



E-İMZA UYGULAMASI KONTROL LİSTESİ

Sürüm 1.3

Kurum/Firma Adı:	
Proje Adı:	
E-imza Oluşturma Yazılımı	
E-imza Doğrulama Yazılımı	
Yüklenici Firma:	
Kullanılan e-imza programları:	<input type="checkbox"/> UEKAE Java e-imza kütüphanesi <input type="checkbox"/> Diğer:
Tarih:	/ /

KATILIMCILAR

KSM Yetkilisi		
<i>Adı, Soyadı</i>	<i>Telefon</i>	<i>İmzası</i>
Kurum Yetkilisi		
<i>Adı, Soyadı</i>	<i>Telefon</i>	<i>İmzası</i>
Firma Yetkilisi		
<i>Adı, Soyadı</i>	<i>Telefon</i>	<i>İmzası</i>

İÇİNDEKİLER

KATILIMCILAR.....	1
İÇİNDEKİLER.....	3
TANIMLAR, KISALTMALAR.....	5
KAYNAKLAR.....	5
GİRİŞ.....	6
BEYANA DAYALI KABULLER.....	7
BÖLÜM 1 GÜVENLİ ELEKTRONİK İMZA OLUŞTURMA YAZILIMI İSTERLERİ ..	8
1 Genel Güvenlik Kriterleri.....	9
1.1 Doğru İmza Verisinin Referans Verilmesi.....	9
1.2 Doğrulanabilir İmzanın Oluşturulması.....	9
1.3 İmza Verisi İsterleri.....	9
2 Kullanıcı Belgesinin Sunulması.....	10
2.1 Kullanıcı Belge Tipi Gereksinimleri.....	10
2.2 Kullanıcı Belgesinin Doğru Görüntülenmesi.....	11
2.3 Görüntülemeye Duyarsız Belge Türlerinin Gösterimi.....	11
2.4 Belge İçeriğinde Olabilecek Dinamik Bileşenler ile İlgili İsterler.....	12
3 İmza Özellikleri Görüntüleyici.....	12
4 İmza Sahibi Etkileşimi.....	13
4.1 Kullanıcı Arayüz Prensipleri.....	13
4.2 İmzanın Bilinçli Oluşturulması.....	14
4.3 İmza İşleminin Zaman Aşımı.....	14
4.4 İmza Sahibinin Kontrolündeki Diğer İşlevler.....	14
5 İmzalanacak Veri Formatının Oluşturulması.....	14
6 Veri Özetleme.....	15
7 Güvenli Elektronik İmza Oluşturma Aracı İletişimi.....	15
7.1 Erişim Verisi Girişi.....	15
7.2 Çoklu Uygulama.....	16
7.3 Sertifikaların Araç İçinden Alınması.....	16
7.4 İmza Oluşturma Verisinin Seçilmesi.....	16
7.5 Kullanıcı Kimlik Doğrulama.....	17
8 Kullanıcı Belgesinin Oluşturulması.....	17
9 Güvenli Elektronik İmza Oluşturma Yazılımı Dış Bağlantıları.....	17
10 İmza Zamanının Belirtilmesi.....	18
BÖLÜM 2 GÜVENLİ ELEKTRONİK İMZA DOĞRULAMA YAZILIMI İSTERLERİ	20
1 İlk İmza Doğrulama İşlemleri.....	21
1.1 İmzanın Yaşam Süresi.....	21
1.2 “İlk imza doğrulama” Zamanı.....	21
1.3 İmza Zamanının Belirlenmesi.....	21
1.4 İmza Formatı.....	22
1.5 “İlk İmza Doğrulama” Girdileri.....	22
1.6 “İlk İmza Doğrulama” Çıktıları.....	22
1.7 “İlk İmza Doğrulama” Süreci ile İlgili Kurallar.....	24
1.7.1 Elektronik Sertifikanın Nitelikli Olmasının Kontrolü.....	24
1.7.2 Sertifika Güven Zincirinin Doğrulanması.....	25
1.7.3 Sertifika Güven Zincirindeki Sertifikaların Geçerlilik Sürelerinin Doğrulanması.....	25
1.7.4 Sertifika İptal Kontrollerinin Yapılması ile İlgili Kurallar.....	25
1.7.5 Sertifika İptal Listesinin Geçerlilik Kontrolleri.....	26

1.7.6	OCSP Cevaplarının Geçerlilik Kontrolleri	27
1.7.7	Zaman Damgasının Doğruluğu ile İlgili Kontroller.....	27
1.7.8	ESHS'nin Yetkili Olmasının Kontrolü	27
1.7.9	Uygun Algoritmaların Kullanıldığının Kontrolü	28
1.7.10	İmza Sahibinin Yetki Kontrolü	28
2	Sonraki İmza Doğrulama İşlemleri	28
2.1.1	Doğrulama Verilerinin Elde Edilmesi.....	28
2.1.2	Zaman Damgası İşlemleri	28
2.1.3	İleri İmza Formatları	29
3	İmza Doğrulama Sistemleri.....	29
3.1	İmza Doğrulama Sistemleri.....	29
3.2	Kullanıcı İşlemleri.....	30
3.2.1	Doğrulama Yapılacak E-imzanın Seçilmesi	30
3.2.2	Kullanıcı Belgesi ve İmza Özelliklerinin Doğrulama Yapan Kişiyeye Gösterilmesi	30
3.2.3	İmza Sahibi Bilgilerinin Doğrulama Yapan Kişiyeye Gösterilmesi	31
3.2.4	Kullanıcı Arayüz İsterleri.....	31
4	Elektronik İmza Arşivleme Sistemleri	32
5	Çoklu İmza	33

TANIMLAR, KISALTMALAR

Kullanıcı belgesi: İmza sahibi tarafından elektronik olarak imzası oluşturulacak veya oluşturulmuş olan belge.

İmza verisi: Elektronik olarak imzalanacak/imzalanmış kullanıcı belgesi ve imza özelliklerinin tamamı (Özet değeri alınacak/alınmış olan veri).

İmza dosyası: İmza verisi ve imzasız imza özelliklerinin içinde bulunduğu ETSI formatındaki dosya.

İlk imza doğrulama: İmza oluşturulduktan “ertelenme süresi” kadar bir süre sonra, uzun dönemde imza doğrulamanın yapılabilmesi için gerekli verilerin toplanarak imza doğrulama yapılması işlemi.

Ertelenme süresi (*Grace Period*): İmzanın oluşturulduğu zamanki sertifika iptal bilgisinin doğru olarak elde edilmesi için, imza zamanından iptal kontrolünün yapıldığı zamana kadar beklenen süre. İlk imza doğrulaması ertelenme süresi sonrasında gerçekleştirilir, elde edilen doğrulama verileri (SİL veya OCSP cevabı) sistemde depolanır ve sonraki imza doğrulama işlemlerinde depolanan bu veriler kullanılır. Ertelenme süresinin ne olması gerektiği imzayı doğrulayan tarafların politikalarınca belirlenir ve uygulanır. Bu süre belirlenirken imza zamanındaki sertifika iptal durumu ile ilgili en doğru bilginin edinilmesi amaçlanır. İmza zamanındaki sertifikanın iptal durumu ile ilgili bilgi, imza zamanından sonra ilk yayınlanan iptal durum bilgisi ile imza zamanında mevcut olan iptal durum bilgisinden edinilebilir. Bu yüzden ertelenme süreleri belirlenirken ESHS’lerin iptal durum bilgilerini güncelleme aralıklarının takip edilmesi en doğru sonucu elde etmede yardımcı olabilir.

ESHS : Elektronik Sertifika Hizmet Sağlayıcısı

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

KSM : Kamu Sertifikasyon Merkezi

NES : Nitelikli Elektronik Sertifika

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

SİL : Sertifika İptal Listesi

CWA : CEN (Comité Européen De Normalisation) Workshop Agreement

TK : Telekomünikasyon Kurumu

KAYNAKLAR

1. CWA 14170: Security Requirements for Signature Creation Applications (İmza Oluşturma Uygulamaları için Güvenlik Gereksinimleri)
2. CWA 14171: Procedures for Electronic Signature Verification (Elektronik İmza Doğrulama için Prosedürler)
3. ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)

GİRİŞ

Bu dokümanda güvenli elektronik imza oluşturma ve doğrulama yazılımlarının sağlanması gereken şartlar kontrol listesi olarak verilmiştir.

Doküman iki bölümden oluşmaktadır. Birinci bölümde güvenli elektronik imza oluşturma yazılımlarının sağlanması gereken özellikler belirtilmiştir. İkinci bölümde güvenli elektronik imza doğrulama yazılımlarının sağlanması gereken özellikler belirtilmiştir. Kontrol listesi hazırlanırken CWA 14170 ve CWA 14171 dokümanları referans alınmıştır. Listede CWA'ye göre sağlanması zorunlu olan, opsiyonel ve koşullu olarak sağlanması gereken özellikler belirtilmiştir. Zorunlu olarak belirtilen özelliklerin yazılım tarafından sağlanması gerekmektedir. Kontrol listesinde bilgilenme amaçlı istenen, yazılımla ilgili diğer bilgiler de mevcuttur.

Aşağıdaki bileşenlerin aksi belirtilmedikçe ve özel bir durum olmadıkça güvenli elektronik imza oluşturma yazılımı içerisinde bulunması CWA 14170'e göre zorunludur.

1. Kullanıcı Belgesinin Sunulması (Signer's Document Presentation) Bileşeni
2. İmza Özellikleri Görüntüleyici (Signature Attribute Viewer) Bileşeni
3. İmza Sahibi Etkileşimi (Signer Interaction Component) Bileşeni
4. İmzalanacak Veri Formatı (Data To Be Signed Formatter) Bileşeni
5. İmza Sahibi Kimlik Doğrulama (Signer Authentication) Bileşeni
6. Veri Özetleme (Data Hashing) Bileşeni
7. Güvenli Elektronik İmza Oluşturma Aracı İletişimcisi (SCDev/SCA Communicator)
8. Güvenli Elektronik İmza Oluşturma Aracı Kimlik Doğrulama (SCDev/SCA Authenticator) –Conditional

Aşağıdaki bileşenlerin aksi belirtilmedikçe ve özel bir durum olmadıkça güvenli elektronik imza doğrulama yazılımı içerisinde bulunması CWA 14171'e göre zorunludur.

1. İmza dosyası içeriğindeki bilgilerin elde edilmesi
2. İmzanın doğrulanması ve doğrulama verilerinin elde edilmesi
3. Doğrulama verilerinin eklenerek gelişmiş imza formatının oluşturulması

Aşağıdaki tablolarda yazılımın sağlanması gereken genel güvenlik bileşenlerinin yanı sıra yukarıdaki bileşenler içerisinde sağlanması gereken özellikler belirtilmiştir.

Tablonun ilk kolonundaki kısaltmalar ve anlamları aşağıdaki gibidir:

- Z : Zorunlu
K : Koşullu
O : Opsiyonel
B : Bilgi amaçlı

Kontrol listesindeki işaretlerin anlamı:

- : Belirtilen özellik sağlanıyor
 : Belirtilen özellik sağlanmıyor
 : Belirsiz (Açıklaması yazılmalıdır)

BEYANA DAYALI KABULLER

Aşağıda belirtilen şartların güvenli elektronik imza oluşturma ve doğrulama yazılımı tarafından sağlandığı yazılımı geliştiren tarafın beyanına dayanılarak kabul edilmiştir:

1. İmzalanacak kullanıcı belgesinin ve imzaya dahil olan imza özelliklerinin (signed attributes) özet değeri hesaplanmadan önce kazara veya bilerek değiştirilmesini engelleyecek önlemler alınıyor.
2. İmza oluşturma aşamasında kabul görmüş standartlar kullanılarak (NIST vb.) özetleme işlemleri gerçekleştiriliyor. Özet değerinin kazara veya bilerek değiştirilmesini engelleyecek önlemler alınıyor.
3. Güvenli elektronik imza oluşturma yazılımı ile aracı arasında giden ve gelen verinin kazara veya bilerek değiştirilmesini engelleyecek önlemler alınıyor.
4. İmza verisinin, imza dosyasının ve akıllı kart erişim verisinin gizliliği sağlanıyor ve yetkisi olmayan taraflarca kopyalarının alınması engelleniyor.
5. Uygulamanın çalıştığı bilgisayar kamuya açık bir ortamda bulunuyorsa imzalanan veri imzalama işleminden sonra bilgisayardan tamamen siliniyor ve kalıcı olarak bilgisayarda depolanmıyor.
6. İmza verisi, imza dosyası ve akıllı kart erişim verisi yazılım bileşenleri arasında taşınırken bütünlük ve gizliliği korunuyor. (Yazılım bileşenleri farklı ortamlarda dağınık vaziyette ise ve bu bileşenler arasında giden ve gelen veriler güvenilir olmayan kanallar, uygulama arabirimleri veya yazılım/donanım modülleri aracılığıyla iletiliyorsa bu şartın sağlanması zorunludur.)
7. Güvenli elektronik imza oluşturma yazılımının çalıştığı ortamdaki diğer güvenilir olmayan bileşenlerin, uygulama veya iletişim kanallarının imza işlemine etki etmesi engelleniyor.
8. Erişim verisi güvenli elektronik imza oluşturma yazılımı içerisinde tutulmak durumunda ise bu aşamada güvenliği sağlanıyor ve kullanımı sona erdiğinde sistemden güvenli bir biçimde siliniyor.
9. Erişim verisi güvenli elektronik imza oluşturma aracına güvenilir bir kanal üzerinden gönderiliyor.
10. Güvenli elektronik imza oluşturma aracı iletişimcisinin fiziksel arabirimleri, imza oluşturma aracının taahhüt ettiği tüm güvenli imza oluşturulmasını sağlayan özellikleri desteklemektedir.
11. Güvenli elektronik imza oluşturma aracı iletişimcisi, imzalanmaya niyet edilen verinin yetkisiz değiştirilmesine karşı korunuyor.
12. Yazılım imzalanan belgenin kullanıcıya gösterilen olduğunu garanti eder.

BÖLÜM 1

GÜVENLİ ELEKTRONİK İMZA OLUŞTURMA YAZILIMI İSTERLERİ

1 Genel Güvenlik Kriterleri

Genel Kontrol Sonucu			<input type="checkbox"/>		
1.1 Doğru İmza Verisinin Referans Verilmesi			<input type="checkbox"/>		
Z	CWA 7.2.3	1	İmza verisi kullanıcıya ekrandan gösteriliyor. İmza verisinin özet değeri de bu veriye bağlı olarak oluşturuluyor. Yazılım, kullanıcıya ekrandan gösterdiği imza verisi yerine başka bir veri ile bu işlemleri gerçekleştiriyor.	<input type="checkbox"/>	
1.2 Doğrulanabilir İmzanın Oluşturulması			<input type="checkbox"/>		
Z	CWA 7.5 CWA 9	1	Yazılımın doğrulanabilir bir imza oluşturması aşağıdaki kontroller yapılarak sağlanıyor: <input type="checkbox"/> Sertifikanın nitelikli olduğunun kontrolü CWA 14171'e uygun olarak (Bölüm 2- 1.7.1) yapılıyor. <input type="checkbox"/> NES ve güven zincirindeki ESHS sertifikalarının üzerindeki elektronik imzalar CWA 14171'e uygun olarak (Bölüm 2-1.7.2'nin 2 ve 3. maddeleri) doğrulanıyor. <input type="checkbox"/> NES ve güven zincirindeki ESHS sertifikalarının geçerlilik süreleri CWA 14171'e uygun olarak (Bölüm 2-1.7.3) doğrulanıyor. <input type="checkbox"/> NES ve güven zincirindeki ESHS sertifikalarının iptal durum kontrolleri güncel iptal durum bilgilerine bakılarak yapılıyor. <input type="checkbox"/> SİL/OCSP sertifikalarının geçerlilik kontrolleri CWA 14171'e uygun olarak (Bölüm 2-1.7'deki ilgili maddeler) yapılıyor. <input type="checkbox"/> Kontrollerin geçersiz olması durumunda kullanıcı geçersizlik sebebi ile ilgili olarak uyarılıyor ve imzalama işlemine izin verilmiyor.	<input type="checkbox"/>	
1.3 İmza Verisi İsterleri			<input type="checkbox"/>		

Z	CWA 7.6	1	Kullanıcı belgesi olmadan imzalama işlemi yapılmıyor.	<input type="checkbox"/>	
Z	CWA 7.6	2	İmza verisi imzada kullanılan sertifika bilgisini içeriyor.	<input type="checkbox"/>	

2 Kullanıcı Belgesinin Sunulması

Genel Kontrol Sonucu			<input type="checkbox"/>		
B	-	1	Belge görüntüleme amaçlı kullanılan araçların tanımı: <input type="checkbox"/> Uygulama dahilinde yazılmış bir araç kullanılıyor. <input type="checkbox"/> Kullanıcının makinasında yüklü görüntüleme aracı kullanılıyor. <input type="checkbox"/> Diğer: _____		
2.1 Kullanıcı Belge Tipi Gereksinimleri			<input type="checkbox"/>		
B	CWA 8.2	1	İmzalanmasına izin verilen kullanıcı belge türleri belirlenmiş ise aşağıda belirtilmelidir: <input type="checkbox"/> Kullanılan görüntülemeye karşı duyarlı (Örn; text, MS dokümanları, pdf, vs..) belge türlerini belirtiniz: _____ <input type="checkbox"/> Kullanılan görüntülemeye karşı duyarsız (Örn; HTML, XML, vs..) belge türlerini belirtiniz: _____		
Z	CWA 8.3 7.6	2	Kullanıcı belge görüntüleyici, belge türünün ne olduğu ve nasıl görüntüleneceği bilgisini aşağıdaki iki yöntemden birisi ile imza doğrulama yapacak kişi için belirliyor: <input type="checkbox"/> Belge türünün ne olduğu bilgisi, belge formatının içeriğinden anlaşılıyor. <input type="checkbox"/> Belge türünün ne olduğu bilgisi imza verisi içeriğindeki, “kullanıcı belge tipi” bilgisinden anlaşılıyor. ¹	<input type="checkbox"/>	

¹ “Kullanıcı belge tipi” bilgisi olarak ETSI TS 101 733’de tanımı yapılan “content-hints” imza özelliği kullanılabilir.

K ²	CWA 8.3	3	Belge görüntüleyicisi, imza verisi içeriğine eklenecek olan “kullanıcı belge tipi” bilgisinde belirtilen belge türü ile kullanıcı belge türünün aynı olduğunu kontrol ediyor, belirtilen belge türü uyuşmuyorsa imza işlemine devam edilmiyor ve kullanıcı ekrandan uyarılıyor. ³	<input type="checkbox"/>	
Z	CWA 8.3	4	İmzalanacak kullanıcı belgesinin formatında hata olması durumunda kullanıcı uyarılıyor ve imzalama işleminden çıkma seçeneği tanınıyor.	<input type="checkbox"/>	
Z	CWA 8.3	5	İmzalanacak belgenin içeriğinin tamamının görüntülenememesi durumunda kullanıcı uyarılıyor ve imza işleminden çıkmasına olanak sağlanıyor.	<input type="checkbox"/>	
K ⁴	CWA 8.3	6	İmzalanmasına izin verilen kullanıcı belge türleri dışındaki bir belgenin imzalanmak istenmesi durumunda kullanıcı uyarılıyor ve imzalama işleminden çıkma seçeneği tanınıyor.	<input type="checkbox"/>	
K ⁵	CWA 8.3	7	Belge üzerinde daha önceden oluşturulmuş imzalar kullanıcıya gösteriliyor.	<input type="checkbox"/>	
K ⁵	CWA 8.3	8	Belge üzerinde daha önceden oluşturulmuş imzaların CWA 14171’e uygun olarak doğrulanmasına imkan tanınıyor.	<input type="checkbox"/>	
Z	CWA 8.3	9	Kazara değiştirmelere karşı, imza işleminden önce belgenin edit edilemez biçimde görüntülenmesi sağlanıyor.	<input type="checkbox"/>	
2.2 Kullanıcı Belgesinin Doğru Görüntülenmesi				<input type="checkbox"/>	
Z	CWA 8.4	1	İmzalanan belgenin imzayı oluşturan kişiye gösterimi ile imzayı doğrulayacak kişiye gösteriminin aynı olması için gereken şartlar sağlanmıştır.	<input type="checkbox"/>	
2.3 Görüntülemeye Duyarsız Belge Türlerinin Gösterimi				<input type="checkbox"/>	
K ⁶	CWA 8.5	1	Görüntülemeye duyarsız belge türleri görüntülenirken belgenin tek ve sadece bir biçimde görüntülenmesi sağlanıyor.	<input type="checkbox"/>	

² İmza doğrulama yapılırken, belge türü ETSI’de tanımlanan “Content-hints” imza özelliği içeriğinden belirlenecekse bu madde sağlanmalıdır.

³ “Kullanıcı belge tipi” bilgisi olarak ETSI TS 101 733’de tanımlanan “content-hints” imza özelliği kullanılabilir.

⁴ İmzalanmasına izin verilen belge tiplerinin sınırlandırılmış olması durumunda bu şart sağlanmalıdır.

⁵ Belge üzerinde birden fazla imza olması durumunda sağlanmalıdır.

⁶ Görüntülemeye duyarsız belge türünün imzalanması durumunda sağlanmalıdır.

2.4 Belge İçeriğinde Olabilecek Dinamik Bileşenler ile İlgili İsterler			<input type="checkbox"/>		
Z	CWA 8.6 8.2	1	<p>Aşağıdaki dört maddeden birisi sağlanıyor:</p> <p><input type="checkbox"/> Saklı veri, macro, script gibi dinamik veri içeren belge türlerinin imzalanmasına izin verilmiyor.</p> <p><input type="checkbox"/> Belge içeriğindeki dinamik verilerin kullanıcı tarafından filtre edilmesine imkan tanınıyor.</p> <p><input type="checkbox"/> Dinamik verinin varlığı konusunda imza sahibi imzalama işleminden önce uyarılıyor ve imzalama işleminden vazgeçme seçeneği tanınıyor.</p> <p><input type="checkbox"/> Belgeyi görüntüleyen program imza işleminden sonra yapılan değişiklikleri farkedip kullanıcıyı uyarabilme kabiliyetine sahiptir.</p>	<input type="checkbox"/>	

3 İmza Özellikleri Görüntüleyici

Genel Kontrol Sonucu			<input type="checkbox"/>		
Z	CWA 9	1	<p>İmza oluşturulmadan önce, imza sahibinin ilgili nitelikli elektronik sertifikasının en azından aşağıdaki bilgilerini görüntüleme imkanı tanınıyor:</p> <p><input type="checkbox"/> Sertifika içerisinde yer alan kullanım amacının güvenli elektronik imza oluşturma olduğu bilgisi</p> <p><input type="checkbox"/> Sertifika sahibinin bilgileri⁷</p> <p><input type="checkbox"/> Sertifika geçerlilik süresi</p> <p><input type="checkbox"/> Sertifikayı veren kurum bilgileri</p> <p><input type="checkbox"/> Nitelikli elektronik sertifika uzantısı içeriğindeki bilgiler</p> <p><input type="checkbox"/> Sertifika seri numarası</p>	<input type="checkbox"/>	
B	-	2	Kullanıcıya ekrandan seçtirilen imza özellikleri:		

⁷ Sertifika içeriğindeki isim alanı bilgileri olan "Subject" ve varsa "SubjectAltName" alanlarının gösterilmesi gerekmektedir.

B	-	3	Uygulamanın otomatik olarak eklediği imza özellikleri:		
Z	CWA 9	4	İmzalanacak imza özelliklerinin neler olduğu kullanıcıya ekrandan doğru bir şekilde gösteriliyor.	<input type="checkbox"/>	
Z	CWA 9	5	İmza özelliklerinin formatı ile ilgili olarak aşağıdaki üç maddeden birisi sağlanıyor. <input type="checkbox"/> Saklı veri, macro, script gibi dinamik veri içeren imza özelliklerinin imzalanmasına izin verilmiyor. <input type="checkbox"/> Dinamik verinin varlığı konusunda imza sahibi imzalama işleminden önce uyarılıyor ve imzalama işleminden vazgeçme seçeneği tanınıyor. <input type="checkbox"/> İmza özelliklerini görüntüleyen program imza işleminden sonra yapılan değişiklikleri farkedip kullanıcıyı uyarabilme kabiliyetine sahiptir.	<input type="checkbox"/>	

4 İmza Sahibi Etkileşimi

Genel Kontrol Sonucu			<input type="checkbox"/>		
4.1 Kullanıcı Arayüz Prensipleri			<input type="checkbox"/>		
Z	CWA 10.1	1	İşlemin etkin ve verimli bir biçimde tamamlanması için kullanıcıya gerekli bilgilendirmeler yapılıyor.	<input type="checkbox"/>	
Z	CWA 10.1 10.6	2	Kullanıcıya yapılan bilgilendirmeler, yapılan işlemin sistemdeki etkisi ve sonuçlarını doğru, düzgün ve tutarlı olarak kullanıcının anlayacağı ve kullanıcının güvenlik açığı oluşturmaya engel olacak bir biçimde ifade ediyor.	<input type="checkbox"/>	
Z	CWA 10.1	3	İmza işlemi tamamlanana kadar kullanıcının kontrol edebilmesi gereken tüm noktalarda bilgilendirme yapılıyor.	<input type="checkbox"/>	
Z	CWA 10.1	4	İmza sahibinin girdiği hatalı verilere karşı tolerans sağlanıyor. Bu gibi hatalarda en az sayıda düzeltme ile bilgilendirme ve yönlendirme amaçlı hata mesajları verilerek işlemin düzgün bir biçimde tamamlanması sağlanıyor.	<input type="checkbox"/>	

K ⁸	CWA 10.1 10.5	5	Bilgilendirmeler kullanıcının bireysel ihtiyacına (örn; dil seçimi) cevap verebilecek bir yapı üzerine kurulmuştur.	<input type="checkbox"/>	
Z	CWA 10.1	6	Yapılan işlemlerin doğruluğu ve güvenilirliği konusunda durum raporları ve hata mesajları veriliyor.	<input type="checkbox"/>	
4.2 İmzanın Bilinçli Oluşturulması				<input type="checkbox"/>	
Z	CWA 10.2	1	Güvenli elektronik imza oluşturma aracında yapılacak işlemin hemen öncesinde, kullanıcıya oluşturulacak imzanın güvenli elektronik imza olduğuna dair bir uyarı mesajı verilerek kullanıcının imzadan vazgeçmesine olanak sağlanıyor.	<input type="checkbox"/>	
4.3 İmza İşleminin Zaman Aşımı				<input type="checkbox"/>	
Z	CWA 10.3	1	İmza oluşturma süreci sırasında, kullanıcı tarafından işleme ara verilmesi durumunda işlem, belirlenen bir zaman aşımı süresi sonunda durduruluyor. Bu sürenin sonunda imza oluşturulmak istendiğinde tekrar güvenli elektronik imza oluşturma aracına erişim verisinin girilmesi isteniyor.	<input type="checkbox"/>	
B	-	2	Kurum tarafından belirlenen zaman aşımı süresi: _____	<input type="checkbox"/>	
4.4 İmza Sahibinin Kontrolündeki Diğer İşlevler				<input type="checkbox"/>	
Z	CWA 10.4	1	Kullanıcı belgesinin imzalama işleminden önce, kullanıcı tarafından seçilmesine ve görüntülenmesine izin veriliyor.	<input type="checkbox"/>	
Z	CWA 10.4	2	İmzalama işlemi kullanıcının isteği ile başlatılıyor ve tamamlanıyor.	<input type="checkbox"/>	
O	CWA 10.4	3	Kullanıcının güvenli elektronik imza oluşturma aracı erişim verisini değiştirme imkanı tanınıyor.	<input type="checkbox"/>	
O	CWA 10.4	4	İmzalanan dosyanın kullanıcı tarafından kopyasının alınmasına imkan veriliyor.	<input type="checkbox"/>	

5 İmzalanacak Veri Formatının Oluşturulması

Genel Kontrol Sonucu	<input type="checkbox"/>	
-----------------------------	--------------------------	--

⁸ Bu madde uluslararası kullanıcıları olan güvenli elektronik imza oluşturma yazılımları tarafından sağlanmalıdır.

O	-	1	Kullanıcıya ekrandan imza formatını seçme imkanı tanınıyor.	<input type="checkbox"/>	
B	-	2	Desteklediği imza formatları: <input type="checkbox"/> ETSI TS 101 733 BES (Basic Electronic Signature) <input type="checkbox"/> ETSI TS 101 733 EPES (Explicit Policy Electronic Sinatures) <input type="checkbox"/> ETSI TS 101 733 Diğer: _____ <input type="checkbox"/> ETSI TS 101 903: _____		
Z	CWA 12.2	3	İmzalanacak veri ilgili formata doğru biçimde çevriliyor.	<input type="checkbox"/>	

6 Veri Özetleme

Genel Kontrol Sonucu			<input type="checkbox"/>		
Z ⁹	-	1	Kullanılan özet algoritmaları: <input type="checkbox"/> RIPEMD – 160 <input type="checkbox"/> SHA – 1 <input type="checkbox"/> SHA-224 <input type="checkbox"/> SHA-256 <input type="checkbox"/> WHIRLPOOL	<input type="checkbox"/>	

7 Güvenli Elektronik İmza Oluşturma Aracı İletişimi

Genel Kontrol Sonucu			<input type="checkbox"/>		
7.1 Erişim Verisi Girişi			<input type="checkbox"/>		
Z	CWA 11.8	1	İmza oluşturma verisine erişim aşamasında güvenli elektronik imza oluşturma aracına erişim verisi, kullanıcı tarafından temin ediliyor.	<input type="checkbox"/>	

⁹ Mevzuata göre burda belirtilen algoritmaların kullanılması zorunludur.

Z	CWA 11.8	2	Erişim verisi parola ise ekrandan girişte verinin görünmemesi için “*” vb. karakteri kullanılıyor.	<input type="checkbox"/>	
Z	CWA 14.1	3	Erişim verisi girişi aşağıdaki üç durumdan birisi ile yapılıyor: <input type="checkbox"/> Her bir imza işlemi için araca erişim verisinin girilmesi isteniyor. <input type="checkbox"/> Erişim verisi bir kere girilerek çoklu imza yapılabilir ve _____ kez imzalamadan sonra tekrar girilmesi isteniyor. <input type="checkbox"/> Erişim verisi bir kere girilerek çoklu imza yapılabilir ve _____ dakika sonra tekrar girilmesi isteniyor.	<input type="checkbox"/>	
7.2 Çoklu Uygulama				<input type="checkbox"/>	
K ¹⁰	CWA 14.4	1	Güvenli elektronik imza oluşturma aracının imza oluşturma dışında başka uygulamaları desteklemesi durumunda, güvenli elektronik imza oluşturma yazılımı araç üzerindeki uygulamalardan birisini seçebilme özelliğine sahiptir.	<input type="checkbox"/>	
7.3 Sertifikaların Araç İçinden Alınması				<input type="checkbox"/>	
Z	CWA 14.5	1	Kullanıcının nitelikli elektronik sertifikası veya bu sertifikaya erişim sağlanabilmesi için gerekli bilgiler güvenli elektronik imza aracı içerisinde temin edilmektedir.	<input type="checkbox"/>	
B	CWA 14.5	2	Güvenli elektronik imza oluşturma aracı içerisinde bulunan ve araçtan alınabilen sertifika türleri: <input type="checkbox"/> Nitelikli elektronik sertifika <input type="checkbox"/> Kimlik doğrulama sertifikası <input type="checkbox"/> Kök / alt kök sertifikaları <input type="checkbox"/> Yetkilendirme sertifikaları <input type="checkbox"/> Diğer: _____	<input type="checkbox"/>	
O	CWA 14.5	3	Sertifikalar araç içinden bir kez alındıktan sonra yazılımın bağlı bulunduğu sistem tarafından depolanabiliyor.	<input type="checkbox"/>	
7.4 İmza Oluşturma Verisinin Seçilmesi				<input type="checkbox"/>	

¹⁰ Güvenli elektronik imza oluşturma aracının imza oluşturma dışında başka uygulamaları desteklemesi durumunda bu madde sağlanmalıdır.

Z	CWA 14.6	1	Güvenli elektronik imza oluşturma aracının birden fazla imza oluşturma verisi içermesi durumunda kullanıcıya imza oluşturma verisini seçme hakkı veriliyor.	<input type="checkbox"/>	
7.5 Kullanıcı Kimlik Doğrulama				<input type="checkbox"/>	
Z	CWA 11.8	1	Güvenli elektronik imza oluşturma aracı erişim verisinin yanlış girilmesi durumunda kullanıcı ekrandan bilgilendiriliyor.	<input type="checkbox"/>	
Z	CWA 14.7	2	Güvenli elektronik imza oluşturma aracı erişim verisinin çok sayıda hatalı denemeden dolayı bloke edilmesi durumunda kullanıcı ekrandan bilgilendiriliyor.	<input type="checkbox"/>	

8 Kullanıcı Belgesinin Oluşturulması

Genel Kontrol Sonucu				<input type="checkbox"/>	
B	-	1	Kullanıcı belgesi: <input type="checkbox"/> Lokalde kullanıcı tarafından oluşturuluyor. <input type="checkbox"/> Kullanıcının kontrolü dışında oluşturuluyor.		
Z	CWA 16.1	2	Kullanıcı belgesini oluşturan bileşen, belge içeriğinde dinamik veri bulunmasına izin vermiyor.	<input type="checkbox"/>	
K ¹¹	CWA 16.1	3	Kullanıcı belgesi içeriğinde dinamik veri varsa veriyi filtreliyor.	<input type="checkbox"/>	

9 Güvenli Elektronik İmza Oluşturma Yazılımı Dış Bağlantıları

Genel Kontrol Sonucu				<input type="checkbox"/>	
-----------------------------	--	--	--	--------------------------	--

¹¹ Kullanıcı belge formatının dinamik verileri desteklemesi durumunda bu madde sağlanmalıdır.

Z	CWA 18.1	1	Güvenli elektronik imza oluşturma yazılımının üçüncü kişilerin müdahalesi veya virüs ile yazılımın bozguna uğratılmasına karşı aşağıdaki önlemler alınmıştır: <input type="checkbox"/> Güvenlik duvarı <input type="checkbox"/> Virüs koruyucular <input type="checkbox"/> Bütün girdiler daha güvenli kapasiteleri olan ara araçlarda tutuluyor	<input type="checkbox"/>	
Z ¹²	CWA 18.2	2	Güvenli elektronik imza oluşturma aracı, imza oluşturmak için gerekli olan NES ve ESHS'ye ait sertifikaları içermiyorsa, yazılım bu sertifikalara erişebilmekte ve doğrulama işlemlerini yerine getirmektedir.	<input type="checkbox"/>	
K ¹³	CWA 18.3	3	Dışarıdaki bir sistemden alınan kullanıcı belgesinin tamamı veya bir bölümü ile imza özelliklerinin içeriği gizli ve dinamik veri içermiyor, başka bir veri ile değiştirilmiyor.	<input type="checkbox"/>	
K ¹⁴	CWA 18.4	4	Güvenli elektronik imza oluşturma yazılımı ortama uzaktan yükleniyorsa (örn; Applet, plug-in) ilgili tarafın ve yüklenen programların güvenilirliği sağlanmaktadır.	<input type="checkbox"/>	

10 İmza Zamanının Belirtilmesi

Genel Kontrol Sonucu			<input type="checkbox"/>		
Z	-	1	İmza zamanı aşağıdaki yöntemlerden birisi kullanılarak belirleniyor: <input type="checkbox"/> İmza sahibi tarafından eklenen zaman damgası <input type="checkbox"/> Güvenilir üçüncü bir tarafça tutulan zaman işareti <input type="checkbox"/> İmza verisi içinde imza özelliği olarak bulunan kullanıcı tarafından beyan edilen zaman bilgisi <input type="checkbox"/> İmza oluşturma sırasında zaman bilgisi eklenmiyor, imza	<input type="checkbox"/>	

¹² NES, güvenli elektronik imza oluşturma aracı içerisinde temin edildiği sürece bu maddenin NES için için sağlanması zorunlu değildir.

¹³ Kullanıcı belgesi veya imza özelliklerinin tamamı veya bir bölümünün dışarıdaki bir sistemden alınması durumunda bu madde sağlanmalıdır.

¹⁴ Güvenli elektronik imza oluşturma yazılımı ortama uzaktan yükleniyorsa bu madde sağlanmalıdır.

			zamanı imzalı belgenin gönderildiği sunucu tarafından belirleniyor. Belirtiniz: _____		
B	-	2	İmza verisi içine imza özelliği olarak eklenen zaman bilgisi: <input type="checkbox"/> kullanıcı makinasının sistem saatinden, <input type="checkbox"/> imza uygulamasının sahibi olan tarafa ait sunucudan elde ediliyor.		
K ¹⁵	-	3	İmzaya zaman damgası ekleniyorsa CWA 14171'e uygun olarak (Bölüm 2-1.7.7) zaman damgasının geçerlilik kontrolleri yapılıyor.	<input type="checkbox"/>	

¹⁵ İmzalama işlemi sırasında imzaya zaman damgası eklenmesi durumunda bu madde sağlanmalıdır.

BÖLÜM 2

GÜVENLİ ELEKTRONİK İMZA DOĞRULAMA YAZILIMI İSTERLERİ

1 İlk İmza Doğrulama İşlemleri

Genel Kontrol Sonucu			<input type="checkbox"/>	
1.1 İmzanın Yaşam Süresi			<input type="checkbox"/>	
B	CWA 5.1	1	Oluşturulan imzaların geçerlilik süresi <input type="checkbox"/> NES geçerlilik süresinden daha azdır. <input type="checkbox"/> NES geçerlilik süresinden daha uzundur.	
1.2 “İlk imza doğrulama” Zamanı			<input type="checkbox"/>	
B	CWA 5.2	1	“İlk imza doğrulama” işlemi (iptal bilgisi verilerinin toplanması) <input type="checkbox"/> İmza sahibi <input type="checkbox"/> İmzayı kabul eden taraf tarafından gerçekleştiriliyor.	
Z	CWA 5.3	2	“İlk imza doğrulama” işlemi, geçerli NES iptal bilgisinin elde edilmesinin sağlanması amacıyla, uygun “ ertelenme süresi (grace period) ” sonunda gerçekleştiriliyor. Ertelenme süresini belirtiniz: _____ saat/ dakika/ gün)	<input type="checkbox"/>
Z	CWA 5.6	3	“İlk imza doğrulama” işlemi NES’in geçerlilik süresi dolmadan ve iptal edilmeden; iptal bilgisini imzalayan ESHS sertifikasının süresi dolmadan ve iptal edilmeden önce gerçekleştiriliyor.	<input type="checkbox"/>
1.3 İmza Zamanının Belirlenmesi			<input type="checkbox"/>	
K ¹⁶	CWA 5.3 CWA 5.5	1	İmza zamanı olarak aşağıdakilerden birisi kabul ediliyor: <input type="checkbox"/> Güvenilir üçüncü bir tarafça tutulan zaman işareti <input type="checkbox"/> İmza dosyası içindeki imza sahibi tarafından eklenen zaman damgası <input type="checkbox"/> İmza verisi içinde kullanıcı tarafından beyan edilen zaman bilgisi	<input type="checkbox"/>

¹⁶ İmza zamanı imza oluşturma sırasında belirlenmişse bu madde sağlanmalıdır.

K ¹⁷	CWA 5.2	2	<p>İmza oluşturulurken zaman bilgisi eklenmemişse “ilk imza doğrulama” sırasında imza zamanı aşağıdaki şekilde belirleniyor.</p> <p><input type="checkbox"/> İmza dosyasının doğrulama yapan tarafa ilk alınma tarihi</p> <p><input type="checkbox"/> Doğrulamayı yapan tarafın imza dosyasına eklediği zaman damgası</p>	<input type="checkbox"/>	
1.4 İmza Formatı				<input type="checkbox"/>	
Z	CWA 5.4	1	<p>İmza formatı olarak ETSI TS 101 733’ün ve/veya ETSI TS 101 903’ün aşağıda belirtilen tiplerinden birisi destekleniyor:</p> <p><input type="checkbox"/> ETSI TS 101 733 BES (Basic Electronic Signature)</p> <p><input type="checkbox"/> ETSI TS 101 733 EPES (Explicit Policy Electronic Sinatures)</p> <p><input type="checkbox"/> ETSI TS 101 733 Diğer: _____</p> <p><input type="checkbox"/> ETSI TS 101 903: _____</p>	<input type="checkbox"/>	
1.5 “İlk İmza Doğrulama” Girdileri				<input type="checkbox"/>	
Z	CWA 5.5	1	<p>“İlk imza doğrulama” işlemine aşağıdaki verilerin tamamı girdi oluşturuyor:</p> <p><input type="checkbox"/> Kullanıcı belgesi</p> <p><input type="checkbox"/> İmza dosyası</p> <p><input type="checkbox"/> İmza sahibinin NES’i veya NES’in özet değerini içeren referans bilgisi</p> <p><input type="checkbox"/> İmza verisi içinde bulunan ve imzaya dahil olan imza özellikleri (Hangi imza özelliklerinin bu işleme dahil olduğu açıklamalarda belirtilmelidir.)</p> <p><input type="checkbox"/> İmza zamanı (1.3. maddede belirtilen seçeneklerden birisi)</p>	<input type="checkbox"/>	
K ¹⁸	CWA 5.5	2	<p>Kullanıcı belgesinin nasıl görüntüleneceği bilgisi “kullanıcı belge tipi bilgisi” içeriğinden bakılarak belirleniyor.</p>	<input type="checkbox"/>	
1.6 “İlk İmza Doğrulama” Çıktıları				<input type="checkbox"/>	

¹⁷ İmza oluşturulurken zaman bilgisinin eklenmemesi durumunda bu madde sağlanmalıdır.

¹⁸ İmza dosyası içeriğinde “kullanıcı belge tipi” bilgisinin (“content-hints” imza özelliği) olması durumunda bu madde sağlanmalıdır.

K ¹⁹	CWA 5.6	1	<p>Aşağıda işaretlenen doğrulama verileri <u>imza dosyasına</u> eklenmektedir:</p> <p><input type="checkbox"/> İmza sahibine ait NES</p> <p><input type="checkbox"/> Sertifika güven zincirindeki tüm ESHS sertifikalarına ait referans bilgileri</p> <p><input type="checkbox"/> Sertifika güven zincirindeki tüm ESHS sertifikaları</p> <p><input type="checkbox"/> İmza sahibine ait NES'in iptal durumuna ilişkin aşağıdaki bilgilerden birisi</p> <ol style="list-style-type: none"> 1. <input type="checkbox"/> SİL referans bilgisi 2. <input type="checkbox"/> OCSP referans bilgisi 3. <input type="checkbox"/> SİL dosyası 4. <input type="checkbox"/> OCSP verisi <p><input type="checkbox"/> Sertifika güven zincirindeki tüm ESHS sertifikalarının iptal durumlarına ilişkin aşağıdaki bilgilerden birisi</p> <ol style="list-style-type: none"> 1. <input type="checkbox"/> SİL referans bilgisi 2. <input type="checkbox"/> OCSP referans bilgisi 3. <input type="checkbox"/> SİL dosyası 4. <input type="checkbox"/> OCSP verisi <p><input type="checkbox"/> "İlk imza doğrulama"nın hemen ardından eklenen zaman damgası</p>	<input type="checkbox"/>	
K ²⁰	CWA 5.6	2	<p>Aşağıda işaretlenen doğrulama verileri <u>ortak kullanıma açık</u> belirlenen bir disk alanına/veri tabanına kaydedilmektedir:</p> <p><input type="checkbox"/> İmza sahibine ait NES</p> <p><input type="checkbox"/> Sertifika güven zincirindeki tüm ESHS sertifikaları</p> <p><input type="checkbox"/> İmza sahibine ait NES'in iptal durumuna ilişkin SİL dosyası / OCSP cevabı</p> <p><input type="checkbox"/> Sertifika güven zincirindeki tüm ESHS sertifikalarının iptal durumlarına ilişkin SİL dosyaları / OCSP cevapları</p>	<input type="checkbox"/>	

¹⁹ Bu maddede belirtilen verilerin tamamının imza dosyasına eklenmesi zorunlu değildir. Veriler ortak kullanıma açık depoya da eklenebilir.

²⁰ Bu maddede belirtilen sertifika veya iptal bilgileri imza dosyasına eklenmişse, ortak kullanıma açık depoya eklenmesi zorunlu değildir.

			<input type="checkbox"/> Diğer: _____		
1.7 “İlk İmza Doğrulama” Süreci ile İlgili Kurallar				<input type="checkbox"/>	
1.7.1 Elektronik Sertifikanın Nitelikli Olmasının Kontrolü				<input type="checkbox"/>	
Z	CWA 5.7.1	1	<p>NES’in kullanım amacı uygunluğu aşağıdaki maddelerin tamamının sağlanması ile kontrol ediliyor:</p> <p>1. “Sertifika ilkeleri”²¹ uzantısı ile ilgili aşağıdaki kontroller yapılıyor:</p> <p><input type="checkbox"/> “User notice” text alanında TK tarafından yayınlanan nitelikli sertifika ibaresinin (“Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır”) UTF8String tipinde yazılı olduğu</p> <p><input type="checkbox"/> “Sertifika ilkeleri” nesne tanımlama numarasının TK tarafından yetkilendirilmiş bir ESHS’ye ait olduğu</p> <p>2. “Nitelikli sertifika ibaresi”²² uzantısı ile ilgili aşağıdaki kontroller yapılıyor:</p> <p><input type="checkbox"/> İçerisinde TK tarafından yayınlanan nitelikli sertifika ibaresi nesne tanımlama numarasının mevcut olduğu (“2.16.792.1.61.0.1.5070.1.1”) ve değer kısmında da ibarenin kendisinin (“Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır”) UTF8String tipinde yazılı olduğu</p> <p><input type="checkbox"/> ETSI TS 101 862 ile uyumlu olduğunun gösterilmesi amacıyla ilgili dokümanda belirtilen (“0.4.0.1862.1.1”) nesne tanımlama numarasının mevcut olduğu</p>	<input type="checkbox"/>	
Z	-	2	<p>Kontrollerin geçersiz olması durumunda kullanıcı uyarılıyor ve imzanın geçersiz olduğu ve geçersizlik sebebi bilgisi ekrandan veriliyor. İlk imza doğrulama işlemi imza sahibi tarafından gerçekleştiriliyorsa imza işleminden vazgeçme seçeneği tanınıyor.</p>	<input type="checkbox"/>	

²¹ CertificatePolicies

²² QcStatement

1.7.2 Sertifika Güven Zincirinin Doğrulması				<input type="checkbox"/>	
Z	CWA 5.5	1	İmza doğrulama işlemi, imza özelliklerinde referans verilen NES ile gerçekleştiriliyor. NES'in imza özellikleri içeriğinde var olan referans bilgilerinin doğruluğu kontrol ediliyor.	<input type="checkbox"/>	
Z	CWA 5.7.2	2	NES üzerindeki ESHS'ye ait sertifikanın elektronik imzası doğrulanıyor.	<input type="checkbox"/>	
Z	CWA 5.7.2	3	NES'i imzalayan ESHS sertifikasının imzası ESHS'ye ait bir üst kök sertifika kullanılarak doğrulanıyor. Bu işlem kendi imzasını taşıyan en üst seviyedeki kök sertifikanın üzerindeki imzanın doğrulanmasına kadar devam ediyor.	<input type="checkbox"/>	
Z	-	4	Kontrollerin geçersiz olması durumunda kullanıcı uyarılıyor ve imzanın geçersiz olduğu ve geçersizlik sebebi bilgisi ekrandan veriliyor. İlk imza doğrulama işlemi imza sahibi tarafından gerçekleştiriliyorsa imza işleminden vazgeçme seçeneği tanınıyor.	<input type="checkbox"/>	
1.7.3 Sertifika Güven Zincirindeki Sertifikaların Geçerlilik Sürelerinin Doğrulması				<input type="checkbox"/>	
Z	CWA 5.7.3	1	NES'in imza zamanında geçerlilik süresi içinde olduğunun kontrolü yapılıyor.	<input type="checkbox"/>	
Z	CWA 5.7.3	2	NES'i imzalayan ESHS'ye ait alt kök sertifikanın imza zamanında geçerlilik süresi içinde bulunduğunun kontrolü yapılıyor. Bu işlem kendi imzasını taşıyan en üst seviyedeki kök sertifikanın geçerlilik süresi içinde bulunduğunun kontrolüne kadar devam ediyor.	<input type="checkbox"/>	
Z	CWA 5.7.3	3	Kontrollerin geçersiz olması durumunda kullanıcı uyarılıyor ve imzanın geçersiz olduğu ve geçersizlik sebebi bilgisi ekrandan veriliyor. İlk imza doğrulama işlemi imza sahibi tarafından gerçekleştiriliyorsa imza işleminden vazgeçme seçeneği tanınıyor.	<input type="checkbox"/>	
1.7.4 Sertifika İptal Kontrollerinin Yapılması ile İlgili Kurallar				<input type="checkbox"/>	
Z	CWA 5.7.3	1	Aşağıdaki yöntemlerden birisi kullanılarak NES iptal durum kontrolü yapılıyor: <input type="checkbox"/> OCSP kontrolü	<input type="checkbox"/>	

			<input type="checkbox"/> Online SİL kontrolü <input type="checkbox"/> Intranet içerisindeki SİL kontrolü		
Z	CWA 5.7.3	2	Aşağıdaki yöntemlerden birisi kullanılarak sertifika güven zincirindeki ESHS sertifikalarının (kök sertifikası hariç) iptal durum kontrolü yapılıyor: <input type="checkbox"/> OCSP kontrolü <input type="checkbox"/> Online SİL kontrolü <input type="checkbox"/> Intranet içerisindeki SİL kontrolü	<input type="checkbox"/>	
Z	CWA 5.7.3	3	Kontrollerin geçersiz olması durumunda kullanıcı uyarılıyor ve imzanın geçersiz olduğu ve geçersizlik sebebi bilgisi ekrandan veriliyor. İlk imza doğrulama işlemi imza sahibi tarafından gerçekleştiriliyorsa imza işleminden vazgeçme seçeneği tanınıyor.	<input type="checkbox"/>	
1.7.5 Sertifika İptal Listesinin Geçerlilik Kontrolleri				<input type="checkbox"/>	
Z	CWA 5.3	1	NES'in kontrol edildiği SİL için aşağıdaki geçerlilik kontrollerinin her ikisi de yapılıyor: <input type="checkbox"/> SİL yayın tarihinin ertelenme süresi (grace period) sonrası olduğu kontrol ediliyor. <input type="checkbox"/> SİL üzerindeki ESHS imzası kontrol ediliyor.	<input type="checkbox"/>	
Z	CWA 5.3	2	ESHs sertifikasının kontrol edildiği SİL için aşağıdaki geçerlilik kontrollerinin her ikisi de yapılıyor: <input type="checkbox"/> SİL'in geçerlilik süresi bitiminin imza zamanından sonrası olduğu kontrol ediliyor. <input type="checkbox"/> SİL üzerindeki ESHs imzası kontrol ediliyor.	<input type="checkbox"/>	
Z	CWA 5.3	3	SİL'i imzalayan ESHs sertifikası ve üst köklerinin, SİL yayınlandığı tarihte geçerlilik sürelerinin içinde olduğu ve iptal durumunda olmadıklarının kontrolleri yapılıyor.	<input type="checkbox"/>	
Z	-	4	Kontrollerin geçersiz olması durumunda kullanıcı uyarılıyor ve imzanın geçersiz olduğu ve geçersizlik sebebi bilgisi ekrandan veriliyor. İlk imza doğrulama işlemi imza sahibi tarafından gerçekleştiriliyorsa imza işleminden vazgeçme seçeneği tanınıyor.	<input type="checkbox"/>	

1.7.6 OCSP Cevaplarının Geçerlilik Kontrolleri				<input type="checkbox"/>	
Z	CWA 5.3	1	OCSP cevabının geçerlilik kontrolü üzerindeki ESHS imzası doğrulanarak yapılıyor.	<input type="checkbox"/>	
Z	CWA 5.3	2	OCSP'yi imzalayan ESHS sertifikası ve üst köklerinin, OCSP cevabının üretildiği tarihte geçerlilik sürelerinin içinde olduğu ve iptal durumunda olmadıklarının kontrolleri yapılıyor.	<input type="checkbox"/>	
Z	-	3	Kontrollerin geçersiz olması durumunda kullanıcı uyarılıyor ve imzanın geçersiz olduğu ve geçersizlik sebebi bilgisi ekrandan veriliyor. İlk imza doğrulama işlemi imza sahibi tarafından gerçekleştiriliyorsa imza işleminden vazgeçme seçeneği tanınmıyor.	<input type="checkbox"/>	
1.7.7 Zaman Damgasının Doğruluğu ile İlgili Kontroller²³				<input type="checkbox"/>	
Z	CWA Annex C	1	Zaman damgası eklendiği anda imza oluşturmada kullanılan NES'in geçerlilik süresi içinde olduğunun ve iptal konumunda olmadığı kontrolü yapılıyor.	<input type="checkbox"/>	
Z	CWA 5.7.4	2	Zaman damgası üzerindeki ESHS imzasının geçerliliği kontrol ediliyor.	<input type="checkbox"/>	
Z	CWA 5.7.4	3	Zaman damgasını imzalayan ESHS sertifikası ve üst köklerinin, zaman damgası üretildiği tarihte geçerlilik sürelerinin içinde oldukları, iptal durumunda olmadıkları ve sertifikalar üzerindeki imzaların doğru olduğunun kontrolleri yapılıyor.	<input type="checkbox"/>	
Z	-	4	Kontrollerin geçersiz olması durumunda kullanıcı uyarılıyor ve imzanın geçersiz olduğu ve geçersizlik sebebi bilgisi ekrandan veriliyor. İlk imza doğrulama işlemi imza sahibi tarafından gerçekleştiriliyorsa imza işleminden vazgeçme seçeneği tanınmıyor.	<input type="checkbox"/>	
1.7.8 ESHS'nin Yetkili Olmasının Kontrolü				<input type="checkbox"/>	
Z	CWA 5.7.5	1	NES'i veren ESHS'nin TK tarafından yetkilendirilmiş bir ESHS olduğunun kontrolü yapılıyor.	<input type="checkbox"/>	

²³ İmza dosyasında zaman damgasının olduğu durumlarda bu kontrol yapılır.

1.7.9 Uygun Algoritmaların Kullanıldığıının Kontrolü			<input type="checkbox"/>	
Z	CWA 5.7.6	1	İmzada TK tarafından tebliğ veya tebliğ ekinde yayınlanan açık anahtarlı algoritmalar ve özet algoritmaları ile anahtar uzunluklarının kullanıldığıının kontrolü yapılıyor.	<input type="checkbox"/>
1.7.10 İmza Sahibinin Yetki Kontrolü			<input type="checkbox"/>	
Z	CWA 5.7.7	1	İmza sahibinin yetkisi aşağıdaki yöntemlerden birisi kullanılarak elde ediliyor ve yazılım tarafından gerekli kontroller yapılıyor: <input type="checkbox"/> NES içeriği <input type="checkbox"/> Yetkilendirme sertifikası içeriği <input type="checkbox"/> Uygulama tarafında yapılan tanımlamalar <input type="checkbox"/> Diğer: _____	<input type="checkbox"/>

2 Sonraki İmza Doğrulama İşlemleri

Genel Kontrol Sonucu			<input type="checkbox"/>	
2.1.1 Doğrulama Verilerinin Elde Edilmesi			<input type="checkbox"/>	
Z	CWA 5.8 6.3.4 7.4.5	1	“İlk imza doğrulama” işleminde toplanan doğrulama verileri kullanılarak “ilk imza doğrulama”da yapılan doğrulama işlemleri (Bölüm 2-1.7’de belirtilen işlemler) imzanın oluşturulduğu zaman referans alınarak gerçekleştiriliyor. Doğrulama verilerinin toplanmamış olması durumunda, , “sonraki imza doğrulama” işlemi tamamlanmayabilir. Bu durumda imzayı doğrulayan kişi bu durumla ve doğrulama verilerinin tamamlanması gerektiği ile ilgili olarak bilgilendiriliyor. Sistem doğrulama verilerinin tamamlanmasına imkan tanıyor.	<input type="checkbox"/>
2.1.2 Zaman Damgası İşlemleri			<input type="checkbox"/>	

Z	CWA 5.7.4	1	“Sonraki imza doğrulama” işleminde imza dosyasına eklenen zaman damgasının geçerlilik kontrolleri Bölüm 2-1.7.7’ye göre yapılıyor.	<input type="checkbox"/>	
2.1.3 İleri İmza Formatları				<input type="checkbox"/>	
Z	-	1	“İleri İmza Formatları” destekleniyor ve bu formatlara uygun olarak doğrulama işlemleri gerçekleştiriliyor. Desteklenen “İleri İmza (Advanced E-Signature)” formatlarını belirtiniz: _____	<input type="checkbox"/>	

3 İmza Doğrulama Sistemleri

Genel Kontrol Sonucu				<input type="checkbox"/>	
3.1 İmza Doğrulama Sistemleri				<input type="checkbox"/>	
Z	CWA 6.1 6.2	1	Doğrulama yapılırken e-imza eklenmiş doğrulanacak belgeyi seçme imkanı tanınıyor.	<input type="checkbox"/>	
Z	CWA 6.1 6.2	2	Doğrulama yapılırken o anki zaman bilgisine erişiliyor.	<input type="checkbox"/>	
O	CWA 6.1 6.2	3	İmza doğrulama işlemi aşağıda belirtilen imza politikasına uygun olarak gerçekleştiriliyor: İmza politikası adı: _____ İmza politikası OID numarası: _____	<input type="checkbox"/>	
K ²⁴	CWA 6.1 6.2	4	İmza zamanı ile ilgili kontrol için güvenilir üçüncü tarafın sunucularına bağlanılıyor.	<input type="checkbox"/>	
Z	CWA 6.1	5	Aşağıdaki yöntemler kullanılarak ilk imza doğrulama verilerine erişim sağlanıyor: <input type="checkbox"/> ESHS sunucularına bağlanılarak doğrulama verileri elde ediliyor.	<input type="checkbox"/>	

²⁴ Bu kontrol imza zamanı olarak zaman işaretinin kullanıldığı durumlarda yapılır.

			<input type="checkbox"/> İnternet üzerinden doğrulama verileri elde ediliyor.		
Z	CWA 6.2	6	Aşağıdaki yöntemler kullanılarak sonraki imza doğrulama verilerine erişim sağlanıyor: <input type="checkbox"/> İnternet üzerinden doğrulama verileri elde ediliyor. <input type="checkbox"/> Zaman damgası sertifikasının geçerlilik kontrolleri için ESHS'ye erişim sağlanabiliyor.	<input type="checkbox"/>	
Z	CWA 6.1 CWA 7.4.5	7	İmza doğrulama aşağıdaki üç durumdan birisi ile sonuçlanıyor ve imza doğrulama yapan tarafa bildiriliyor. İmza doğrulanamadı veya doğrulama işlemi tamamlanamadı ise sebebi açıklanıyor: 1. İmza doğrulandı 2. İmza doğrulanamadı 3. İmza doğrulama işlemi tamamlanamadı	<input type="checkbox"/>	
3.2 Kullanıcı İşlemleri				<input type="checkbox"/>	
3.2.1 Doğrulama Yapılacak E-imzanın Seçilmesi				<input type="checkbox"/>	
Z	CWA 6.3.1	1	İmzalanan veriye eklenen imzaların ayrı ayrı seçilip doğrulanmasına imkan tanınıyor.	<input type="checkbox"/>	
3.2.2 Kullanıcı Belgesi ve İmza Özelliklerinin Doğrulama Yapan Kişiye Gösterilmesi				<input type="checkbox"/>	
Z	CWA 6.3.2	1	İmzalanan kullanıcı belgesi ve imzalı veya imzasız imza özellikleri doğru formatta, düzgün ve anlaşılabilir şekilde ekrandan doğrulamayı yapan kişiye gösteriliyor.	<input type="checkbox"/>	
K ²⁵	CWA 6.3.2	2	Dinamik veri içeren belge veya imza özellikleri kullanıcıya gösterilirken: <input type="checkbox"/> İçeriğin farklı görüntülenebileceği konusunda bilgilendirme yapılıyor. <input type="checkbox"/> Belgenin farklı görüntülenmesi durumunda bilgilendirme yapılıyor.	<input type="checkbox"/>	

²⁵ İmzalanan kullanıcı belgesinin dinamik veri içermesi durumunda bu madde sağlanmalıdır.

			<input type="checkbox"/> Değişen kısımlar hakkında bilgilendirme yapılıyor.		
3.2.3 İmza Sahibi Bilgilerinin Doğrulama Yapan Kişiyi Gösterilmesi					
Z	CWA 6.3.3	1	İmza sahibinin NES içeriğinde mevcut olan isim alanı bilgileri ²⁶ ekrandan doğrulamayı yapan kişiye gösteriliyor.	<input type="checkbox"/>	
Z	CWA 6.3.3	2	NES'i veren kök ve alt kök sertifikaların isim alanı bilgileri ekrandan doğrulamayı yapan kişiye gösteriliyor.	<input type="checkbox"/>	
Z	CWA 6.3.3	3	İmza zamanı (varsa zaman damgası, zaman işareti veya imza özelliği olarak eklenen zaman bilgisi) ekrandan doğrulamayı yapan kişiye gösteriliyor.	<input type="checkbox"/>	
O	CWA 6.3.3	4	İmza sahibine ait NES ekrandan doğrulamayı yapan kişiye gösteriliyor.	<input type="checkbox"/>	
K ²⁷	CWA 6.3.3	5	İmza sahibinin rolü ekrandan doğrulamayı yapan kişiye gösteriliyor.	<input type="checkbox"/>	
K ²⁸	CWA 6.3.3	6	İmza İlkeleri bilgisi ekrandan doğrulamayı yapan kişiye gösteriliyor.	<input type="checkbox"/>	
K ²⁹	CWA 6.3.3	7	İmza dosyası içeriğindeki, imza sahibi ile ilgili imza özellikleri (Örn: İmza amacı, imza yeri, vs..) ekrandan doğrulamayı yapan kişiye gösteriliyor.	<input type="checkbox"/>	
3.2.4 Kullanıcı Arayüz İsterleri					
Z	CWA 6.3.5	1	Sistemden dönen ve gerektiğinde kullanıcının talebi doğrultusunda oluşturulan diyaloglar kullanıcının anlayabileceği dilde ve açıklayıcı niteliktedir.	<input type="checkbox"/>	
Z	CWA 6.3.5	2	Kullanıcıya yapılan bilgilendirmeler, yapılan işlemin sistemdeki etkisi ve sonuçlarını doğru, düzgün ve tutarlı olarak kullanıcının anlayacağı ve kullanıcının güvenlik açığı oluşturmasına engel olacak bir biçimde ifade ediyor.	<input type="checkbox"/>	
Z	CWA 6.3.5	3	Doğrulama yapan kişinin girdiği hatalı verilere karşı tolerans sağlanıyor. Bu gibi hatalarda en az sayıda düzeltme ile	<input type="checkbox"/>	

²⁶ Sertifika içeriğindeki isim alanı bilgileri olan "Subject" ve varsa "SubjectAltName" alanlarının gösterilmesi gerekmektedir.

²⁷ İmza sahibi rolü mevcutsa bu madde sağlanmalıdır.

²⁸ İmza ilkelerinin mevcut olması durumunda bu madde sağlanmalıdır.

²⁹ İlgili imza özelliklerinin imza dosyasında mevcut olması durumunda bu madde sağlanmalıdır.

			bilgilendirme ve yönlendirme amaçlı hata mesajları verilerek işlemin düzgün bir biçimde tamamlanması sağlanıyor.		
Z	CWA 6.3.5	4	Yapılan işlemlerin doğruluğu ve güvenilirliği konusunda durum raporları ve hata mesajları veriliyor.	<input type="checkbox"/>	
Z	CWA 6.3.5	5	Herhangi bir zamanda yapılan işlemde vazgeçme, ana menüye dönme veya sistemden çıkmaya imkan veriyor.	<input type="checkbox"/>	

4 Elektronik İmza Arşivleme Sistemleri

Genel Kontrol Sonucu				<input type="checkbox"/>	
Z	CWA 8	1	Kullanıcı belgesi üzerindeki arşivlenecek imzaların seçilmesine imkan sağlanıyor.	<input type="checkbox"/>	
O	CWA 8	2	Güvenilir ve güvenilir olmayan açık anahtarlı ve özet algoritmaların listesine arayüzlerden erişilebiliyor.	<input type="checkbox"/>	
O	CWA 8	3	İmzanın arşivlenmesinin gerektiği durumlarda, ilgili bir uyarı mesajı ekrandan kullanıcıya gösterilerek arşivleme seçeneği sunuluyor.	<input type="checkbox"/>	
Z	CWA 8	4	İmzalar arşivlenirken zaman damgası alabilme özelliği mevcuttur.	<input type="checkbox"/>	
Z ³⁰	CWA 8	5	Arşiv dosyasına eklenen zaman damgasının geçerlilik kontrolleri Bölüm 2-1.7.7'ye göre yapılıyor. Zaman Damgası Hizmet Sağlayıcısı'na ait elektronik sertifikaya ait güncel SİL sistemde tutulmaktadır.	<input type="checkbox"/>	
Z	CWA 5.2 8	6	Arşivleme yapılırken imza dosyasına en son eklenen zaman damgası ile ilgili aşağıdaki durumlarda yeni zaman damgası imza dosyasına ekleniyor: <input type="checkbox"/> Zaman damgası sunucusuna ait elektronik sertifikanın geçerlilik süresinin dolmak üzere olması (geçerlilik süresi dolmadan bu işlem yapılmalıdır.) <input type="checkbox"/> Zaman damgası sunucusuna ait elektronik sertifikanın iptal	<input type="checkbox"/>	

³⁰ Zaman Damgası Hizmet Sağlayıcısı'nın sertifikasına güven farklı biçimlerde tanımlanmışsa, SİL üzerinden kontrol yapılmasına gerek yoktur.

		<p>olması (sertifikanın iptal edildiği bilgisi alındığı anda bu işlem yapılmalıdır.)</p> <p><input type="checkbox"/> Zaman damgasını imzalamada kullanılan algoritmaların güvenliğini yitirmesi (hangi algoritmaların güvenli kabul edilmediğine dair uygulamaya bilgi girişinin yapılabilmesi gerekmektedir.)</p>		
--	--	--	--	--

5 Çoklu İmza

Genel Kontrol Sonucu			<input type="checkbox"/>	
B	CWA Annex B	1	<p>Kullanıcı belgesi üzerinde aşağıda belirtilen türdeki çoklu imzaya imkan veriliyor:</p> <p><input type="checkbox"/> Paralel imza</p> <p><input type="checkbox"/> Seri imza</p> <p><input type="checkbox"/> Kapsamlı imza³¹</p>	<input type="checkbox"/>

³¹ “Kapsamlı imza” hem dokümanın hem de doküman üzerindeki imzaların imzalanmasıyla elde edilir. Arşivleme sırasında zaman damgası alınırken kullanılır.