TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

EYP UYUM DEĞERLENDİRME ÖN HAZIRLIK REHBERİ

Doküman Kodu
REH.05.02

Revizyon No
05

Revizyon Tarihi
16.09.2022

TASNİF DIŞI

EYP UYUM DEĞERLENDİRME ÖN HAZIRLIK REHBERİ

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
00	İlk Çıkış.	05.06.2017
01	Arayüz ile ilgili kontroller eklenmiştir.	15.10.2017
02	Güvenilir algoritmalar için beyaz liste kavramı eklendi. İmzanın sunucuda yükseltilmesiyle ilgili madde eklendi. Doküman kodu güncellendi.	08.12.2017
03	Doküman biçimi yeni şablona aktarılmıştır. Doküman kodu güncellenmiştir. Dokümanın eski revizyonları Kamu SM doküman yönetim sisteminde “REH-001-019” kodu ile yer almaktadır.	01.06.2018
04	Kullanım kılavuzu ve içeriği hakkında madde eklendi. Uygulama özet değerlerinin imzalanmasıyla ilgili bilgilendirme eklendi. Arşivleme Rehberi sözde kodu EYP için düzenlendi. EYP 2.0’ a göre düzenleme yapıldı.	17.02.2021
05	Zaman damgası sunucularının erişim bilgileri güncellendi. EC anahtarlı sertifikalar için gereksinimler belirtildi. Kripto Suit Bilgilendirme Yönergesi eklendi. EYP 2.0 doğrultusunda yeni isterler eklendi.	16.09.2022

İÇİNDEKİLER

1 Amaç ve Kapsam

Bu doküman, e-imza uyum değerlendirme çalışması öncesi kuruma gönderilen test paketinin içeriği hakkında bilgi vermek ve kurum tarafından ön hazırlık olarak yerine getirilmesi gereken şartları belirtmek için oluşturulmuştur. Uyum değerlendirme çalışması format kontrolü, imza oluşturma, doğrulama, arşivleme ve gerçek ortam testleri olmak üzere beş bölümden oluşmaktadır. Testlerin ayrıntılı biçimde yapılabilmesi için Kamu SM tarafından hazırlanmış olan Kamu SM Test Suit çalışması kullanılmaktadır.

Kamu kurumlarının Elektronik Belge Yönetim Sistemlerinin (EBYS), Elektronik Yazışma Paketi (EYP) oluşturması/doğrulaması durumunda EYP uyum değerlendirme çalışması yapılacaktır. Bu çalışma, Elektronik Yazışma Paketi'ndeki elektronik imzaların ve mührün uluslararası standartlara uygunluğunun kontrolünden ibarettir. Ayrıca, imzaların Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan Elektronik İmza Kullanım Profilleri Rehberi'nde yer alan "Uzun Dönemli ve ÇİSDuP Kontrollü Güvenli Elektronik İmza Politikaları (Profil P4)'na uygunluğunun kontrolü yapılmaktadır. Bu kontrol kapsamında, EYP uygulamasının oluşturduğu imzaların tipinin, P4 CAdES ES X-Long ve mühür tipinin P4 ES-A olması gerekmektedir.

EYP uyum değerlendirme çalışması kapsamında EYP'nin temel bileşenlerinin kontrolü yapılmaktadır. Bu bileşenlerin kontrolünde T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan "e-Yazışma Teknik Rehberi" sürüm 2.0 temel alınmıştır. e-Yazışma Teknik Rehberi sürüm 2.0 ile birlikte olanak tanınan şifreli paket gönderimi ve alımına ilişkin kontroller kapsam dışı tutulmuştur.

Bu doküman;

CWA 14170: Security Requirements for Signature Creation Applications (İmza Oluşturma Uygulamaları için Güvenlik Gereksinimleri),

CWA 14171: Procedures for Electronic Signature Verification (Elektronik İmza Doğrulama için Prosedürler) ,

ETSI TS 119 101: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Applications for Signature Creation and Signature Validation,

ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES),

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi e-Yazışma Teknik Rehberi sürüm 2.0 standartları referans alınarak hazırlanmıştır.

2 Kısaltmalar

CAdES:	CMS Advanced Electronic Signature - CMS Gelişmiş Elektronik İmza
CMS:	Cryptographic Message Syntax- Kriptografik Mesaj Sözdizimi
CWA:	CEN (Comité Européen De Normalisation) Workshop Agreement-CEN Çalıştay Kararları
DED:	Dahili Elektronik Doküman
EBYS:	Elektronik Belge Yönetim Sistemleri
ES-A:	Archival Electronic Signature - Arşiv Elektronik İmza
ES X-Long:	EXtended Long Electronic Signature - Genişletilmiş Uzun Elektronik İmza
ETSI:	European Telecommunications Standards Institute-Avrupa Telekomünikasyon Standartları Enstitüsü
EYP:	Elektronik Yazışma Paketi
HSM:	Donanımsal Güvenlik Modülü (Hardware Security Module)
Kamu SM:	Kamu Sertifikasyon Merkezi
XML:	Extensible Markup Language - Genişletilebilir İşaretleme Dili
Zaman Damgası:	E-imza mevzuatında tanımlanan Zaman Damgası

3 İmza Oluşturma Testleri Ön İsterleri

1. TÜBİTAK API kullanan uygulamalar API'nin son sürümünü ve son sürümü barındıran paketten çıkan politika dosyasını kullanmalıdır. API'nin son versiyonuna https://yazilim.kamusm.gov.tr/ adresinden ulaşabilirsiniz. Eski sürüm API kullanan uygulamalar değerlendirilmeyecektir.

2. Testlerde Kamu SM Test Suit'in kullanılabilmesi için size gönderilen, RootCerts.rar klasöründe bulunan test köklerinin uygulamanın güvenli kökler dizinine eklenmesi gerekmektedir. TÜBİTAK API kullananlar ilgili politika dosyası içerisinde aşağıdaki düzenlemeyi yaparak bu hazırlığı tamamlayabilirler.

```
<trustedcertificate>
        <class
        name="tr.gov.tubitak.uekae.esya.api.certificate.validation.
        find.certificate.
        trusted.TrustedCertificateFinderFromFileSystem">
                <param name="dizin" value="D:\Trusted\" />
        </class>
        <class
        name="tr.gov.tubitak.uekae.esya.api.certificate.validation.
        find.certificate.trusted.TrustedCertificateFinderFromECertSt
        ore">
                <param name="securitylevel" value="legal" />
        </class>
</trustedcertificate>
```

Politika dosyasında ayrıca aşağıdaki ayarların yapılması gerekmektedir.

```
Bu kısım yorum satırına çekilmelidir.

<!--class name =
"tr.gov.tubitak.uekae.esya.api.certificate.validation.find.crl.CRLFi
nderFromECertStore"/>

<class name =
"tr.gov.tubitak.uekae.esya.api.certificate.validation.find.crl.CRLFi
nderFromECertStore">
<param name = "getactivecrl" value="true"/>
</class -->
```

3. Uygulamada, RSA anahtarlı sertifikaların yanı sıra Eliptik Eğri anahtarlı sertifikalarla da imza oluşturulmasına izin verilmelidir. Ek-A'da verilen "Kripto Suit Testleri Bilgilendirme Yönergesi"nde belirtilen talimatlara uygun olarak Eliptik Eğri anahtarlı sertifikalarla imza oluşturulabilmelidir.

4. İmza oluşturma, doğrulama ve arşivleme modüllerinin nasıl kullanılacağına dair net bir kullanım kılavuzu sağlanmalıdır. Kullanım kılavuzu aşağıdaki maddeleri sağlamalıdır:

    a. Uygulama içerisinden erişilebilir olmalıdır.
    b. Kılavuzun giriş bölümü ya da kapak sayfasında uygulama adı, üretici firma bilgileri ve uygulama versiyonu gibi uygulamaya özgü bilgiler yer almalıdır.
    c. İmza oluşturma, doğrulama ve arşivleme işlemlerinin nasıl yapılacağı ekran görüntüleriyle desteklenerek açıklanmalıdır.
    d. Desteklenen belge ve imza türleri belirtilmelidir.

5. Doğrudan uzun dönemli imza oluşturulduğu takdirde zaman damgası alırken sistemsel bazı aksaklıklar oluşabileceğinden imza oluşturma işlemi gerçekleşemeyebilir. Kullanıcı tarafında basit elektronik imza oluşturulduktan sonra sunucuda uzun dönemli imzaya çevrilerek bu aksaklıkların önüne geçilmesi tavsiye edilmektedir.
6. İmza oluşturma testleri, sadece imzanın formatının yukarıda belirtilen uluslararası standartlara uygunluğunun kontrolünü değil sertifika doğrulama kontrollerini de içermektedir. Bu nedenle imza uygulaması bu kontrolleri yerine getirmelidir.
7. Sertifika doğrulama, yanlış PIN girme, bloke olmuş kartla imzalama ve benzeri hatalı durumlarla ilgili kullanıcı bilgilendirmelerinde standart hata kabul edilmeyecektir. Kullanıcı bilgilendirmeleri hatayı net ifade edecek şekilde olmalıdır.
8. İmza oluşturma esnasında, birden fazla sertifikanın bulunduğu kartlarda, kullanıcıya imza oluşturma işlemi için karttaki sertifikaları seçme hakkı verilmeli ve **sadece nitelikli sertifikalar gösterilmelidir**. Sertifika seçim ekranı akıllı kartın çıkarılması, yeni kart takılması vb. durumlarda yenilenmelidir. (Bu işlem, yenileme butonu, kart okuyucunun sürekli olarak dinlenmesi gibi yöntemler ile yapılabilir.)
9. Uygulamanın, sertifika içeriğini kullanıcı istediği takdirde gösterecek şekilde geliştirilmesi gerekmektedir. Uygulama sertifikayı, işletim sisteminin sertifika görüntüleyicisi vasıtasıyla da gösterebilir.
10. İmza oluşturma işleminin yapıldığı ekrana, "**Bu imza 5070 Sayılı Elektronik İmza Kanunu'na göre güvenli elektronik imzadır.**" ibaresi eklenmelidir. Kullanıcıya imzalamadan vazgeçme seçeneği sunulmalıdır.
11. Son kullanıcı nitelikli elektronik sertifikalarıyla elektronik mühür oluşturulmasına izin verilmemelidir.
12. İmza ve mühür bileşenleri için imzaya dahil olan imza özelliklerinde "mime-type" imza özelliği text/xml olacak şekilde yer almalıdır.
13. İmza oluşturma işlemi için kullanılan sertifikanın süresinin dolmasına 2 ay veya daha az zaman kalması durumunda, kullanıcıyı bilgilendiren bir uyarı verilmelidir.
14. Kullanıcıya imza oluşturma esnasında, imzaladığı içeriği değiştirilemez bir şekilde görüntüleme imkânı verilmelidir.
15. İmzalanmasına izin verilen belge türleri, Kalkınma Bakanlığı tarafından yayımlanan Birlikte Çalışabilirlik Esasları Rehberi'nin güncel sürümünün "2.1. Dosya Sunumu ve Değişimi" bölümünde tanımlanmaktadır. EYP'de üst yazı bileşeni ve (imzalı) ek bileşenindeki metin tabanlı ekler için yalnızca PDF/A formatı kabul edilmelidir.

16. Uygulama tarafından imzalanmasına izin verilen belge türü olarak PDF/A-1 ve PDF/A-2 belgeleri doğrudan kabul edilebilirken; PDF/A-3 belgeleri PDF/A uyumlu olmayan ek içerebildiğinden uygulamanın aşağıdaki yöntemlerden birini tercih etmesi gerekmektedir:

    a. Belge formatı PDF/A-3 olduğu için imzalanmasına izin vermemelidir.
    b. İmzalanacak belgenin PDF/A dışında ek içerdiğini tespit etmeli ve imzalanmasına izin vermemelidir.

17. Uygulamada imzacının PIN bilgisinin saklanması son derece tehlikelidir. PIN bilgisinin ve son kullanıcı bilgisayarındaki hakların saldırganlar tarafından ele geçirilmesi halinde kişi adına imza oluşturulabilir. Bu sebeple PIN bilgisinin saklanması tavsiye edilmez.

18. PIN bilgisi saklandığı takdirde EYP oluşturma uygulamasının, karta "log in" olduktan belirli bir süre sonra (maksimum 30 dakika) "log out" olması gerekmektedir. Uygulamanın bir kez “log in” olup, sınırsız imzalamaya izin vermesi kabul edilmemektedir. Güvenlik açısından önerilen metot, imzalama işlemi bittikten sonra hemen “log out” olunmasıdır.

19. Sertifika seçimi yapılmadan PIN girişine izin verilmemelidir. EYP oluşturma uygulamasındaki PIN girme alanının, PIN girilmeye başladıktan bir süre sonra imzalama işlemi bitirilmediği takdirde temizlenmesi gerekmektedir. PIN alanını temizlemek için bekleme süresi maksimum 30 saniyedir.

20. EYP uygulama arayüzünde imzalı ve imzasız belgeler ayırt edilebilir olmalıdır. Belgenin niteliğine göre ilgili seçenekler gösterilmelidir.

21. Kullanıcı, imzalama işleminden sonra imzanın/mührün oluşup oluşmadığına dair anlaşılır bir şekilde bilgilendirilmelidir.

22. Uygulamada imza/mühür oluşturma işlemine dair log tutulmalıdır. Log, en az işlem tarihi, imzanın oluşturulma/oluşturulamama durumu ve imza sahibi bilgilerini içermelidir.

23. Uygulama, imza oluşturma aşamasında zaman damgası alırken, zaman damgasının geçerlilik kontrolünü yapmalıdır. TÜBİTAK API kullananlar bu özelliği aktive etmek için imza oluşturma kodundaki parametrelere aşağıda belirtilen eklemeyi yapmalıdır:

CAdES	`params.put(EParameters.P_VALIDATE_TIMESTAMP_WHILE_SIGNING, true);`

Testte kullanılacak zaman damgası sunucularının erişim bilgileri aşağıda verilmiştir. Testler esnasında varsayılan olarak TSA1 zaman damgası sunucunun ayarlanması gerekmektedir.

Kullanıcı Adı: *1*	***Şifre:*** *12345678 (Tüm hesaplar için kullanıcı adı ve şifre aynıdır.)*
TSA1: http://zdsA1.test3.kamusm.gov.tr	**TSB:** http://zdsB.test3.kamusm.gov.tr
TSA2: http://zdsA2.test3.kamusm.gov.tr	**TSC1:** http://zdsC1.test3.kamusm.gov.tr
TSA3: http://zdsA3.test3.kamusm.gov.tr	**TSC2:** http://zdsC2.test3.kamusm.gov.tr
TSA4: http://zdsA4.test3.kamusm.gov.tr	**TSC3:** http://zdsC3.test3.kamusm.gov.tr
TSA5: http://zdsA5.test3.kamusm.gov.tr	**TSD**: http://zdsD.test3.kamusm.gov.tr

24. Sunucu erişim bilgilerinin kod içeriğinden ayarlanması ve uyum değerlendirme testlerinden sonra değişmesi durumunda uygulama özet değeri bozulacaktır. Bu nedenle zaman damgası sunucu erişim bilgilerinin koddan bağımsız bir şekilde konfigüre edilmesi tavsiye edilmektedir.
25. EYP'de imzaya dahil olan ve olmayan bileşenler ile ilgili kullanıcı bilgilendirilmelidir.
26. NES içeriğinde maddi limit bilgisi olduğu takdirde sertifika doğrulama yapılırken aşağıdaki yöntemlerden biri izlenmelidir:
    a. Sertifikada bulunan maddi limit ile belgenin maddi içeriğinin karşılaştırılmadığı durumda, kullanıcıya imzacı sertifikasında maddi limit bilgisi olduğu uyarısı verilmeli ve imzanın oluşturulup oluşturulmayacağı EBYS uygulaması politikalarına göre belirlenmelidir.
    b. Sertifikada bulunan maddi limit ile belgenin maddi içeriğinin karşılaştırıldığı durumda:
        i. Sertifika maddi limiti belge maddi değeri için yeterli ise imza oluşturulmalıdır.
        ii. Sertifika maddi limiti belge maddi değeri için yeterli değil ise imza oluşturulmamalıdır.
27. Uygulama, mühür için arşivleme modülüne sahip olmalıdır. Arşivleme modülü Ek-B'de verilen "İmza Arşivleme Rehberi"nde belirtilen talimatlara uygun olarak geliştirilmelidir.
28. Uygulamada kullanılan sertifika deposu, imza modüllerine ilişkin politika ve konfigürasyon dosyalarının güvenliği sağlanmalıdır.
29. İmza oluşturma, doğrulama ve arşivleme uygulaması, kullanıcı ile uygulama arasında akan verilerin bütünlüğünü ve gizliliğini korumalıdır (SSL sertifikası kullanımı vb.).
30. Uygulama, akıllı kart ve/veya HSM cihazını desteklemelidir.
31. Uygulamada mühür bileşenine seri ve paralel mühür eklenmesine izin verilmemelidir.
32. Uygulamada paket oluşturulurken imza bileşeni doğrulanamıyorsa, mühür bileşeninin eklenmesine izin verilmemelidir.
33. Kurumun test mühür sertifikası bulunmaması durumunda, Uyum Değerlendirme sürecinde kullanılmak üzere belirli süreli test mühür sertifikası sağlanacaktır. Uyum değerlendirme testleri öncesi ilgili sertifika talebi yapılmalıdır.

4 İmza Doğrulama Testleri Ön İsterleri

1. Göndermiş olduğumuz imzalı EYP paketlerini EBYS uygulamasına dâhil etmeniz ve doğrulama testleri için hazır hale getirmeniz gerekmektedir.

2. Uygulamada oluşturulan bir EYP paketi T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından sağlanan "e-Yazışma Test Platformu" web arayüzü aracılığıyla doğrulanabilmelidir.

3. Uygulamada, RSA anahtarlı sertifikalarla oluşturulan imzaların yanı sıra Eliptik Eğri anahtarlı sertifikalarla oluşturulan imzaların da doğrulanmasına izin verilmelidir.

4. Uygulama arayüzünde imzalı ve imzasız belgeler ayırt edilebilir olmalıdır. Belgenin niteliğine göre ilgili seçenekler gösterilmelidir.

5. Uygulama, doğrulanacak paketin seçilmesine ve imzalanan içeriğin gösterilmesine imkân vermelidir.

6. İmza doğrulama ekranında imzacının isim bilgisi, imza zamanı ve imzanın genel doğrulama sonucu açıkça belirtilmelidir. Kullanıcı istediği takdirde imzacının sertifika bilgilerinin ve doğrulama sonuçlarının tamamını ayırt edilebilir şekilde görüntüleyebilmelidir. Uygulama sertifikayı işletim sisteminin sertifika görüntüleyicisi vasıtasıyla da gösterebilir.

7. Seri/Paralel imzacılar, doğrulama ekranında hiyerarşik bir düzende ağaç yapısına benzer şekilde gösterilmeli ve imzalar doğrulanırken kullanıcıyı net bir şekilde bilgilendirecek genel doğrulama sonucu ve imzacıların ayrı ayrı doğrulama sonuçları yer almalıdır.

8. İmza/mühür doğrulama sonuçları kullanıcıya anlaşılır şekilde gösterilmelidir. Kullanıcı bilgilendirmelerinde standart hata dönülmemeli, bilgilendirmeler hatayı net ifade edecek şekilde olmalıdır.

9. İmza ve mühür bileşenleri için imzaya dahil olan imza özelliklerinden "mime-type" imza özelliği ile imzalanan dosya türü karşılaştırılmalıdır. Eşleşmediği durumlarda imza doğrulanmamalıdır ve kullanıcı bilgilendirilmelidir.

10. TÜBİTAK API kullananlar, imza doğrulama kodundaki parametrelere aşağıda belirtilen eklemeleri yapmalıdır:

CAdES (Native API)	`params.put(EParameters.P_FORCE_STRICT_REFERENCE_USE, true);`

CAdES (Common API)	esya-signature-config.xml'de params içerisine aşağıdaki parametre eklenmelidir.
	
	`<!--loosening below 2 settings will cause warnings instead of validation failure-->`
	`<!--referenced validation data must be used for cert validation is set true-->`
	`<force-strict-reference-use>true</force-strict-reference-use>`

11. TÜBİTAK API kullananların, sistem saati ve zaman damgası arasındaki saat farkından oluşabilecek sorunların önüne geçmek için imza doğrulama kodunda *P_TOLERATE_SIGNING_TIME_BY_SECONDS* parametresini 7200 olarak set etmeleri tavsiye edilir.

12. Uygulamada geçersiz özet algoritması kontrolü yapılmalıdır. Bu sebeple uygulamanın kabul edilen özet algoritmaları listesi olmalıdır ve bu listede BTK'nın 24 Mart 2020 tarihli Resmi Gazete'de yayımlanan "ELEKTRONİK İMZA İLE İLGİLİ SÜREÇLERE VE TEKNİK KRİTERLERE İLİŞKİN TEBLİĞDE DEĞİŞİKLİK YAPILMASINA DAİR TEBLİĞ"in 1. maddesinde belirtilen özetleme algoritmaları bulunmalıdır. Uygulama, doğrulama aşamasında izin verilen algoritmalar dışında bir algoritma tespit ettiğinde, "Geçersiz Özet Algoritması, Mühür En Kısa Sürede Yeniden Arşivlenmelidir" uyarısı dönmelidir. Mührün statüsü geçerliyse, özet algoritması uyarısı sebebiyle geçersiz hale getirilmemelidir.

13. Uygulama, EYP paketinde paraf imza varsa Üstveri, Üst Yazı ve DED ekleri bileşenlerinin özetlerinin ParafOzeti.xml bileşeni içerisinde doğru bir şekilde yer aldığını kontrol etmelidir.

14. Uygulama; Üstveri, Üst Yazı, DED ekleri ve varsa Paraf İmza ile Paraf Özeti bileşenlerinin özetlerinin PaketOzeti.xml bileşeni içerisinde doğru bir şekilde yer aldığını kontrol etmelidir.

15. Uygulama; Üstveri, Üst Yazı, DED ekleri, Paket Özeti, Elektronik İmza, Core, Nihai Üstveri ve varsa Paraf İmza ile Paraf Özeti bileşenlerinin özetlerinin NihaiOzet.xml bileşeni içerisinde doğru bir şekilde yer aldığını kontrol etmelidir.

16. Uygulamada paraf imza oluşturulması zorunlu olmasa bile, paraf imza bulunduran bir paketin doğrulaması için paraf imza kontrolü yer almalıdır.

17. PaketOzeti.xml bileşeninin imzalandığı ve NihaiOzet.xml bileşeninin mühürlendiği kontrol edilmelidir.

18. Dağıtım listesinde bulunan kuruma özgü ekler kontrol edilmelidir. Dağıtım listesinde konulmamış ek listesinde yer alan eklerin kontrolü yapılmamalıdır.

19. Uygulama, NihaiÜstveri.xml bileşeninde yer alan imzacı bilgisi ile elektronik imza içerisindeki imzacı bilgisinin aynı olduğunu kontrol etmelidir.

20. İmzacı sertifikası içeriğinde maddi limit bilgisi varsa aşağıdaki yöntemlerden biri izlenerek imza kontrol edilmelidir:

    a. Sertifikada bulunan maddi limit ile belgenin maddi içeriğinin karşılaştırılmadığı durumda, kullanıcıya imzacı sertifikasında maddi limit bilgisi olduğu uyarısı verilmeli ve imzanın doğrulanıp doğrulanmayacağı EBYS uygulaması politikalarına göre belirlenmelidir.
    b. Sertifikada bulunan maddi limit ile belgenin maddi içeriğinin karşılaştırıldığı durumda:
        i. Sertifika maddi limiti belge maddi değeri için yeterli ise imza doğrulanmalıdır.
        ii. Sertifika maddi limiti belge maddi değeri için yeterli değil ise imza doğrulanmamalıdır.

5 Uyum Değerlendirme Test Süreci Hakkında Bilgilendirmeler

Değerlendirmeye alınan kuruluşlar tarafından, yukarıda belirtilen maddelerin uyum değerlendirme çalışması öncesi tamamlanması gerekmektedir. Bu çalışmalar sonrasında uyum değerlendirme süreci başlayacaktır. Bu maddeler uyum değerlendirme sürecinin temel maddeleridir, değerlendirme sürecinde bu maddeler dışında farklı kontroller de yapılacaktır.

Ön Hazırlık çalışması tamamlandıktan sonra kuruma randevu tarihi verilir. Randevu tarihi uyum değerlendirme hizmetinin resmi olarak başladığı tarihtir. Test süreci ilk randevu tarihinden itibaren en fazla 50 iş günü içerisinde tamamlanmış olmalıdır, aksi takdirde sürecin bedeli kurum tarafından ödenerek yeniden başlatılması gerekmektedir.

EYP Uyum Değerlendirme testleri beş ana bölümden oluşmaktadır. İlk bölüm olan Format Testi'nde, uygulama kullanılarak oluşturulmuş imzalı dosyaların ilgili standartlarda belirtilen imza formatlarına uygunluğu kontrol edilir. Ayrıca bu bölümde, EYP formatının uygunluğu "e-Yazışma Teknik Rehberi" sürüm 2.0' a göre kontrol edilir. Format Testinden sonraki bölüm olan İmza Oluşturma Testinde, sertifika ve zaman damgası doğrulama ile ilgili kontroller yapılarak güvenli elektronik imza oluşturma yazılımının uygunluğu test edilir. İmza Doğrulama Testi'nde imza doğrulama testleri yapılarak güvenli elektronik imza doğrulama yazılımının uygunluğu test edilir. İmza Arşivleme Testinde arşivleme uygulamasının değerlendirilmesi yapılır. Son bölüm olan Gerçek Ortam Testinde ise uygulamanın gerçek ortamda olması gerektiği gibi çalıştığının kontrolü yapılır.

Yukarıda ana bölümleri belirtilen Uyum Değerlendirme test maddelerinin uygulamada sağlanmadığı tespit edilirse, kuruma eksikliklerini tamamlaması, uygulamadaki hataları düzeltmesi için zaman tanınır. Kurum hataları düzelttiğini belirttikten sonra tekrar randevu tarihi verilerek test sürecine devam edilir. Test yapılan uygulama, EYP Uyum Değerlendirme Raporu'nda belirtilen zorunlu olarak sağlanması gereken maddelerin tamamını sağlayana kadar, kuruma hataları iletme, randevu verme ve test sürecine devam etme işlemleri tekrarlanır. EYP Uyum Değerlendirme Raporu'nda belirtilen tüm zorunlu maddeler sağlandığında, Uyum Değerlendirme testleri tamamlanmış olur.

Uyum Değerlendirme testleri tamamlandıktan sonra uygulamanın arayüz, politika, imza oluşturma, doğrulama, arşivleme kısımlarına ve kullanılan e-imza kütüphanesine (TÜBİTAK ESYA API hariç) ait SHA-256 özet değerlerinin 1 (bir) iş günü içinde, Uyum Değerlendirme Taahhütname Formu'nda belirtilmesi ve bu formun ıslak imzalı ve kaşeli halinin tarafımıza iletilmesi gerekmektedir. Aksi takdirde süreç yenilenecektir. Kurumun Uyum Değerlendirme Taahhütname Formu'nda belirtmiş olduğu özet değerleri Uyum Değerlendirme Raporu'na yazılır ve raporun onaylanmasının ardından özet değerleri https://kamusm.bilgem.tubitak.gov.tr internet sitesinden ilan edilir.

6 Ek-A Kripto Suit Testleri Bilgilendirme Yönergesi

RSA algoritmasında anahtar uzunluğuna göre özet algoritması seçimi konusunda kriptografik olarak bir kısıt bulunmazken Eliptik Eğri anahtar kullanılarak oluşturulan imzaların kriptografik anlamda güvenli sayılabilmesi için anahtar uzunluğuna uygun özet algoritması kullanılması gerekmektedir[1].

Kamu SM, ETSI TS 119 312 Electronic Signatures and Infrastructures; Cryptographic Suites standardını dikkate alarak hem güvenliği artırmayı hem de ortak çalışabilirliği sağlamayı esas almaktadır. Bu doğrultuda, Tablo 1'de verilen anahtar ve özet algoritması kombinasyonları dikkate alınmalıdır. E-imza uygulamaları, son kullanıcı sertifikasının anahtarını tespit etmeli ve Eliptik Eğri anahtarlar için imza algoritması seçimini kullanıcı tercihine bırakmamalıdır.

Eliptik Eğri anahtarlı sertifikalar ile imza oluşturma işlemlerinde ilgili standarda uygunluğu sağlamak için Tablo 1'de belirtilen her bir anahtar için ilgili özet algoritmasının kullanılması gerekmektedir. Belirtilenler dışında bir anahtar uzunluğuna sahip sertifika ile imza oluşturulamaması beklenmekte ve belirtilenin dışında bir anahtar-özet algoritması kombinasyonu kabul edilmemektedir.

Tablo 1. Eliptik Eğri Anahtarlar için Özet Algoritması Seçimi

Anahtar	Özet Algoritması	İmza Algoritması
NIST P-256 (OID: 1.2.840.10045.3.1.7)	SHA-256	ECDSA_SHA256
NIST P-384 (OID: 1.3.132.0.34)	SHA-384	ECDSA_SHA384
NIST P-521 (OID: 1.3.132.0.35)	SHA-512	ECDSA_SHA512

P-256, P-384 ve P-521 anahtarlı sertifikalar ile imza oluşturulabilmelidir. Bununla birlikte P-256 anahtarlı bir sertifika için sadece SHA-256, P-384 anahtarlı bir sertifika için sadece SHA-384 ve P-521 anahtarlı bir sertifika için sadece SHA-512 özet algoritmasının kullanımı sağlanmalıdır.

TÜBİTAK MA3 API kullanılması durumunda imza oluşturma işlemi için aşağıda belirtilen ayarlamaların yapılması gerekmektedir.

- Kullanılan e-imza kütüphanesinin Eliptik Eğri desteği olduğundan emin olunmalıdır. TÜBİTAK MA3 API, Eliptik Eğri algoritmasını desteklemektedir, https://yazilim.kamusm.gov.tr/?q=/node/14 adresinde yer alan güncel sürüm kullanılabilir.
- Eliptik Eğri imza oluşturabilmek için *ECUtil.getConvenientECSignatureAlgForECCertificate* adlı metot kullanılarak Tablo 1'e uygun şekilde algoritma seçimi yapılması sağlanmalıdır. Bu metodun kullanımına yeni sürüm API'nin *SmartCardManagerBase* sınıfındaki örnek kodlardan erişilebilir.
- Akisp11.dll'in güncel sürümünün kullanıldığından emin olunmalıdır. Akisp11.dll'in güncel sürümüne https://kamusm.bilgem.tubitak.gov.tr/islemler/surucu_yukleme_servisi/ adresinden ulaşılabilir.

[1] *ETSI TS 119 312, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites*

7 Ek-B İmza Arşivleme Rehberi

Arşiv imza, e-imzalı belgelerin sertifika makamına ait kök/alt kök, OCSP ve zaman damgası sertifikalarının geçerlilik süresinden daha uzun bir süre saklanması gerektiği durumlarda kullanılması gereken imza tipidir.

Arşivleme, sertifika makamına ait sertifikaların geçerlilik süresinin sonuna yaklaşılması, sertifikaların iptal olması veya kullanılan algoritmaların geçerliliğini yitirmesi durumlarında yapılır. Arşivlemenin yukarıdaki durumlar oluşmadan önce yapılmasında da bir sakınca yoktur. Arşivleme, hali hazırda arşiv tipindeki imzalı dosyaların içindeki son arşiv zaman damgasının geçerliliği tehlikeye girdiği takdirde, ESHS tarafından yeni bir hiyerarşiden yayınlanmış zaman damgası ayarları girilerek tekrarlanmalıdır. Uygulama tarafında ise ilgili altyapı sağlanmış olmalıdır.

Aşağıdaki bölümde arşivleme ihtiyacı gerektirecek senaryolar belirlenmiştir.

Arşivleme Senaryoları:

1. Sertifika ile ilgili senaryolar
    a. OCSP sertifikasının iptal olma ve süresinin dolma durumu
    b. İmza ZD sertifikasının iptal olma ve süresinin dolma durumu
    c. “İmza ve referans zaman damgası” ya da “referans zaman damgası” sertifikasının (eğer imzada varsa) iptal olma ve süresinin dolma durumu
    d. Arşiv ZD sertifikasının süresinin dolma durumu
    e. Alt kök sertifikasının iptal olma ve süresinin dolma durumu
    f. Kök sertifikasının süresinin dolma durumu
2. Güvenilir kök deposu değişiklikleri ile ilgili senaryolar
    a. Kök Sertifikasının kara listeye girme durumu
3. Algoritma geçersizlikleri ile ilgili senaryolar
    a. İmza zaman damgası algoritmasının geçersiz olma durumu
    b. “İmza ve referans zaman damgası” ya da “referans zaman damgası” (eğer imzada varsa) algoritmasının geçersiz olma durumu
    c. Arşiv zaman damgası algoritmasının geçersiz olma durumu
    d. İmza algoritmalarının geçersiz olma durumu

Senaryoları sağlamak adına kurulması istenen işleyiş aşağıda anlatılmakta ve sözde (pseudo) kodu verilmektedir.

1. Sistemin arka planında çalışacak uygulama kullanıcıdan bağımsız olarak toplu işlem (batch process) yapmalıdır.
2. İçerisine güvenilirliğini yitirmiş kök sertifikaların özet değerlerinin eklenebileceği kara liste (blacklist) yapısı kurulmalıdır.
3. Güvenli algoritmaların eklenebileceği beyaz liste (whitelist) yapısı kurulmalıdır.

CAdES API'de arşivleme işleminin aşağıda yazan sözde koda göre gerçeklenmesi tavsiye edilmektedir.

```
//Arşiv kontrolünden geçecek mühürler toplanır ve tek tek kontrolden geçirilir.
List<Signature> signatureFileList = getAllSignatures();

foreach(Signature s in signatureFileList){
    //Öncelikle imza doğrulaması yapılır, imza doğrulanmadığı takdirde arşivlenmez ve hata
loglanır.
    //İmza doğrulama işleminde algoritmalar için whitelist ve sertifikalar için blacklist
kontrolü yapılmaz.
    if (verifySignature(s)) {

        //Son arşiv zaman damgasının algoritmaları alınır.
        List<String> lastArchiveTSAlgorithmList = getLastArchiveTSAlgorithms(s);

        //Geçerli algoritma listesi alınır. Eğer yakın zamanda geçersiz olacak
        //algoritma varsa bu listeden çıkarılmalıdır. Son arşiv zaman damgasındaki
        //algoritmalar geçerli algoritma listesiyle karşılaştırılır.
        boolean isAlgorithmInWhiteList =
isAlgorithmInWhiteList(lastArchiveTSAlgorithmList);

        //Son arşiv zaman damgasında geçersiz algoritma varsa imza arşivlenir.
        if (!isAlgorithmInWhiteList) {
            archive(s);
            log("Son arşiv zaman damgasında geçersiz algoritma bulunması sebebiyle imza
yeniden arşivlendi.");
            continue;
        }

        //Son arşiv zaman damgası sertifikası alınır.
        Certificate lastArchiveTSCertificate = getLastArchiveTSCertificate(s);

        //Son arşiv zaman damgası sertifika süresinin dolmasına 2 aydan az kaldıysa
        //yeni arşiv zaman damgası ayarları yapılır ve imza arşivlenir.
        Date certificateExpirationDate =
getCertificateExpirationDate(lastArchiveTSCertificate);
        if (certificateExpirationDate < Date.now + 2 months) {
            newArchiveTsSettings();
            archive(s);
            log("Sertifika süresinin dolmasına 2 aydan az kaldığı için imza yeniden
arşivlendi.");
            continue;
        }
        //Son arşiv zaman damgası sertifikası doğrulanamazsa yeni arşiv zaman damgası
        //ayarları yapılır ve imza arşivlenir.
        if (!verifyCertificate(lastArchiveTSCertificate)) {
            newArchiveTsSettings();
            archive(s);
            log("Sertifika doğrulanamadığı için imza yeniden arşivlendi.");
            continue;
        }

        //Son arşiv zaman damgası kök sertifikası alınır.
        Certificate lastArchiveTSRootCertificate =
getLastArchiveTSRootCertificate(lastArchiveTSCertificate);
        //Son arşiv zaman damgası kök sertifikasının kara listede olup olmadığına
        //bakılır. İptal olan kök sertifikalar öncelikle bu listeye eklenmiş olmalıdır.
        boolean isInRootCertificateBlackList =
isInRootCertificateBlackList(lastArchiveTSRootCertificate);

        //Son arşiv zaman damgası kök sertifikası kara listedeyse yeni arşiv zaman
        //damgası ayarları yapılır ve imza arşivlenir.
```

```
            if (isInRootCertificateBlackList) {
                newArchiveTsSettings();
                archive(s);
                log("Son arşiv zaman damgası kök sertifikası kara listede olduğu için imza
yeniden arşivlendi.");
                continue;
            }

            log("İmzanın arşivlenmesine gerek yok.");

        } else
            log("İmza doğrulanamadığı için arşivlenmedi.");
}
```

EYP Uygulamalarında yapılacak olan arşivleme işlemi, arşiv imza tipinde oluşturulan mührün arşivlenmesi testlerinden oluşmaktadır.

Arşivleme testlerinin tarafımızca yapılabilmesi için toplu işlemi (batch process) tetikleyip logların alınabileceği ve sonrasında arşivlenen dosyaların indirilebileceği geçici basit bir arayüz yapılmalıdır. Arayüz, kara listeye eklenen kök sertifikalarını ve beyaz listeye eklenen özet algoritmalarını görmeye imkan vermelidir.