Bu doküman, Kamu SM tarafından kurulacak yeni nitelikli elektronik sertifika (NES) altyapısına geçiş sürecinde TÜBİTAK ESYA E-İmza Kütüphaneleri’ni kullanan uygulamalara rehberlik sağlamak amacıyla oluşturulmuştur. Testin hedef kitlesi ESYA API kullanarak kendi uygulamalarını geliştiren kurumlar veya entegratör firmalardır. **Eğer e-imza uygulamanızı kendiniz geliştirmediyseniz, lütfen entegratörünüzle iletişime geçerek ilgili testlere katılım sağlamasını ve testten geçen güncel uygulamayı sizinle paylaşmasını isteyiniz.**

Hali hazırda e-imza uygulaması barındıran sistemlerin geçişten olumsuz olarak etkilenmemesi için, yeni NES altyapısı kurulmadan evvel, aynı altyapı test ortamında kurulmuş ve uygulama geliştiricilere uygulamalarını test etme imkanı sağlanmıştır.

Testler imza oluşturma ve doğrulama olmak üzere 2 kategoride gerçekleşecektir. İmza oluşturma testleri için tarafınıza imza kartı ve zaman damgası (ZD) hesabı iletilmiştir. **İmza kartının şifresi** kurye ile gönderilen zarf içerisinde yer almaktadır. İmza doğrulama testleri için ise yine tarafınıza imza doğrulama paketi içerisinde gönderilen imzalı dosyalar ve kök sertifikalarını kullanarak testlerinizi gerçekleştirebilirsiniz.

Eğer henüz imza kartı, ZD hesabı ve imza doğrulama paketi temin etmediyseniz, ana duyuruda belirtildiği şekilde başvurunuzu yaptığınız takdirde tarafınıza gönderilecektir.

## TEST SİSTEMİ

Yeni kurulan sertifika hiyerarşisinde kök ve alt kök sertifikaları Eliptik Eğri 384 anahtara sahip olacak şekilde üretilmiş; onun haricinde hiyerarşide yer alan NES, OCSP ve Zaman Damgası sertifikası anahtarlarında herhangi bir değişiklik yapılmamıştır. Kriptografik ortak çalışabilirlik kapsamında oluşturulan test sistemi, yeni sertifika altyapısıyla aynı şekilde oluşturulmuştur (Şekil 1).



Şekil 1. ECC 384 Test Sistemi

Testler için aşağıdaki adımların izlenmesi yeterlidir:

1.    API güncellemesi,

2.    Test kök sertifikasının güvenilir köklere tanıtılması,

3.    Zaman damgası hesap bilgilerinin değiştirilmesi.

## API Güncellemesi

TÜBİTAK ESYA API’nin yakın zamanda yeni sürümü yayımlanmıştır. Testlere başlamadan önce <https://yazilim.kamusm.gov.tr/?q=tr/node/14/surum> adresinde yer alan son sürümü kullandığınızdan emin olunuz.

## Test Kök Sertifikasının Güvenilir Köklere Tanıtılması

İmza Doğrulama Paketi içerisinde yer alan Eliptik Eğri 384 kök sertifikası test amaçlı oluşturulduğundan "SertifikaDeposu.svt" dosyası içerisinde yer almamakta; ilgili test kök sertifikasının uygulamanın güvenilir kökler deposuna tanıtılması gerekmektedir. Bunun için örn: D:\Trusted klasörü oluşturup kök sertifikalarını içine kopyaladıktan sonra, uygulamanın kullandığı policy.xml içerisinden aşağıdaki düzenlemenin yapılması yeterlidir:

|  |
| --- |
| <trustedcertificate>       <classname=*"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.TrustedCertificateFinderFromECertStore"*>             <param name=*"securitylevel"* value=*"legal"* />       </class></trustedcertificate> |

Gerçek ortamda, yeni üretilen kök sertifikasının güvenilir olarak tanınması için SertifikaDeposu.svt’yi yenilemeniz yeterli olacaktır. Test maksatlı üretilen kök sertifikasını, sahadaki uygulamalarınızı güncellerken güvenli kök sertifikaları arasında göstermemenizi önemle hatırlatmak isteriz.

## Zaman Damgası Hesap Bilgilerinin Değiştirilmesi

Testlerde <http://testzdec384.kamusm.gov.tr> zaman damgası kullanılmalıdır. Zaman damgası hesap bilgilerini aşağıda belirtildiği şekilde değiştirebilirsiniz. ZD sunucularında kriptografik algoritma anlamında değişiklik olmadığından digestAlg değişkeni SHA-512 olmalıdır.

|  |
| --- |
| Java API |
|  params.put(Eparameters.P\_TSS\_INFO, new TSSettings(“http://testzdec384.kamusm.gov.tr”, userID, pass, digestAlg)); |
| .NET API |
| params\_[EParameters.P\_TSS\_INFO] = new TSSettings([“http://testzdec384.kamusm.gov.tr”](http://testzdrsa4096.kamusm.gov.tr), userID, pass, digestAlg); |

## EK KONTROLLER

Testler esnasında kriptografik algoritma değişikliği dışında, güncel ESYA API’nin kullanımıyla ilgili dikkat edilmesi gereken birkaç husus aşağıda belirtilmektedir:

* TÜBİTAK ESYA API’nin bir önceki sürümünün bakım sözleşmesi sona erdiği için API güncellemesiyle birlikte bundle içerisinde yer alan lisans dosyasının da güncellenmesi gerekmektedir.
* API’nin eski sürümlerinde sistem saati ve zaman damgasındaki saat farklarından dolayı sorunlar oluşmaktaydı, bu sorunları çözmek için API güncellemesiyle birlikte yeni bir parametre eklenmiştir. Bu parametre ile zaman farkı göz ardı edilebilmektedir. İmza doğrulama tarafında sorun yaşamanız halinde aşağıdaki parametreyi kullanarak sorunun çözümünü sağlayabilirsiniz.

|  |
| --- |
| Java API |
|  params.put(Eparameters.P\_TOLERATE\_SIGNING\_TIME\_BY\_SECONDS , 3600); |
| .NET API |
| params\_[EParameters.P\_TOLERATE\_SIGNING\_TIME\_BY\_SECONDS]=3600; |

* Bütünleşik imzalı dosya doğrulanırken yanında belge verilmesi uygun değildir. İmzalanan belge bütünleşik imzanın içerisinden alınmalıdır. Bu kontrol ayrık imza beklenen sistemlere; bütünleşik imza ve imzalanan dışında farklı bir evrak vererek sistemi yanıltma çabasının önüne geçilmesi için düzenlenmiştir. Bütünleşik imza, harici içerik verilmeden doğrulanmalıdır.