeriğinde "OCSPNoCheck" alanı bulunmaktadır ve iptal kontrolleri yapılmamaktadır. Ancak OCSP sertifikaları iptal kontrolleri için tanımlanan testler için "OCSPNoCheck" alanı tanımlanmamış OCSP sertifikalarının iptal kontrolleri SİL üzerinden yapılmaktadır.
7. Zaman Damgası sunucu sertifikaları kök sertifikalar tarafından yayınlanmaktadır.
8. İmza dosyası içeriğinde zaman damgasına ait kök sertifikası mevcuttur.
9. İmza dosyasına yeni bir zaman damgası eklenirken dosya içeriğindeki bir önceki zaman damgasına ait SİL, imza dosyasına eklenmektedir.

4.2 Test Sisteminde Kullanılan Sertifikalar, SİL'ler, ZD ve OCSP Sunucuları

4.2.1 Kök, Alt Kök Sertifikaları ve NES'ler



Şekil 4.1: Testlerde Kullanılan Sertifikaların Hiyerarşik Zincir Yapısı

Çizelge 4.1: Kök, Alt Kök Sertifikaları ve NES'lerin Özellikleri

Kök Sertifika Dosya İsmi	**Kökten Üretilen Alt Kök Sertifika Dosya İsmi**	**Alt Kökten Üretilen NES PFX Dosya İsmi**
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_1.pfx, (Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_2.pfx, (Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_3.pfx, ("anahtar kullanım (keyusage)" uzantısı içeriğinde inkar edilemezlik (non-repuduation) özelliği olmayan NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_4.pfx, ("sertifika,ilkeleri (CertificatePolicies)" uzantısının içeriğinde "kullanıcı uyarısı,(user notice)" alanında aşağıdaki ibarenin olmadığı NES: "Bu sertifika, 5070,sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır.")
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_5.pfx, ("nitelikli elektronik sertifika ibareleri (Qualified Certificate Statement)" uzantısının içeriğinde yer alan "ibare tanımlayıcı(statementid)" alanında ETSI TS 101 862'de tanımlanan "idetsiqcs-QcCompliance" ibaresine ait OID bulunmayan NES. OID: 0.4.0.1862.1.1)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_6.pfx,("nitelikli elektronik sertifika ibareleri (Qualified Certificate Statement)" uzantısının içeriğinde yer alan "ibare tanımlayıcı (statementid)" alanında BTK tarafından belirlenen ibareye ait OID bulunmayan NES. OID: 2.16.792.1.61.0.1.5070.1.1)

Çizelge 4.1: Kök, Alt Kök Sertifikaları ve NES'lerin Özellikleri (Devam)

Kök Sertifika Dosya İsmi	**Kökten Üretilen Alt Kök Sertifika Dosya İsmi**	**Alt Kökten Üretilen NES PFX Dosya İsmi**
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_7.pfx,("nitelikli elektronik sertifika ibareleri (Qualified Certificate Statement)" uzantısının içeriğinde yer alan "ibare bilgisi" (statementInfo) alanında aşağıdaki ibarenin olmadığı NES: "Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır.")
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_8.pfx,(Süresi dolmuş NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_9.pfx,(Üzerindeki ESHS imzası bozuk)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_11.pfx,(OCSP'de iptal olmuş)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_12.pfx,(Kontrol edildiği SİL'in geçerlilik süresi dolmuş)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_13.pfx,(Kontrol edildiği SİL'in üzerindeki ESHS imzası bozuk)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_14.pfx,(Kontrol edildiği OCSP cevabının geçerlilik süresi dolmuş)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_15.pfx,(Kontrol edildiği OCSP cevabı üzerindeki ESHS imzası bozuk)

Çizelge 4.1: Kök, Alt Kök Sertifikaları ve NES'lerin Özellikleri (Devam)

Kök Sertifika Dosya İsmi	**Kökten Üretilen Alt Kök Sertifika Dosya İsmi**	**Alt Kökten Üretilen NES PFX Dosya İsmi**
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_17.pfx,(Kontrol edildiği OCSP sertifikasının süresi dolmuş)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_18.pfx,(Kontrol edildiği OCSP sertifikası iptal olmuş)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_19.pfx,(Para limiti "0" olarak eklenmiş sertifika)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_20.pfx,(Kullanım kısıtlı sertifika: " nitelikli elektronik sertifika ibareleri (Qualified Certificate Statement)" uzantısının içeriğinde yer alan "ibare tanımlayıcı (statementid)" alanında kullanım kısıtı ibaresine ait OID (2.16.792.1.2.1.1.5.7.2.9999) ve "ibare bilgisi (statementInfo)" alanında "Test kullanım kısıtı" bulunan sertifika)
RootA.crt (Geçerli kök sertifikası)	SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA1_21.pfx,(OCSP sorgusunun içinde sorgulanandan farklı bir sertifika mevcut)

Çizelge 4.1: Kök, Alt Kök Sertifikaları ve NES'lerin Özellikleri (Devam)

Kök Sertifika Dosya İsmi	**Kökten Üretilen Alt Kök Sertifika Dosya İsmi**	**Alt Kökten Üretilen NES PFX Dosya İsmi**
RootA.crt (Geçerli kök sertifikası)	SubRootA2.crt, (Üzerindeki kök ESHS imzası bozuk) SubRootA1.crt, (Geçerli alt kök sertifikası)	QCA2.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA3.crt,(SİL'de iptal olmuş)	QCA3.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA4.crt,(Süresi dolmuş SİL'e referans veriyor)	QCA4.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA5.crt,(İmzası bozuk SİL'e referans veriyor)	QCA5.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA6.crt, (OCSP'de iptal olmuş)	QCA6.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA7.crt,(Süresi dolmuş OCSP Cevabına referans veriyor)	QCA7.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA8.crt, (İmzası bozuk OCSP'ye referans veriyor)	QCA8.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA9.crt,(Referans verdiği OCSP'yi imzalayan sertifikanın geçerlilik süresi dolmuş)	QCA9.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA10.crt, (Referans verdiği OCSP'yi imzalayan sertifikanın üzerindeki ESHS imzası bozulmuş)	QCA10.pfx,(Geçerli NES)

Çizelge 4.1: Kök, Alt Kök Sertifikaları ve NES'lerin Özellikleri (Devam)

Kök Sertifika Dosya İsmi	**Kökten Üretilen Alt Kök Sertifika Dosya İsmi**	**Alt Kökten Üretilen NES PFX Dosya İsmi**
RootA.crt (Geçerli kök sertifikası)	SubRootA11.crt, (Referans verdiği OCSP'yi imzalayan sertifika iptal olmuş)	QCA11.pfx,(Geçerli NES)
RootA.crt (Geçerli kök sertifikası)	SubRootA12.crt,(OCSP'ye referans veren geçerli alt kök sertifikası)	QCA12.pfx,(Geçerli NES)
RootB.crt (İmzası bozuk kök sertifikası)	SubRootB.crt,(Geçerli alt kök sertifikası)	QCB.pfx,(Geçerli NES)
RootC.crt, (Geçerli)	YOK	YOK

4.2.2 OCSP Sunucuları

Testte kullanılan OCSP sunucularına ait sertifikalar, sunucuların ürettikleri OCSP cevaplarının özellikleri ve OCSP'de iptal konumunda olan sertifikalar aşağıdaki tabloda verilmiştir. Sertifikanın iptal tarihi OCSP'de iptal konumunda olan sertifikanın geçerlilik başlangıcından ne kadar süre sonra iptal edildiğini gösterir.

Testte kullanılan OCSP sunucularının erişim bilgileri aşağıda verilmiştir:

OCSPA1 : http://ocspsA1.test2.kamusm.gov.tr

OCSPA2 : http://ocspsA2.test2.kamusm.gov.tr

OCSPA3 : http://ocspsA3.test2.kamusm.gov.tr

OCSPA4 : http://ocspsA4.test2.kamusm.gov.tr

OCSPA5 : http://ocspsA5.test2.kamusm.gov.tr

OCSPA6 : http://ocspsA6.test2.kamusm.gov.tr

OCSPAConst : http://ocspsAConst.test2.kamusm.gov.tr

OCSPA11 : http://ocspsA11.test2.kamusm.gov.tr

OCSPA12 : http://ocspsA12.test2.kamusm.gov.tr

OCSPA13 : http://ocspsA13.test2.kamusm.gov.tr

OCSPA14 : http://ocspsA14.test2.kamusm.gov.tr

OCSPA15 : http://ocspsA15.test2.kamusm.gov.tr

OCSPA16 : http://ocspsA16.test2.kamusm.gov.tr

OCSPA17 : http://ocspsA17.test2.kamusm.gov.tr

OCSPA1Const : http://ocspsA1Const.test2.kamusm.gov.tr

Çizelge 4.2: OCSP Sunucu ve Sertifikalarının Özellikleri

OCSP Sertifikasını İmzalayan	**OCSP Sertifikası**	**OCSP Özelliği**	İptal Konumunda Olan Sertifikalar
RootA.crt	OCSPA1.crt	Geçerli	SubRootA6.crt
RootA.crt	OCSPA2.crt	İmza zamanında süresi dolmuş OCSP,cevabı üretiyor	-
RootA.crt	OCSPA3.crt	İmzası bozuk OCSP cevabı üretiyor	-
RootA.crt	OCSPA4.crt	OCSP sertifikasının geçerlilik,süresi dolmuş	-
RootA.crt	OCSPA5.crt	OCSP sertifikasının üzerindeki ESHS imzası bozuk	-
RootA.crt	OCSPA6.crt	OCSP sertifikası SİL'de iptal olmuş	-
SubRootA1.crt	OCSPAConst.crt	OCSP 30 Mayıs 2013 saat 11:00 için sabit cevap dönüyor	-
SubRootA1.crt	OCSPA11.crt	Geçerli	QCA1_11.crt

Çizelge 4.2: OCSP Sunucu ve Sertifikalarının Özellikleri (Devam)

OCSP Sertifikasını İmzalayan	**OCSP Sertifikası**	**OCSP Özelliği**	İptal Konumunda Olan Sertifikalar
SubRootA1.crt	OCSPA12.crt	İmza zamanında süresi dolmuş OCSPcevabı üretiyor	-
SubRootA1.crt	OCSPA13.crt	İmzası bozuk OCSP cevabı üretiyor	-
SubRootA1.crt	OCSPA14.crt	OCSP sertifikasının geçerlilik süresi dolmuş	-
SubRootA1.crt	OCSPA15.crt	OCSP sertifikasının üzerindeki ESHS imzası bozuk	-
SubRootA1.crt	OCSPA16.crt	OCSP sertifikası SİL'de iptal olmuş	-
SubRootA1.crt	OCSPA17.crt	OCSP cevabı sabit olarak QCA1_2.crt için üretiliyor	-
SubRootA1.crt	OCSPA1Const.crt	OCSP 30 Mayıs 2013 saat 11:00 için sabit cevap dönüyor	-

4.2.3 ZD Sunucuları

Testte kullanılan Zaman Damgası sunucularına ait sertifikalar ve sunucuların ürettikleri zaman damgalarının özellikleri aşağıdaki tabloda verilmiştir. ZD sunucularına ait sertifikaların iptal kontrolleri sertifikayı veren ESHS kök sertifikasının ürettiği SiL'ler üzerinden yapılacaktır. ZD sunucularının erişim bilgileri aşağıda verilmiştir:

TSA1 : http://zdsA1.test2.kamusm.gov.tr

TSA2 : http://zdsA2.test2.kamusm.gov.tr

TSA3 : http://zdsA3.test2.kamusm.gov.tr

TSA4 : http://zdsA4.test2.kamusm.gov.tr

TSA5 : http://zdsA5.test2.kamusm.gov.tr

TSB : http://zdsB.test2.kamusm.gov.tr

TSC1 : http://zdsC1.test2.kamusm.gov.tr

TSC2 : http://zdsC2.test2.kamusm.gov.tr

TSC3 : http://zdsC3.test2.kamusm.gov.tr

TSACONST : http://zdsAconst.test2.kamusm.gov.tr

Tüm sunuculara erişim için kullanıcı adı ve parola bulunmamaktadır.

Çizelge 4.3: ZD Sunucu ve Sertifikalarının Özellikleri

Zaman Damgası Sertifikasını İmzalayan	**Zaman Damgası Sertifikası**	**ZD Özelliği**
RootA.crt	TSA1.crt	Geçerli
RootA.crt	TSA2.crt	ZD imzası bozuk
RootA.crt	TSA3.crt	ZD sertifikasının geçerlilik süresi dolmuş
RootA.crt	TSA4.crt	ZD sertifikasının üzerindeki ESHS imzası bozuk
RootA.crt,.crt	TSA5.crt	ZD sertifikası iptal olmuş
RootA.crt	TSACONST.crt	30 Mayıs 2013 saat 11:00 için zaman dönüyor
RootB.crt	TSB.crt	Kök sertifikasının imzası bozuk
RootC.crt	TSC1.crt	Geçerli
RootC.crt	TSC2.crt	ZD sertifikası iptal kontrolünün yapıldığı SİL'in geçerlilik süresi dolmuş
RootC.crt	TSC3.crt	ZD sertifikası iptal kontrolünün yapıldığı SİL'in imzası bozuk

4.2.4 SİL'ler

Testte kullanılan ve SİL üreten ESHS sertifikaları, ürettikleri SİL dosya isimleri, üretilen SİL'lerin özellikleri, SİL içinde iptal konumunda olan sertifikalar ve iptal tarihleri aşağıdaki tabloda verilmiştir. OCSP sunucular da SİL üzerinden kontrol yapıp hizmet vereceğinden, OCSP sunucuların iptal kontrolü yaptığı SİL'ler de ayrıca belirtilmiştir. SİL'ler http://depo.test2.kamusm.gov.tr/ web adresinden yayınlanmaktadır. SİL'lere erişim web adresinin sonuna tabloda belirtilen SİL dosya isminin yazılması ile sağlanacaktır. Örn: http://depo.test2.kamusm.gov.tr/RootA1.crl

4.2.5 Testlerde Kullanılan Sertifikaların Profilleri

Kök, Alt Kök, OCSP ve zaman damgası sertifikaları ile NES'lerin geçerlilik süreleri, sertifika içeriğinde (CRLDistributionPoints, AuthorithyInfoAccess sertifika eklentileri) yazılan üst kök sertifika erişim bilgileri, iptal kontrolünün yapılacağı SİL/OCSP ile ilgili bilgiler ve sertifikaların iptal geçerlilik durumu aşağıdaki tablolarda verilmektedir.

Sertifika içeriğine yazılacak olan üst kök sertifika erişim bilgileri aşağıda verilen KSM web adresinin sonuna tabloda belirtilen sertifika dosya isminin yazılması ile oluşturulmuştur. Örn: http://depo.test2.kamusm.gov.tr/RootA.crt.

Sertifika içeriğinde SİL dosya bilgisi ve/veya OCSP erişim bilgilerinden tabloda verilenler mevcuttur.

Sertifika içeriğine yazılacak olan SİL erişim bilgileri aşağıda verilen KSM web adresinin sonuna tabloda belirtilen SİL dosya isminin yazılması ile oluşturulmuştur. Örn: http://depo.test2.kamusm.gov.tr/RootA1.crl.

Sertifika içeriğine yazılacak olan OCSP erişim bilgileri aşağıda verilen KSM web adresinin başına tabloda belirtilen OCSP servis isminin yazılması ile oluşturulmuştur. Örn: http://ocspsA1.test2.kamusm.gov.tr.

Çizelge 4.4: SİL Dosyalarının Özellikleri

SİL Sertifikasını İmzalayan	**SİL Dosya İsmi**	**SİL Özelliği**	**İptal Konumunda Olan Sertifikalar**
RootA.crt	RootA1.crl	Geçerli	SubRootA3.crt, OCSPA6.crt, TSA5.crt
RootA.crt	RootA2.crl	İmza zamanında süresi dolmuş	-
RootA.crt,	RootA3.crl	Üzerindeki ESHS imzası bozulmuş	-
RootA.crt	RootAOCSP.crl	Geçerli (OCSP'de iptal olan sertifikalar)	SubRootA6.crt
RootB.crt	RootB.crl	Geçerli	-
RootC.crt	RootC1.crl	Geçerli	-
RootC.crt	RootC2.crl	İmza zamanında süresi dolmuş	-
RootC.crt	RootC3.crl	Üzerindeki ESHS imzası bozulmuş	-
SubRootA1.crt	SubRootA1_1.crl	Geçerli	QCA1_10.crt, OCSPA1_6.crt
SubRootA1.crt	SubRootA1_2.crl	İmza zamanında süresi dolmuş	-
SubRootA1.crt	SubRootA1_3.crl	Üzerindeki ESHS imzası bozulmuş	-
SubRootA1.crt	SubRootA1OCSP.crl	Geçerli (OCSP'de iptal olan sertifikalar)	QCA1_11.crt
SubRoot {A2,.,A12}.crt	SubRoot {A2,.,A12}.crl,	Geçerli	-
SubRootB.crt	SubRootB.crl	Geçerli	-

Çizelge 4.5: Testlerde Kullanılan Kök ve Alt kök Sertifikaları

Sertifika Dosya İsmi	**DN Alanı Bilgileri**	**Geçerlilik Süresi**	**SİL Dosyası**	**OCSP Servisi**	**İptal Durumu**
RootA.crt	CN: Root A O: Valid C: TR	10 yıl	-	-	Geçerli
RootB.crt	CN: Root B O: Signature forged C: TR	10 yıl	-	-	Geçerli
RootC.crt	CN: Root C O: Valid C: TR	10 yıl	-	-	Geçerli
SubRootA1.crt	CN: SubRoot A1 O: Valid C: TR	10 yıl	RootA1.crl	-	Geçerli
SubRootA2.crt	CN: SubRoot A2 O: Signature forged C: TR	10 yıl	RootA1.crl	-	Geçerli
SubRootA3.crt	CN: SubRoot A3 O: Revoked in CRL C: TR	10 yıl	RootA1.crl	-	İptal
SubRootA4.crt	CN: SubRoot A4 O: Expired CRL C: TR	10 yıl	RootA2.crl	-	Geçerli
SubRootA5.crt	CN: SubRoot A5 O: CRL Signature Forged C: TR	10 yıl	RootA3.crl	-	Geçerli

Çizelge 4.5: Testlerde Kullanılan Kök ve Alt kök Sertifikaları (Devam)

Sertifika Dosya İsmi	**DN Alanı Bilgileri**	**Geçerlilik Süresi**	**SİL Dosyası**	**OCSP Servisi**	**İptal Durumu**
SubRootA6.crt	CN: SubRoot A6 O: Revoked in OCSP C: TR	10 yıl	-	OCSPA1	İptal
SubRootA7.crt	CN: SubRoot A7 O: Expired OCSP Response C: TR	10 yıl	-	OCSPA2	Geçerli
SubRootA8.crt	CN: SubRoot A8 O: OCSP Signature Forged C: TR	10 yıl	-	OCSPA3	Geçerli
SubRootA9.crt	CN: SubRoot A9 O: Expired OCSP Certificate C: TR	10 yıl	-	OCSPA4	Geçerli
SubRootA10.crt	CN: SubRoot A10 O: OCSP Certificate Signature Forged C: TR	10 yıl	-	OCSPA5	Geçerli
SubRootA11.crt	CN: SubRoot A11 O: Revoked OCSP Certificate C: TR	10 yıl	-	OCSPA6	Geçerli
SubRootB.crt	CN: SubRoot B O: Valid C: TR	10 yıl	RootB.crl	-	Geçerli

Çizelge 4.6: Testlerde Kullanılan OCSP Sertifikaları

Sertifika Dosya İsmi	**DN Alanı Bilgileri**	**OCSP No Check**	**Süresi**	**SİL Dosyası**	**İptal Durumu**
OCSPA1.crt	CN: OCSP A1 O: Valid C: TR	Var	10 yıl	RootA1.crl	Geçerli
OCSPA2.crt	CN: OCSP A2 O: Expired OCSP Response C: TR	Var	10 yıl	RootA1.crl	Geçerli
OCSPA3.crt	CN: OCSP A3 O: OCSP Response Signature Forged C: TR	Var	10 yıl	RootA1.crl	Geçerli
OCSPA4.crt	CN: OCSP A4 O: Expired C: TR	Var	3 ay	RootA1.crl	Geçerli
OCSPA5.crt	CN: OCSP A5 O: Signature Forged C: TR	Var	10 yıl	RootA1.crl	Geçerli
OCSPA6.crt	CN: OCSP A6 O: Revoked C: TR	Yok	10 yıl	RootA1.crl	İptal
OCSPAConst.crt	CN: OCSP AConst O: Valid C: TR	Var	10 yıl	RootA1.crl	Geçerli

Çizelge 4.6: Testlerde Kullanılan OCSP Sertifikaları (Devam)

OCSPA1_1.crt	CN: OCSP A1 1 O: Valid C: TR	Var	10 yıl	SubRoot A1_1.crl	Geçerli
OCSPA1_2.crt	CN: OCSP A1 2 O: Expired OCSP Response C: TR	Var	10 yıl	SubRoot A1_1.crl	Geçerli
OCSPA1_3.crt	CN: OCSP A1 3 O: OCSP Response Signature Forged C: TR	Var	10 yıl	SubRoot A1_1.crl	Geçerli
OCSPA1_4.crt	CN: OCSP A1 4 O: Expired C: TR	Var	3 ay	SubRoot A1_1.crl	Geçerli
OCSPA1_5.crt	CN: OCSP A1 5 O: Signature Forged C: TR	Var	10 yıl	SubRoot A1_1.crl	Geçerli
OCSPA1_6.crt	CN: OCSP A1 6 O: Revoked C: TR	Yok	10 yıl	SubRoot A1_1.crl	İptal
OCSPA1_7.crt	CN: OCSP A1 7 O: Wrong Certificate Response C: TR	Var	10 yıl	SubRoot A1_1.crl	Geçerli
OCSPAConst.crt	CN: OCSP A1 Const O: Valid C: TR	Var	10 yıl	SubRootA1_1.crl	Geçerli

Çizelge 4.7: Testlerde Kullanılan Zaman Damgası Sertifikaları

Sertifika Dosya İsmi	**Sertifika DN Alanı Bilgileri**	**Süresi**	**SİL Dosyası**	**İptal Durumu**
TSA1.crt	CN: TS A1 O: Valid C: TR	10 yıl	RootA1.crl	Geçerli
TSA2.crt	CN: TS A2 O: TS Signature Forged C: TR	10 yıl	RootA1.crl	Geçerli
TSA3.crt	CN: TS A3 O: Expired C: TR	3 ay	RootA1.crl	Geçerli
TSA4.crt	CN: TS A4 O: Signature Forged C: TR	10 yıl	RootA1.crl	Geçerli
TSA5.crt	CN: TS A5 O: Revoked C: TR	10 yıl	RootA1.crl	İptal
TSACONST.crt	CN: TS AConst O: Valid C: TR	10 yıl	RootA1.crl	Geçerli
TSB.crt	CN: TS B O: Root Signature Forged C: TR	10 yıl	RootB.crl	Geçerli
TSC1.crt	CN: TS C1 O: Valid C: TR	10 yıl	RootC1.crl	Geçerli
TSC2.crt	CN: TS C2 O: Expired CRL C: TR	10 yıl	RootC2.crl	Geçerli
TSC3.crt	CN: TS C3 O: CRL Signature Forged C: TR	10 yıl	RootC3.crl	Geçerli

Çizelge 4.8: Testlerde Kullanılan NES'ler

Sertifika Dosya İsmi	**DN Alanı Bilgileri**	**Süresi**	**SİL Dosyası**	**OCSP Servisi**	**İptal Durumu**
QCA1_1.crt	CN: QC A1 1 O: Valid C: TR	10 yıl	SubRoot A1_1.crl	-	Geçerli
QCA1_2.crt	CN: QC A1 2 O: Valid C: TR	10 yıl	-	OCSPA11	Geçerli
QCA1_3.crt	CN: QC A1 3 O: Non-repuduation Absent C: TR	10 yıl	SubRoot A1_1.crl	OCSPA11	Geçerli
QCA1_4.crt	CN: QC A1 4 O: CP user notice Statement Absent C: TR	10 yıl	SubRoot A1_1.crl	OCSPA11	Geçerli
QCA1_5.crt	CN: QC A1 5 O: ETSI QC Statementid Absent C: TR	10 yıl	SubRoot A1_1.crl	OCSPA11	Geçerli
QCA1_6.crt	CN: QC A1 6 O: BTK QC Statementid Absent C: TR	10 yıl	SubRoot A1_1.crl	OCSPA11	Geçerli
QCA1_7.crt	CN: QC A1 7 O: BTK QC Statementinfo Absent C: TR	10 yıl	SubRoot A1_1.crl	OCSPA11	Geçerli

Çizelge 4.8: Testlerde Kullanılan NES'ler (Devam)

Sertifika Dosya İsmi	**DN Alanı Bilgileri**	**Süresi**	**SİL Dosyası**	**OCSP Servisi**	**İptal Durumu**
QCA1_8.crt	CN: QC A1 8 O: Expired C: TR	3 ay	SubRoot A1_1.crl	OCSPA11	Geçerli
QCA1_9.crt	CN: QC A1 9 O: Signature Forged C: TR	10 yıl	SubRoot A1_1.crl	OCSPA11	Geçerli
QCA1_10.crt	CN: QC A1 10 O: Revoked in CRL C: TR	10 yıl	SubRoot A1_1.crl	-	İptal
QCA1_11.crt	CN: QC A1 11 O: Revoked in OCSP C: TR	10 yıl	-	OCSPA11	İptal
QCA1_12.crt	CN: QC A1 12 O: Expired CRL C: TR	10 yıl	SubRoot A1_2.crl	-	Geçerli
QCA1_13.crt	CN: QCA1 13 O: CRL Signature Forged C: TR	10 yıl	SubRoot A1_3.crl	-	Geçerli
QCA1_14.crt	CN: QC A1 14 O: Expired OCSP Response C: TR	10 yıl	-	OCSPA12	Geçerli

Çizelge 4.8: Testlerde Kullanılan NES'ler (Devam)

Sertifika Dosya İsmi	**DN Alanı Bilgileri**	**Süresi**	**SİL Dosyası**	**OCSP Servisi**	**İptal Durumu**
QCA1_15.crt	CN: QC A1 15 O: OCSP Response Signature Forged C: TR	10 yıl	-	OCSPA13	Geçerli
QCA1_16.crt	CN: QC A1 16 O: Expired OCSP Certificate C: TR	10 yıl	-	OCSPA14	Geçerli
QCA1_17.crt	CN: QC A1 17 O: OCSP Certificate Signature Forged C: TR	10 yıl	-	OCSPA15	Geçerli
QCA1_18.crt	CN: QC A1 18 O: Revoked OCSP Certificate C: TR	10 yıl	-	OCSPA16	Geçerli
QCA1_19.crt	CN: QC A1 19 O: Monetary Limit Included C: TR	10 yıl	SubRoot A1_1.crl	-	Geçerli
QCA1_20.crt	CN: QC A1 20 O: Usage Limit Included C: TR	10 yıl	SubRoot A1_1.crl	-	Geçerli
QCA1_21.crt	CN: QC A1 21 O: Wrong Certificate's OCSP Respose C: TR	10 yıl	-	OCSPA17	Geçerli

Çizelge 4.8: Testlerde Kullanılan NES'ler (Devam)

Sertifika Dosya İsmi	**DN Alanı Bilgileri**	**Süresi**	**SİL Dosyası**	**OCSP Servisi**	**İptal Durumu**
QCA2.crt	CN: QC A2 O: SubRoot Certificate Signature Forged C: TR	10 yıl	SubRoot A2.crl	-	Geçerli
QCA3.crt	CN: QC A3 O: SubRoot Certificate Revoked in CRL C: TR	10 yıl	SubRoot A3.crl	-	Geçerli
QCA4.crt	CN: QC A4 O: SubRoot CRL Expired C: TR	10 yıl	SubRoot A4.crl	-	Geçerli
QCA5.crt	CN: QC A5 O: SubRoot CRL Signature Forged C: TR	10 yıl	SubRoot A5.crl	-	Geçerli
QCA6.crt	CN: QC A6 O: SubRoot Revoked in OCSP C: TR	10 yıl	SubRoot A6.crl	-	Geçerli
QCA7.crt	CN: QC A7 O: SubRoot's OCSP Response Expired C: TR	10 yıl	SubRoot A7.crl	-	Geçerli

Çizelge 4.8: Testlerde Kullanılan NES'ler (Devam)

Sertifika Dosya İsmi	**DN Alanı Bilgileri**	**Süresi**	**SİL Dosyası**	**OCSP Servisi**	**İptal Durumu**
QCA8.crt	CN: QC A8 O: SubRoot's OCSP Response Signature Forged C: TR	10 yıl	SubRoot A8.crl	-	Geçerli
QCA9.crt	CN: QC A9 O: SubRoot's OCSP Certificate Expired C: TR	10 yıl	SubRoot A9.crl	-	Geçerli
QCA10.crt	CN: QC A10 O: SubRoot's OCSP Certificate Signature Forged C: TR	10 yıl	SubRoot A10.crl	-	Geçerli
QCA12.crt	CN: QC A12 O: Valid C: TR	10 yıl	SubRoot A12.crl	-	Geçerli
QCB.crt	CN: QC B O: Root Certificate Signature Forged C: TR	10 yıl	SubRoo tB.crl	-	Geçerli

4.3 Test Sisteminde Kullanılan İmzalı Dosyalar ve Özellikleri

İmzalı test dosyalarının her biri hatalı bir durum içermektedir. Bu hatalar imzada kullanılan sertifikalar veya imza dosya formatı ile ilgilidir.

Aşağıda belirtilen imza türleri için PAdES imzalı test dosyaları oluşturulmuştur:

1. B-Type :Basic Electronic Signature (Basit Elektronik İmza)
2. LT-Type :PAdES Long Term Validation (Uzun Dönem Doğrulama)
3. LTA-Type :Archival Electronic Signature (Arşiv Elektronik İmza)

İmzalı dosyalarda mevcut olan zaman damgaları aksi belirtilmedikçe TSA1'den alınmış geçerli zaman damgalarıdır. Ancak alt kök sertifikası iptal kontrollerinin yapıldığı geçersiz SİL, geçersiz OCSP sertifikası ve geçersiz OCSP cevabı testleri için oluşturulan imzalı test dosyalarında mevcut olan zaman damgaları TSC1'den alınmış zaman damgalarıdır.

Doğrulama verileri içeren imza dosyaları içinde kök sertifikalarına ait iptal verileri ve referans değerlerinin bulunması zorunlu değildir.

Tablo'lardaki imzaların içerikleri PDF-A dır.

Çizelge 4.9: İmzalı Dosyalar

İmzalı Dosya İsmi	**İmzada Kullanılan Sertifika**	**İmzalı Dosyanın Özelliği**
B-Type_1, LT-Type_1, LTA_Type_1	QCA1_1.crt	Geçerli imza (Tüm imzalı özellikler eklenmiş)
B-Type_4, LT-Type_4, LTA_Type_4	QCA1_1.crt	"ESS-Signing-Certificate" içeriği bozulmuş
B-Type_5, LT-Type_5, LTA_Type_5	QCA1_1.crt	"messageDigest" imza özelliği bozulmuş
B-Type_6, LT-Type_6, LTA_Type_6	QCA1_1.crt	SHA-1 algoritması kullanılarak imzalanmış
B-Type_7, LT-Type_7, LTA_Type_7	QCA1_1.crt	İmza dosyasının imzası bozulmuş
B-Type_8, LT-Type_8, LTA_Type_8	QCA1_2.crt	Geçerli imza
B-Type_9, LT-Type_9, LTA_Type_9	QCA1_3.crt	"anahtar kullanım (keyusage)" uzantısı içeriğinde "inkâr edilemezlik" özelliği olmayan sertifika ile imzalanmış
B-Type_10, LT-Type_10, LTA_Type_10	QCA1_4.crt	"sertifika ilkeleri" uzantısının içeriğinde ibare olmayan sertifik ile imzalanmış
B-Type_11, LT-Type_11, LTA_Type_11	QCA1_5.crt	"nitelikli elektronik sertifika ibareleri" uzantısının içeriğinde ETSI ibaresine ait OID bulunmayan sertifika ile imzalanmış
B-Type_12, LT-Type_12, LTA_Type_12	QCA1_6.crt	"nitelikli elektronik sertifika ibareleri" içeriğinde BTK tarafından belirlenen ibareye ait OID bulunmayan sertifika ile imzalanmış
B-Type_13, LT-Type_13, LTA_Type_13	QCA1_7.crt	"nitelikli elektronik sertifika ibareleri" içeriğinde BTK tarafından belirlenen ibare olmayan sertifika ile imzalanmış

Çizelge 4.9: İmzalı Dosyalar (Devam)

İmzalı Dosya İsmi	**İmzada Kullanılan Sertifika**	**İmzalı Dosyanın Özelliği**
B-Type_14, LT-Type_14, LTA_Type_14	QCA1_8.crt	Süresi dolmuş sertifika ile imzalanmış
B-Type_15, LT-Type_15, LTA_Type_15	QCA1_9.crt	İmzası bozuk sertifika ile imzalanmış
B-Type_16_1, LT-Type_16_1, LTA_Type_16_1	QCA1_10.crt	SİL'de iptal olmuş sertifika ile imzalanmış, sertifika imza tarihinden önce iptal edilmiş
LT-Type_16_2, LTA_Type_16_2	QCA1_10.crt	SİL'de iptal olmuş sertifika ile imzalanmış, sertifika imza tarihinden sonra iptal edilmiş
B-Type_17_1, LT-Type_17_1, LTA_Type_17_1	QCA1_11.crt	OCSP'de iptal olmuş sertifika ile imzalanmış, sertifika imza tarihinden önce iptal edilmiş
LT-Type_17_2, LTA_Type_17_2	QCA1_11.crt	OCSP'de iptal olmuş sertifika ile imzalanmış, sertifika imza tarihinden sonra iptal edilmiş
B-Type_18, LT-Type_18, LTA_Type_18	QCA1_12.crt	Kontrol edildiği SİL'in geçerlilik süresi dolmuş
B-Type_19, LT-Type_19, LTA_Type_19	QCA1_13.crt	Kontrol edildiği SİL'in üzerindeki ESHS imzası bozuk
B-Type_20, LT-Type_20, LTA_Type_20	QCA1_14.crt	Kontrol edildiği OCSP cevabının geçerlilik süresi dolmuş
B-Type_21, LT-Type_21, LTA_Type_21	QCA1_2.crt	Kontrol edildiği OCSP cevabı üzerindeki ESHS imzası bozuk
B-Type_22, LT-Type_22, LTA_Type_22	QCA1_16.crt	Kontrol edildiği OCSP sertifikasının süresi dolmuş

Çizelge 4.9: İmzalı Dosyalar (Devam)

İmzalı Dosya İsmi	**İmzada Kullanılan Sertifika**	**İmzalı Dosyanın Özelliği**
B-Type_23, LT-Type_23, LTA_Type_23	QCA1_17.crt	Kontrol edildiği OCSP sertifikasının imzası bozuk
B-Type_24_1, LT-Type_24_1, LTA_Type_24_1	QCA1_18.crt	Kontrol edildiği OCSP sertifikası iptal olmuş, sertifika imza tarihinden önce iptal edilmiş
LT-Type_24_2, LTA_Type_24_2	QCA1_18.crt	Kontrol edildiği OCSP sertifikası iptal olmuş, sertifika imza tarihinden sonra iptal edilmiş
B-Type_25, LT-Type_25, LTA_Type_25	QCA1_19.crt	Maddi limit alanı "0" olan sertifika il imzalanmış
B-Type_26, LT-Type_26, LTA_Type_26	QCA1_20.crt	Kullanım kısıtı olan sertifika ile imzalanmış
B-Type_27, LT-Type_27, LTA_Type_27	QCA1_21.crt	OCSP response içindeki sertifika farklı
B-Type_28, LT-Type_28, LTA_Type_28	QCA2.crt	Alt kök sertifikasının imzası bozuk
B-Type_29_1, LT-Type_29_1, LTA_Type_29_1	QCA3.crt	Alt kök sertifikası SİL'de iptal olmuş, sertifika imza tarihinden önce iptal edilmiş
LT-Type_29_2, LTA_Type_29_2	QCA3.crt	Alt kök sertifikası SİL'de iptal olmuş, sertifika imza tarihinden sonra iptal edilmiş
B-Type_30, LT-Type_30, LTA_Type_30	QCA4.crt	Alt kök sertifikası süresi dolmuş SİL'e referans veriyor
B-Type_31, LT-Type_31, LTA_Type_31	QCA5.crt	Alt kök sertifikası imzası bozuk SİL'e referans veriyor

Çizelge 4.9: İmzalı Dosyalar (Devam)

İmzalı Dosya İsmi	**İmzada Kullanılan Sertifika**	**İmzalı Dosyanın Özelliği**
B-Type_32_1, LT-Type_32_1, LTA_Type_32_1	QCA6.crt	Alt kök sertifikası OCSP'de iptal olmuş, sertifika imza tarihinden önce iptal edilmiş
LT-Type_32_2, LTA_Type_32_2	QCA6.crt	Alt kök sertifikası OCSP'de iptal olmuş, sertifika imza tarihinden sonra iptal edilmiş
B-Type_33, LT-Type_33, LTA_Type_33	QCA7.crt	Alt kök sertifikasının iptal kontrolünün yapıldığı OCSP cevabının süresi dolmuş
B-Type_34, LT-Type_34, LTA_Type_34	QCA12.crt	Alt kök sertifikasının iptal kontrolünün yapıldığı OCSP cevabının imzası bozuk
B-Type_35, LT-Type_35, LTA_Type_35	QCA9.crt	Alt kök sertifikasının iptal kontrolünün yapıldığı OCSP sertifikasının geçerlilik süresi dolmuş
B-Type_36, LT-Type_36, LTA_Type_36	QCA10.crt	Alt kök sertifikasının iptal kontrolünün yapıldığı OCSP sertifikasının imzası bozuk
B-Type_37_1, LT-Type_37_1, LTA_Type_37_1	QCA11.crt	Alt kök sertifikasının iptal kontrolünün yapıldığı OCSP sertifikası iptal olmuş, sertifika imza tarihinden önce iptal edilmiş
LT-Type_37_2, LTA_Type_37_2	QCA11.crt	Alt kök sertifikasının iptal kontrolünün yapıldığı OCSP sertifikası iptal olmuş, sertifika imza tarihinden sonra iptal edilmiş
B-Type_38, LT-Type_38, LTA_Type_38	QCB.crt	Kök sertifikasının imzası bozuk
LT-Type_40, LTA_Type_40	QCA1_1.crt	"İmza ZD" TSA1'den alınmış; "TSTInfo" içeriğindeki "messageImprint" özeti bozulmuş imza dosyası

Çizelge 4.9: İmzalı Dosyalar (Devam)

İmzalı Dosya İsmi	**İmzada Kullanılan Sertifika**	**İmzalı Dosyanın Özelliği**
LT-Type_41, LTA_Type_41	QCA1_1.crt	"İmza ZD" TSA2'den alınmış ZD imzası bozuk
LT-Type_42, LTA_Type_42	QCA1_1.crt	"İmza ZD" TSA3'den alınmış; ZD sertifikasının geçerlilik süresi dolmuş
LT-Type_43, LTA_Type_43	QCA1_1.crt	"İmza ZD" TSA4'den alınmış; ZD sertifikasının üzerindeki ESHS imzası bozuk
LT-Type_44, LTA_Type_44	QCA1_1.crt	"İmza ZD" TSA5'den alınmış; ZD sertifikası iptal olmuş; sertifika imza tarihinden önce iptal edilmiş
LT-Type_45, LTA_Type_45	QCA1_1.crt	"İmza ZD" TSA5'den alınmış; ZD sertifikası iptal olmuş; sertifika imza tarihinden sonra iptal edilmiş
LT-Type_46, LTA_Type_46	QCA1_1.crt	"İmza ZD" TSB'den alınmış; ZD sertifikası imzası bozuk kök tarafından üretilmiş
LT-Type_47, LTA_Type_47	QCA1_1.crt	"İmza ZD" TSC1'den alınmış; Geçerli
LT-Type_48, LTA_Type_48	QCA1_1.crt	"İmza ZD" TSC2'den alınmış; ZD sertifikası süresi dolmuş SİL'e referans veriyor
LT-Type_49, LTA_Type_49	QCA1_1.crt	"İmza ZD" TSC3'den alınmış; ZD sertifikası imzası bozuk SİL'e referans veriyor

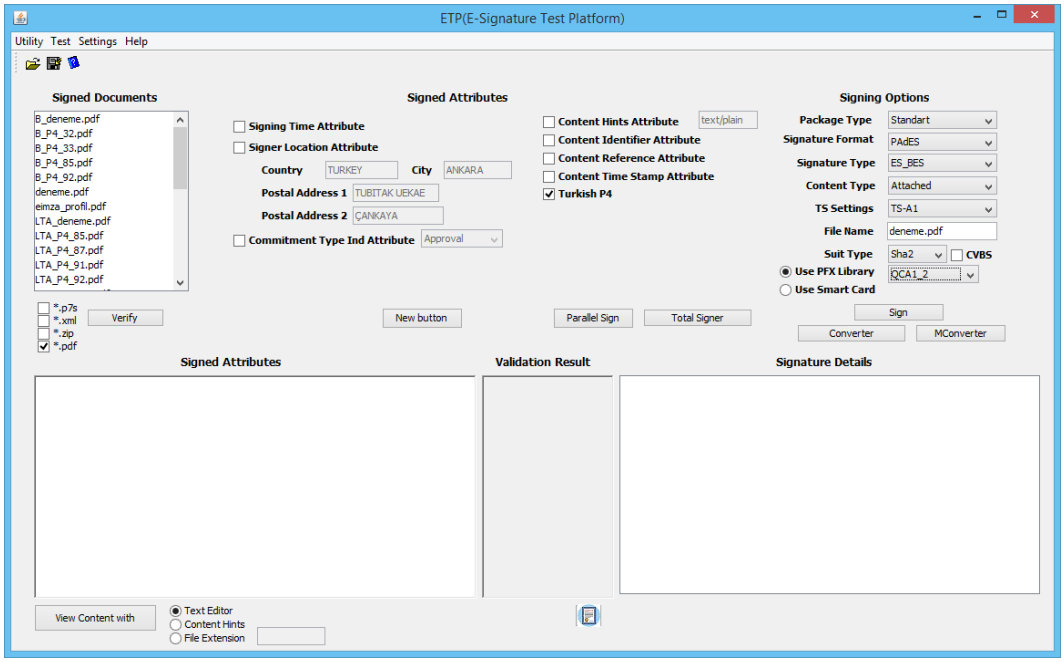
Çizelge 4.9: İmzalı Dosyalar (Devam)

İmzalı Dosya İsmi	**İmzada Kullanılan Sertifika**	**İmzalı Dosyanın Özelliği**
LTA_Type_84	QCA1_1.crt	"Arşiv ZD" TSA1'den alınmış; "TSTInfo" içeriğindeki "messageImprint" özeti bozulmuş imza dosyası
LTA_Type_85	QCA1_1.crt	"Arşiv ZD" TSA2'den alınmış ZD imzası bozuk
LTA_Type_86	QCA1_1.crt	"Arşiv ZD" TSA3'den alınmış; ZD sertifikasının geçerlilik süresi dolmuş
LTA_Type_102	QCA1_2.crt	XLONG imzalı OCSP sertifikasının süresi imza tarihinden sonra dolmuş
LTA_Type_103	QCA1_1.crt	XLONG imzalı "İmza ZD" sertifikasının süresi imza tarihinden sonra dolmuş
LTA_Type_107	QCA1_1.crt	XLONG imzalı Alt Kök sertifikasının süresi imza tarihinden sonra dolmuş
LTA_Type_108	QCA1_1.crt	XLONG imzalı Kök sertifikasının süresi imza tarihinden sonra dolmuş

4.4 Geliştirilen Program

PAdES Test Suit'i oluşturmak için kurduğumuz yapılardan önceki bölümlerde bahsedilmiştir. İmza oluşturma testlerinde bu yapıları kullanarak testler yapıldığı belirtilmiştir. İmza doğrulama testlerinde kullanmak için imza oluşturan bir program yazılması gerekmektedir. Bu amaçla hem akıllı kartla (smartcard) hem de pfx ile PAdES imza oluşturabilen, imza doğrulayabilen, imzalı dosyayı üst formatlara yükseltebilen, çeşitli imza bozma işlemlerini yapabilen bir program tarafımızdan geliştirilmiştir. Programda imzalama sırasında kullanılacak algoritmanın seçilmesine, kullanılacak zaman damgası sunucusunun, "TS Settings" kısmından seçilmesine olanak sağlanmaktadır. Ayrıca pfx ile imza oluşturulmasına imkan sağlandığından, içerisinde bulunan pfx'ler "Use PFX Library (PFX Kütüphanesi Kullan)" seçeneğiyle aktif edilebilmekte ve imza oluşturulmasında kullanılacak PFX, kombo kutusu (combo box) ile seçilebilmektedir. İmza oluşturma sırasında sertifika doğrulamanın aktifleştirilmesi: "CVBS (Certificate Validation Before Signing - İmza Öncesinde Sertifika Doğrulaması)" parametresi ile kontrol edilmektedir. İmza oluşturma sonrasında oluşacak imza tipi; B-Type, LT-Type, LTA-Type olmak üzere "Signature Type (İmza Tipi)" kısmında bulunan kombo kutusuyla seçilebilmektedir. Oluşturulan imza tipleri, birbirine çevirici (converter) kullanılarak dönüştürülebilmektedir. Örneğin, B-Type olan bir imzalı dosya LT-Type'a çevirici kullanılarak yükseltilebilmektedir. Dönüştürülmek istenen imzalı dosyada hata bulunma durumunda, manuel çevirici (MConverter) kullanılmalıdır. Manuel çevirici, dosyanın ilgili imza formatında sahip olması gereken; iptal verisi (SİL ve/veya OCSP) ve sertifikaları eklemektedir. Ayrıca program kullanılarak imzalı dosyaların "Signed Documents (İmzalı Dokumanlar)" altında listelenmesi sağlanmıştır. İmzalı dosya oluşturulduktan sonra uygulama tarafından doğrulanıp, ilgili hatalı durumun istenildiği üzere oluşturulup oluşturulmadığı kontrol edilebilir. İmzalı dosyanın özellikleri, kullanılan algoritmalar, içerisinde bulunan zaman damgası bilgileri, imzalı özellikleri (signed attributes), beyan edilen zaman özelliği (signing time), imzacının sertifika bilgileri, imzada bulunan sertifikalar ve iptal değerleri program tarafından gösterilebilmektedir. Programda bulunan Signature Format (İmza Formatı) kısmı değiştirilerek, CAdES ve XAdES'e geçiş yapılabilmektedir. Bu sayede sadece PAdES imza oluşturan ve imza doğrulayan bir programdan daha fazlası olarak CAdES ve XAdES standartlarına uygun, imza oluşturabilen, imza doğrulayabilen bir program oluşturulmuştur. Arayüzde bulunan seçenekli imzalı özellikler bölümünden (Optional Signed Attributes)

CAdES imza için tanımlanmış olan bütün seçenekli özelliklerin eklenebilmesine olanak sağlanmıştır. Programın görüntüsü Şekil 4.2'deki gibidir.



Şekil 4.2: Geliştirilen Program

5. SONUÇLAR VE ÖNERİLER

Testlerimizde; Adobe Reader'da bir takım önemli hatalar bulduk. İmza oluşturma testlerinde, imzası bozuk sertifikayla kesinlikle imza oluşturmaması gerekirken imza oluşturmaya izin verdiğini tespit ettik. İmzası bozuk sertifika ile imza oluşturulması imzacının geçersiz imzalar oluşturmasına sebebiyet verecektir. Bu durum oldukça önemlidir ve mutlaka giderilmelidir. İmza oluşturma kısmındaysa; hata mesajlarının hatayı net olarak tarif etmediği görülmüştür. İmza doğrulama kısmında alt kökle ilgili senaryolarda; B-type imzalı dosyanın doğrulanması sonucunda net bir hata vermek yerine, zincirin kurulamadığına dair genel bir hata verilmiştir. Ayrıca Adobe Reader OCSP CertID si SHA2 olan OCSP cevaplarını da çözümleyememekte ve kullanamamaktadır. SHA1'in güvenini yitirdiği günümüzde Adobe'nin bu eksikliği gidermesi gerekmektedir.

Oluşturduğumuz suit sayesinde, bütün PAdES imza oluşturma ve imza doğrulama mekanizmaları derinlemesine test edilebilecek ve Adobe Reader'da yaptığımız üzere, hatalı durumlar tespit edilebilecektir.

KAYNAKLAR

[1] T. ERGUN, *Security analysis of electronic signature applications and test suite study.* PhD thesis, Orta Doğu Teknik Üniversitesi, 2013.

[2] ESI, "Pades baseline profile," ETSI TS 103 172 V2.2.2, Electronic Signatures and Infrastructures, 2013.

[3] RFC, "Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile," RFC 5280, Network Working Group, Geneva, Switzerland, 2008.

[4] ESI, "Cms advanced electronic signatures (cades)," ETSI TS 101 733 V2.2.1, Electronic Signatures and Infrastructures, 2013.

[5] ESI, "Cms advanced electronic signatures (cades)," ETSI TS 101 903 V1.4.1, Electronic Signatures and Infrastructures, 2009.

[6] NIST, "Public key interoperability test suite," PKI TS, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[7] ESI, "Plug test," etsi, Electronic Signatures and Infrastructures, France, 2011.

[8] ISO, "Information technology - security techniques - hash-functions - part 1: General," ISO/IEC 10118-1, International Organization for Standardization, Geneva, Switzerland, 2000.

[9] ISO, "Information technology - security techniques - hash-functions - part 2: Hash-functions using an n-bit block cipher," ISO/IEC 10118-2, International Organization for Standardization, Geneva, Switzerland, 2000.

[10] ISO, "Information technology - security techniques - hash-functions - part 3: Dedicated hash-functions," ISO/IEC 10118-3, International Organization for Standardization, Geneva, Switzerland, 2004.

[11] ISO, "Information technology - security techniques - hash-functions - part 4: Hash-functions using modular arithmetic," ISO/IEC 10118-4, International Organization for Standardization, Geneva, Switzerland, 1998.

[12] ANSI, "Public key cryptography using irreversible algorithms - part 2: The secure hash algorithm (sha-1)," ANSI X9, Accredited Standards Committee, 1997.

[13] ESI, "Algorithms and parameters for secure electronic signatures; part 1: Hash functions and asymmetric algorithms," ETSI TS 102 176-1 V2.0.0, Electronic Signatures and Infrastructures, 2007.

[14] S. Boren and A. Brisson, "Dynamic distributed key system and method for identity management, authentication servers, data security and preventing man-in-the-middle attacks," Apr. 23 2009. US Patent App. 12/297,884.

[15] ITU-T, "Information technology - open systems," ITU-T X.509, Network Working Group, 2008.

[16] R. Gazete, "Elektronik İmza kanunu," Kanun No. 5070, 2004.

[17] ESI, "Signature verification procedures and policies," ETSI TS 102 853 V1.1.1, Electronic Signatures and Infrastructures, 2012.

[18] Council of European Union, "Directive 1999/93/ec of the european parliement and of the council," 1999.

[19] ESI, "Qualified certificate profile," ETSI TS 101 862 V1.3.1, Electronic Signatures and Infrastructures, 2004.

[20] R. Gazete, "Elektronik İmza kanununun uygulanmasına İlişkin usul ve esaslar hakkında yönetmelik," No. 25692, 2005.

[21] R. Gazete, "Elektronik İmza ile İlgili süreçlere ve teknik kriterlere İlişkin tebliğ," No. 25692, 2005.

[22] K. Kararı, "Güvenli elektronik İmza oluşturma ve doğrulama uygulamaları ile güvenli elektronik İmza formatlarına dair usul ve esaslar hakkında kurul kararı," DK 77/353, 2006.

[23] ESI, "Application of electronic signature standards in europe," ETSI TR 102 438 V1.1.1, Electronic Signatures and Infrastructures, 2006.

[24] ESI, "Policy requirements for certification authorities issuing qualified certificates," ETSI TS 101 456 V1.4.3, Electronic Signatures and Infrastructures, 2007.

[25] RFC, "X.509 internet public key infrastructure online certificate status protocol - ocsp," RFC 3161, Internet Engineering Task Force (IETF), 2013.

[26] RFC, "Internet x.509 public key infrastructure time-stamp protocol (tsp)," RFC 3161, Network Working Group, 2001.

[27] ESI, "Pdf advanced electronic signature profiles; part 2: Pades basic - profile based on iso 32000-1," ETSI TS 102 778-2 V1.2.1, Electronic Signatures and Infrastructures, 2009.

[28] ESI, "Pdf advanced electronic signature profiles; part 4: Pades long term - pades-ltv profile," ETSI TS 102 778-4 V1.1.2, Electronic Signatures and Infrastructures, 2009.

[29] ISO, "Document management portable document format part 1: PDF 1.7," ISO 32000-2012 1:2008, International Organization for Standardization, Geneva, Switzerland, 2008.

[30] RFC, "Cryptographic message syntax (cms)," RFC 5652, Network Working Group, 2009.

[31] ESI, "Pdf advanced electronic signature profiles; part 5: Pades for xml content - profiles for xades signatures," ETSI TS 102 778-5 V1.1.2, Electronic Signatures and Infrastructures, 2009.

[32] ESI, "Pdf advanced electronic signature profiles; part 6: Visual representations of electronic signatures," ETSI TS 102 778-6 V1.1.1, Electronic Signatures and Infrastructures, 2010.

[33] ESI, "Pdf advanced electronic signature profiles; part 1: Pades overview - a framework document for pades," ETSI TS 102 778-1 V1.1.1, Electronic Signatures and Infrastructures, 2009.

[34] ISO, "Use of iso 32000-1 with support for embedded files (pdf/a-3)," ISO 19005˜, International Organization for Standardization, Geneva, Switzerland, 2008.

[35] RFC, "Electronic signature policies," RFC 3125, Network Working Group, 2001.

[36] ESI, "Electronic signature formats," ETSI ES 201 733 V1.1.3, Electronic Signatures and Infrastructures, 2000.

[37] ESI, "Pdf advanced electronic signature profiles; part 3: Pades enhanced - pades-bes and pades-epes profiles," ETSI TS 102 778-3 V1.2.1, Electronic Signatures and Infrastructures, 2010.

[38] K. Kararı, "Nitelikli elektronik sertifika, sİl ve ocsp İstek cevap mesajları profilleri rehberine İlişkin kurul kararı," DK 77/207, 2007.

[39] IETF, "Ess update: Adding certid algorithm agility," RFC 5035, Network Working Group, 2007.

[40] B. T. Kurumu, "Elektronik İmza ile İlgili süreçlere ve teknik kriterlere İlişkin tebliğ'de değişiklik yapılmasına dair tebliğ," 2013.

[41] RFC, "Pkcs 10 certification request syntax specification," RFC 2986 V1.7, Network Working Group, 2003.

[42] ITU-T, "Information technology abstract syntax notation one (asn.1): Specification of basic notation," ITU-T 680, Network Working Group, 1997.

[43] ITU-T, "Specification of abstract syntax notation one (asn.1)," ITU-T 208, Telecemmunication Standardization Sector Of ITU, 1988.

[44] ITU-T, "Information technology asn.1 encoding rules: Specification of basic encoding rules (ber), canonical encoding rules (cer) and distinguished encoding rules (der)," ITU-T 690, Telecemmunication Standardization Sector Of ITU, 2002.

[45] CEN, "Security requirements for signature creation applications," CWA 14170, EUROPEAN COMMITTEE FOR STANDARDIZATION, Management Centre: rue de Stassart, 36 B-1050 Brussels, 2004.

[46] CEN, "General guidelines for electronic signature verification," CWA 14171, EUROPEAN COMMITTEE FOR STANDARDIZATION, Management Centre: rue de Stassart, 36 B-1050 Brussels, 2004.

[47] RFC, "Public-key cryptography standards (pkcs) 1: Rsa cryptography specifications version 2.1," RFC 3447, Network Working Group, 2003.

[48] IEEE, "Standard specifications for public key cryptography," IEEE 1363, The Institute of Electrical and Electronics Engineers, Brussels, Belgium, 2008.

[49] FIPS, "Secure hash standard (shs)," FIPS PUB1802, Federal Information Processing Standards, United States, 2002.

[50] S. A. V. Alfred J. Menezes, Paul C. van Oorschot, *Handbook of Applied Cryptography*. CRC Press, 2001.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Soyadı, Adı	: TURAN, Erhan
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 04.05.1989 Aydın
Medeni hali	: Bekar
Telefon	: 262 648 1000
Faks	: 262 648 1800
e-mail	: erhanturan@windowslive.com

EĞİTİM

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Y. Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi	2015
Lisans	Erciyes Üniversitesi Bilgisayar Mühendisliği	2012
Lisans	Erciyes Üniversitesi Elektrik Elektronik Mühendisliği	2012

İLGİ ALANLARI

Kriptoloji	Açık Anahtar Altyapısı	Elektronik İmza
Programlama	İnternet Güvenliği	Java
Hardware Security Modules	SmartCards	E-Signature API

İŞ DENEYİMi

Yıl	**Yer**	**Görev**
2012-	TÜBİTAK BİLGEM KAMUSM	Araştırmacı

YABANCI DİL

İngilizce (Çok iyi)
İspanyolca (Az)

ÇALIŞMA ALANLARI

Programlama	Java,
	C, C
	Android Development
	CAdES E-imza Kütüphanesi
	XAdES E-imza Kütüphanesi
	PAdES E-imza Kütüphanesi
Web Teknolojileri	Vaadin
	Java Applets
	.net
Geliştirme Araçları	Eclipse SDK
	jDeveloper
	NetBeans
	Visual Studio

HOBİLER

Masa Tenisi, Yüzme

YAYINLAR

E. TURAN, A. AYDIN SELÇUK, T. ERGUN "PAdES Test Suite For Adobe Reader", Crypto Days 2015, Kocaeli, 2015 (Kabul edildi, Nisan 2015)