ELEKTRONİK İMZA

KULLANIM PROFİLLERİ

REHBERİ

Sürüm 1.0

HAZİRAN 2012

İçindekiler

1. Amaç ve Kapsam 3
2. Dayanak 4
3. Tanımlar 5
4. Kısaltmalar 6
5. İmza Tipleri 7
6. Elektronik İmza Oluşturma ve Doğrulama 8
   - 6.1 Kesinleşme Süresi 8
   - 6.2 İlk Doğrulama 9
   - 6.3 Doğrulama Verisi 10
   - 6.4 Sonraki Doğrulama 10
7. Elektronik İmza Ömrü 10
8. İmza Profilleri 11
   - 8.1 Elektronik İmza Profili 1 (P1) 12
   - 8.2 Elektronik İmza Profili 2 (P2) 12
   - 8.3 Elektronik İmza Profili 3 (P3) 13
   - 8.4 Elektronik İmza Profili 4 (P4) 13
   - 8.5 Profillerde Kullanılan İmza Özellikleri 14
9. Periyodik Güncelleme (Arşivleme) 18

Ek A - Kaynakça 18

Ek B - Referanslar 19

1. Amaç ve Kapsam

23 Ocak 2004 tarihinde Resmi Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu ile elektronik imza ile ilgili ikincil düzenlemelerin hazırlanması ve Elektronik Sertifika Hizmet Sağlayıcı (ESHS)'larının denetlenmesi görevi Bilgi Teknolojileri ve İletişim Kurumu (BTK)'na verilmiştir. Bu görev kapsamında BTK tarafından hazırlanan "Sertifika Mali Sorumluluk Sigortası Yönetmeliği" 26 Ağustos 2004 tarihli ve 25565 sayılı Resmi Gazete'de ve "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" ile "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" 6 Ocak 2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Son olarak Hazine Müsteşarlığı tarafından "Sertifika Mali Sorumluluk Sigortası Yönetmeliği" doğrultusunda sigortaya ilişkin "Genel Şartlar, Tarife ve Talimatı" hazırlanmış ve bunlar 27 Ocak 2005 tarihli ve 25709 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. 2005 yılında tamamlanan bu düzenlemeler ile Elektronik Sertifika Hizmet Sağlayıcılarının (ESHS) kurulması ve işletilmesi için gerekli kurallar tanımlanmış belirli standartlara atıflar yapılarak Nitelikli Elektronik Sertifika (NES) ve güvenli elektronik imzayla ilgili genel çerçeve çizilmiştir.

2005 yılında ESHS'lerin faaliyete başlamasıyla birlikte ülkemizde elektronik imzaya ilişkin bir pazar oluşmaya başlamıştır. Uygulamalar gelişmeye başladıkça ESHS'lerin yayımladıkları NES'lerin aynı standarda uygun olarak oluşturulmasına rağmen standardın kesin olarak belirlemediği sertifika profilindeki bazı alanların ESHS'ler tarafından farklı kullanılmasından dolayı birlikte çalışabilirliğinin sağlanmasında sorunlar yaşanmaya başlamıştır. ESHS'lerin yayınladıkları NES'lerin birbiriyle uyumlu olması, birlikte çalışabilirliğin sağlanması amacıyla BTK'nın koordinasyonunda tüm ESHS'lerin birlikte hazırlayarak üzerinde anlaşmaya vardığı "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi" oluşturulmuş ve 18 Nisan 2007 tarih ve 2007/DK-77/207 sayılı Kurul Kararı ile yayınlanmıştır.

"Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi", ESHS'lerin oluşturdukları NES'ler arasında arzu edilen uyumu sağlamış olmakla birlikte NES'lere bağlı olarak oluşturulan güvenli elektronik imzaların uyumluluğu konusunda

sorunların yaşanmaya devam ettiği belirlenmiştir. Yaşanan bu sorunların da çözüme kavuşturulabilmesi için güvenli elektronik imza oluşturma ve doğrulama süreçlerinde kullanılabilecek imza profillerinin tanımlandığı bu rehber doküman oluşturulmuştur. Rehberde, ETSI TS 101 733, TS 101 903 ve TS 102 778 dokümanlarında anlatılan imza formatları temel olarak kabul edilmiş, imzaların uzun süreli kullanımında işlev ve güvenilirliklerini kaybetmemesi amacıyla yapılması gerekenlere yer verilmiştir.

Rehberde P1, P2, P3 ve P4 olmak üzere 4 farklı imza profili tanımlanmış ve bu profillerden P2, P3 ve P4 için elektronik imza politikaları da ayrı dokümanlar olarak yayımlanmıştır. Bu imza politikaları dokümanları CAdES, XAdES ve PAdES için birlikte hazırlanmıştır. P2, P3 ve P4 profillerine göre oluşturulan imzaların içeriğinde "Signature-policy-identifier" imza özelliğinin bulunması zorunludur. Bu şekilde oluşturulan imzaların ETSI TS 101 733 V1.8.1, ETSI TS 101 903 V1.4.2 ve ETSI TS 102 778-3 V1.2.1 ile ETSI TS 102 778-5 V1.1.2 dokümanlarında tanımlanan "*Explicit Policy Electronic Signatures* (EPES)" imza formatına uygun olarak oluşturulması gereklidir.

2. Dayanak

6 Ocak 2005 tarih ve 25692 sayılı Resmi Gazete yayımlanan 5070 Sayılı Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 35 inci maddesinde "Elektronik imzayla ilgili bu Yönetmelikte hüküm bulunmayan haller için Kurul Kararı ile düzenleme yapılır" hükmü yer almaktadır.

Bu bağlamda ESHS'lerin yayınladıkları nitelikli elektronik sertifikalara bağlı olarak oluşturulan güvenli elektronik imzaların birbiriyle uyumlu olması ve birlikte çalışabilirliğin sağlanması açısından varolan ihtiyaçların karşılanmasına yönelik olarak söz konusu Yönetmeliğin 35 inci maddesine istinaden "Elektronik İmza Kullanım Profilleri Rehberi" oluşturulmuştur.

3. Tanımlar

Nitelikli Elektronik Sertifika: 5070 sayılı Elektronik İmza Kanunu'nun 9 uncu maddesinde tanımlanan elektronik sertifika.

Güvenli Elektronik İmza: 5070 sayılı Elektronik İmza Kanunu'nun 4 üncü maddesinde tanımlanan elektronik imza.

Gelişmiş Elektronik İmza: Oluşturulmasından uzun süre sonra imzanın güvenilir bir şekilde doğrulanabilmesi için doğrulamada kullanılacak zaman damgası, son kullanıcı sertifikaları ve ESHS'ye ait sertifikalar ile ilgili tüm sertifikaların iptal verilerinin veya bu verileri tanımlayıcı referans bilgilerinin imza dosyasına eklenmesi ile elde edilen elektronik imza formatı.

İptal Bilgisi: Bir sertifikanın belirli bir zamanda geçerli olup olmadığını belirten ve sertifikayı veren ESHS veya onun yetkilendirdiği güvenilir bir makam aracılığıyla duyurulan sertifika iptal bilgisi (SİL, ÇiSDuP)

ÇiSDuP: İptal bilgisinin ESHS'ye ait sunucular üzerinden sorgulama yapılarak kontrol edilmesine imkân veren standart yöntem. Bu dokümanda ÇiSDuP üzerinden yayınlanan iptal bilgilerinin "gerçek zamanlı" olduğu yani iptal duyurusunun iptal talebinin alındığı anda yayıldığı kabul edilmiştir.

Kesinleşme Süresi (Grace Period): Sertifikaya ait iptal bilgisinin ilgili kanallarda yayılması için imza zamanından sertifikanın iptal kontrolünün yapılacağı zamana kadar beklenmesi gereken süre.

Zaman Damgası: Zaman damgası bir verinin belirli bir tarihten öncesinde varolduğunu ispatlamak için kullanılır. Bir imza atılırken, bu imza için bir de zaman damgası alınarak imzanın hangi tarihten önce oluşturulduğu ispatlanır. Eğer zaman içinde sertifika iptal edildi ise, imzanın iptalden önce atıldığını teknik olarak ispatlamak için de zaman damgası gerekmektedir.

4. Kısaltmalar

BTK : Bilgi Teknolojileri ve İletişim Kurumu

CAdES (CMS Advanced Electronic Signatures) : CMS Gelişmiş Elektronik İmza

CMS (Cryptographic Message Syntax) : Kriptografik Mesaj Sözdizimi

ESHS : Elektronik Sertifika Hizmet Sağlayıcısı

EPES (Explicit Policy Electronic Signatures) : Belirlenmiş Politika Temelli Elektronik İmza

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

ETSI TS (ETSI Technical Specification) : ETSI Teknik Özellikleri

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

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

ITU (International Telecommunication Union) : Uluslararası Telekomünikasyon Birliği

NES : Nitelikli Elektronik Sertifika

PAdES (PDF Advanced Electronic Signatures) : PDF Gelişmiş Elektronik İmza

PAdES-LTV (PAdES Long Term Validation) : PAdES Uzun Dönem Doğrulama

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

SHA (Secure Hash Algorithm) : Güvenli Özet Algoritması

SİL : Sertifika İptal Listesi

XAdES (XML Advanced Electronic Signatures) : XML Gelişmiş Elektronik İmza

XFA (XML Forms Architecture) : XML Form Mimarisi

XML (Extensible Markup Language) : Genişletilebilir İşaretleme Dili

5. İmza Tipleri

Bu rehberde anlatılan elektronik imza formatları;

- CAdES için ETSI TS 101 733 V1.8.1,
- XAdES için ETSI TS 101 903 V1.4.2 ve
- PAdES için ETSI TS 102 778-3 V1.2.1, ETSI TS 102 778-4 V1.1.2, ETSI TS 102 778-5 V1.1.2

dokümanlarına uygun olarak gerçeklenmelidir. Bu imza formatlarından bazıları arasında çok küçük farklar bulunması nedeniyle elektronik imza alanında birlikte çalışabilirlik ve uyumluluk sağlanabilmesi için bu rehberde,aşağıda tanımlarına yer verilen elektronik imza formatlarından sadece bazılarının kullanımı zorunlu tutulmuştur.

BES (Basit Elektronik İmza) : BES, içinde imza zamanına ait bilgi bulundurabilir, ancak imza zamanını ispatlama özelliğinden yoksundur.

EPES (Belirlenmiş Politika Temelli Elektronik İmza) : EPES tipindeki bir elektronik imza, oluşturma ve doğrulama kurallarını belirleyen bir politikaya sahip olarak yaratılmış bir BES tipinde imzadır.

ES-T (Zaman Damgalı Elektronik İmza) : BES veya EPES tipindeki elektronik imzaya zaman damgası eklenerek elde edilen elektronik imza formatıdır.

ES-C (Doğrulama Verisi Taşıyan Elektronik İmza) : Doğrulama verilerinin referanslarını içeren ES-T formatından türetilen bir elektronik imza formatıdır.

ES-X (Genişletilmiş Elektronik İmza) : ES-C formatından türetilen ve sadece doğrulama verilerinin referanslarına veya ES-C'nin tamamına zaman damgası eklenerek elde edilen elektronik imza formatıdır.

ES-XL (Genişletilmiş Uzun Elektronik İmza) : Doğrulama verisini kendi içinde barındıran elektronik imza tipidir.

ES-A (Arşiv Elektronik İmza) : Kriptografik metodların zaman içinde koruyucu özelliğini yitirmesine karşı periyodik olarak alınan zaman damgası ile korunan elektronik imzadır.

6. Elektronik İmza Oluşturma ve Doğrulama

BES oluşturmanın teknik ayrıntıları ilgili ETSI standartlarında tanımlanmış olduğundan bu dokümanın kapsamı dışında tutulmuştur. BES oluşturulduktan sonra bu dokümanda anlatılan gelişmiş elektronik imza tiplerine dönüştürülmesi mümkündür. Bunun yanında BES içerisindeki "imza zamanı" özelliği ile elektronik imzanın zamanının kesin olarak ispatlanması mümkün olamayacağı gibi elektronik sertifika zincirindeki bir sertifikanın zaman içinde iptal edilmesi durumunda imzanın, sertifika iptalinden önce mi yoksa sonra mı oluşturulduğunun da belirlenmesi mümkün değildir. Bu nedenle de elektronik imzanın uzun dönem kullanımı için BES'in gelişmiş elektronik imzaya dönüştürülmesi gereklidir.

Gelişmiş elektronik imza oluşturmak için doğrulama verisinin toplanması ve zaman damgasının kullanılması gereklidir. SİL üzerinden kontrolü yapılan sertifika iptal bilgisinin sağlıklı olması için elektronik imza oluşturulduktan sonra kesinleşme süresi kadar beklenmesi gerekli olmakla birlikte sertifika iptal bilgisinin ÇiSDuP üzerinden kontrol edildiği durumlarda kesinleşme süresi kadar beklenmesi gerekli değildir.

6.1 Kesinleşme Süresi

Kesinleşme Süresi, elektronik sertifikaya ait iptal bilgisinin ilgili dizinlerde yayımlanmasına imkân sağlamak için beklenmesi gereken minimum süre olarak tanımlanmaktadır.

ESHS'lerin verdikleri sertifikalarla ilgili iptal bilgisini içeren SİL içerisinde SİL'in yayınlanacağı en geç zamanı gösteren bir sonraki güncelleme zamanını gösteren bir alan mevcuttur ve ESHS'ler bu zamandan önce mutlaka yeni SİL yayınlamak zorundadırlar.

Sertifika sahibi iptal talebini elektronik sertifikasını yayımlayan ESHS'ye ilettikten sonra iptal anında gerçekleşse bile sertifikanın iptal bilgisinin SİL'de yayınlanması ancak bir sonraki SİL yayın zamanı sonunda gerçekleşmektedir. Tüm ESHS'ler arasında standart bir yapının oluşturulabilmesi için uygun bir "Kesinleşme Süresi" nin belirlenmesi ve bu sürenin elektronik imza doğrulama işlemlerinde dikkate alınması gereklidir.

İşlemin kritikliğine göre ”Kesinleşme Süresi” uygulamasında

- Sertifika zincirindeki tüm sertifikalara uygulanır,
- Elektronik imza oluşturan sertifikaya uygulanır,
- Uygulanmaz

olmak üzere 3 farklı yaklaşım mevcuttur.

Bu dokümanda bahsi geçen profillerde uygulanacak “Kesinleşme Süresi”, ilgili elektronik imza politikaları dokümanlarında belirtilmiştir.

Her ne kadar güvenli bir doğrulama için Kesinleşme Süresi kadar beklenmesi gerekiyorsa da, elektronik imzanın bir iş sürecinin parçası olduğu senaryolarda teknik gerekçeleri ne olursa olsun bir işleme devam etmeden önce imza doğrulama için dakika ve hatta gün ölçeğinde beklemek kabul edilebilir değildir.

Bu sebeple elektronik imza altyapısı destekleyen uygulamalar, Kesinleşme Süresi tamamlanmadan önce yapılan ön doğrulama sonucuna göre işlem yapmalı ve Kesinleşme Süresi sonrasında yapılan doğrulama ardından doğrulama verisini toplamalıdır. Sonraki doğrulamada, sertifikaların Kesinleşme Süresi bitmeden iptal edildiğine dair bir bilgi elde edilirse elektronik imzaya dayanılarak yapılan işlemin iptali veya geri alınması yoluna gidilmeli ve elektronik imza sahibinin bu durumdan haberdar edilmesi gereklidir. İşlemin iptali veya geri alınması mümkün olmayan süreçlerde Kesinleşme Süresi uygulanmaması ve mutlaka ÇiSDuP ile doğrulama yapılması gereklidir.

6.2 İlk Doğrulama

İlk doğrulama, doğrulama verisinin de toplanması gereken süreç olması nedeniyle diğer doğrulama işlemlerinden ayrılır. İptal kontrolünün SİL üzerinden yapıldığı durumlarda ilk imza doğrulama işlemi Kesinleşme Süresi sonrasında gerçekleştirilir.

Eğer elektronik imzayı oluşturan ile imzayı arşivleyecek taraf aynı ise doğrulama verisini toplamak ve elektronik imza ile birlikte arşivlemek onun görevidir.

Elektronik imza, imzalayan sertifikanın ömründen daha uzun bir süre kullanılacaksa bu durumda ileri bir tarihte erişilemez olacak doğrulama verisinin mutlaka toplanması gereklidir.

6.3 Doğrulama Verisi

Doğrulama verisi, elektronik imzanın doğrulanması için imzayı oluşturan ve/veya doğrulayan tarafından toplanması gereken sertifikalar, iptal bilgisi ve zaman damgası gibi bilgilerin tamamından oluşur.

Bir elektronik imzanın uzun süre sonra doğrulanabilmesi için gereken doğrulama verisi;

- İmza sertifikası ve imza sertifikasına ait güven zincirindeki tüm sertifikalar,
- İmza sertifikası ve güven zinciri üzerindeki sertifikalara ait SİL/ÇiSDuP bilgileri,
- İlgili iptal verisi için gerekiyorsa sertifika zinciri ve bu zincire ait SİL/ÇiSDuP bilgileri

bileşenlerinden oluşur. Bununla birlikte imza içerisindeki her bir zaman damgası için

- Zaman damgası imza sertifikası ve bu sertifikaya ait güven zincirindeki tüm sertifikalar ile
- İlgili sertifikalara ait SİL/ÇiSDuP bilgileri de doğrulama verisi içerisinde yer almalıdır.

6.4 Sonraki Doğrulama

Elektronik imzanın ilk doğrulamasından daha sonra herhangi bir tarihte yapılan doğrulama işlemi sonraki doğrulama olarak isimlendirilir. Gelişmiş imzanın oluşturulması aşamasında yapılan ilk doğrulama işleminde toplanan Doğrulama Verisinin toplanarak ileri bir tarihte yapılabilecek doğrulama işlemleri için saklanmalıdır.

7. Elektronik İmza Ömrü

Elektronik imza oluşturma ve doğrulama süreçlerinde veya bir uygulamaya elektronik imza kabiliyeti eklenirken kullanılacak elektronik imzanın kullanım ömrünün belirlenmesi

gereklidir. Elektronik imzanın kullanım ömrü, ileride tekrar doğrulanabilme ihtiyacına göre üç kategoride incelenebilir:

- **Anlık Elektronik İmza**

  Anlık imzalar, kullanım ömrü bir sonraki iptal bilgisinin yayınlanmasından daha kısa olan imza tipidir. Örneğin; 4 saatte bir SİL yayınlanan senaryoda anlık imzaların ömrü bir kaç dakikadan başlayıp 4 saate kadar uzayabilir.

- **Kısa Ömürlü Elektronik İmza**

  Kısa ömürlü imzalar, imza ömrünün, imza sertifikasının kalan ömründen kısa olduğu imzadır. Kısa ömürlü imzalar sertifika ömrü kadar ömüre sahip olabilirler. Örneğin 3 yıla kadar.

- **Uzun Ömürlü Elektronik İmza**

  Uzun ömürlü imzalar, ilk iki kategoriye girmeyen imza sertifikasının ve imza sertifikasını imzalayan ESHS sertifikasının geçerlilik süresi dolduktan sonra da doğrulanabilecek imza tipidir.

8. İmza Profilleri

Tablo 1 - İmza Profilleri

Profil	İmza Ömrü	Zaman Damgası	İptal Bilgisi [1]	Kesinleşme Süresi	İmza Formatı	İmza Dosya Boyutu
P1	Anlık	Yok	SİL/ ÇiSDuP	Uygulanmaz	BES	Düşük
P2	Kısa	Var	SİL	Uygulanır	ES-T	Orta
P3	Uzun Süreli	Var	SİL	Uygulanır	ES-XL [3,4]	Çok yüksek
P4		Var	ÇiSDuP	Uygulanmaz [2]	ES-XL [4]	Yüksek

[1] İmza sertifikası için iptal bilgisi

[2] Kontrol edilecek ÇiSDuP bilgisinin "gerçek zamanlı" ÇiSDuP olduğu kabul edilmiştir.

[3] İmza ES-T tipinde atılır. Kesinleşme süresi sonrası ES-XL'a çevrilir.

[4] ES-XL formatı [2][3][5][6] da bahsi geçen XAdES-XL Type 1, CAdES-XL, PAdES-LTV formatlarına karşılık gelir.

8.1 Elektronik İmza Profili 1 (P1)

Anlık doğrulama gerektiren güvenlik ihtiyacı düşük seviyede olan uygulamalarda kullanılır. İmza doğrulayıcının eline geçtiği an, imza zamanı sayılır. Gelecekte imzayı tekrar doğrulama ihtiyacı olmayacak senaryolarda tercih edilmelidir.

Doğrulamada iptal bilgisine erişmek doğrulayıcının görevidir. Anlık kullanımda kesinleşme süresi kadar bekleme şansı yoktur. Güvenlik açısında doğrulamada SİL yerine "gerçek zamanlı" ÇiSDuP kullanılması tercih edilmelidir.

Avantajları	**Dezavantajları**
• Düşük imza boyutu	• Kullanım ömrü anlık • Doğrulamada SİL kulanılırsa güvenilirlik seviyesi düşük • İmza zamanı belirsiz • Doğrulama verisini içermediği için doğrulama güçlüğü

Bu imza profili tanımlanmış bir imza politikasına referans vermemektedir.

8.2 Elektronik İmza Profili 2 (P2)

ÇiSDuP erişimi bulunmayan ortamlarda kısa süreli kullanım ömrü olan imzalar tercih edilmelidir. ÇisDuP erişimi olan ortamlarda ise P4 profili kullanılmalıdır.

Avantajları	**Dezavantajları**
• Orta seviye imza boyutu • İmza zamanı ispatı	• Kullanım ömrü limitli • İmza doğrulama için kesinleşme süresi kadar bekleme gereksinimi • Doğrulama verilerini içermediğinden doğrulama güçlüğü

Bu imza profili ile oluşturulan imzaların "Kısa Dönemli ve SİL Kontrollü Güvenli Elektronik İmza Politikaları (Profil P2) [R.1]" dokümanının güncel versiyonuna uygun olması ve politika dokümanına referans vermesi zorunludur.

8.3 Elektronik İmza Profili 3 (P3)

ÇiSDuP erişimi olmayan ortamlarda kullanılabilir. Aksi durumda P3 profilinin, P4 profiline tercih edilebilecek herhangi bir avantajı yoktur, dezavantajları aşağıda listelenmiştir.

Avantajları	**Dezavantajları**
• Maksimum imza ömrü • Yüksek güvenilirlik • Doğrulama verilerini içerdiğinden doğrulama kolaylığı • İmza zamanı ispatı	• Yüksek imza boyutu • İmza doğrulama için kesinleşme süresi kadar bekleme gereksinimi

Bu imza profili ile oluşturulan imzaların " Uzun Dönemli ve SİL Kontrollü Güvenli Elektronik İmza Politikaları (Profil P3) [R.2]" dokümanının güncel versiyonuna uygun olması ve politika dokümanına referans vermesi zorunludur.

8.4 Elektronik İmza Profili 4 (P4)

En güvenilir, uzun ömürlü ve sorunsuz imza profilidir.

Avantajları	**Dezavantajları**
• Maksimum imza ömrü • Maksimum güvenilirlik • Doğrulama verilerini içerdiğinden doğrulama kolaylığı • İmza zamanı ispatı	• Görece yüksek imza boyutu

Bu imza profili ile oluşturulan imzaların "Uzun Dönemli ve ÇİSDuP Kontrollü Güvenli Elektronik İmza Politikaları (Profil P4) [R.3]" dokümanının güncel versiyonuna uygun olması ve politika dokümanına referans vermesi zorunludur.

8.5 Profillerde Kullanılan İmza Özellikleri

Aşağıdaki tabloda bu dokümanda anlatılan imza profillerine göre imza oluşturulurken eklenecek imza özellikleri ile ilgili kısıtlamalar belirtilmiştir. Zorunlu tutulan özelliklerin eklenmediği imzalar profile göre doğrulanamaz. Ancak profilde zorunlu tutulmayan özelliklerin imzaya eklenmiş olması durumunda imzayı doğrulayan tarafların isterlerse eklentiyi işleme almalarına imkan verilmiştir.

Tablo 2 - Profillerde Kullanılan İmza Özellikleri

	CAdES	XAdES	PAdES-CMS	PAdES-XFA	İmza Oluşturma				İmza Doğrulama			
					P1	P2	P3	P4	P1	P2	P3	P4
İmzalı Özellikler	Content-type	-	Content-type	-	Z	Z	Z	Z	Z	Z	Z	Z
	Message-digest	Reference/DigestValue	Message-digest	Reference/DigestValue	Z	Z	Z	Z	Z	Z	Z	Z
	ESS signing-certificate v2	SigningCertificate	ESS signing-certificate v2	SigningCertificate	Z	Z	Z	Z	Z	Z	Z	Z
	Signing-time[1]	SigningTime	M entry in the signature dictionary	CreateDate element defined within the XMP ns.adobe.com/xap/1.0/ namespace	Z	Z	Z	Z	Z	Z	Z	Z
	Content-reference	-	-	-	O	O	O	O	O	O	O	O
	Content-identifier	-	-	-	O	O	O	O	O	O	O	O

[1] Kullanıcı makinasındaki sistem saatinden veya kurumdaki bir sunucudan alınan zaman bilgisi imza sahibinin beyan ettiği imza zamanı olarak imzaya eklenir.

	Commitment-type-indication	CommitmentTypeIndication	Reason entry in the signature dictionary	CommitmentTypeIndication[2] description element defined within the Dublin Core http://purl.org/dc/elements/1.1/ namespace[3]	O	O	O	O	O	O	O	O
	Signer-location	SignatureProductionPlace	Location entry in the signature dictionary	SignatureProductionPlace	O	O	O	O	O	O	O	O
	Signer-attributes	SignerRole	Signer-attributes	SignerRole	O	O	O	O	O	O	O	O
	Content-time-stamp	AllDataObjectsTimeStamp IndividualDataObjectsTimeStamp	Content-time-stamp	AllDataObjectsTimeStamp IndividualDataObjectsTimeStamp	O	O	O	O	O	O	O	O
	Signature-policy-identifier[4]	SignaturePolicyIdentifier	Signature-policy-identifier	SignaturePolicyIdentifier	X	Z	Z	Z	O	Z	Z	Z
	sigPolicyQualifiers	SigPolicyQualifier	sigPolicyQualifiers	SigPolicyQualifier	X	Z	Z	Z	O	Z	Z	Z
	spuri	SPURI	spuri	SPURI	X	Z	Z	Z	O	Z	Z	Z
	sp-user-notice	SPUserNotice	sp-user-notice	SPUserNotice	X	O	O	O	O	Z	Z	Z

[2] İmza XAdES-BES ise kullanılır.

[3] İmza XAdES-EPES veya onun üzerine kurulmuş ise kullanılır.

[4] Bu dokümanda referans verilen ilgili imza politikaları dokümanına ait bilgiler bu özellik içinde belirtilmelidir.

	CAdES	XAdES	PAdES-CMS	PAdES-XFA	İmza Oluşturma				İmza Doğrulama			
					P1	P2	P3	P4	P1	P2	P3	P4
İmzasız Özellikler	CounterSignature	CounterSignature	PDF Serial Signature	CounterSignature	O	O	O	O	Z	Z	Z	Z
	Signature-time-stamp	SignatureTimeStamp	/Type/DocTimeStamp /SubFilter /ETSI.RFC3161	SignatureTimeStamp	O	Z	Z	Z	Z	Z	Z	Z
	SignedData certificates	XAdESv141:TimeStampValidationData/CertificateValues	/DSS/Certs Array /DSS/VRI/Cert Array	/DSS/Certs Array /DSS/VRI/Cert Array	O	O	Z	Z	O	Z	Z	Z
	SignedData crls	XAdESv141:TimeStampValidationData/RevocationValues	/DSS/CRLs Array /DSS/OCSPs Array /DSS/VRI/CRL Array /DSS/VRI/OCSP Array	/DSS/CRLs Array /DSS/OCSPs Array /DSS/VRI/CRL Array /DSS/VRI/OCSP Array	O	O	Z	Z	O	Z	Z	Z
	Complete-certificate-references	CompleteCertificateRefs	-	-	X	X	Z	Z	O	O	Z	Z
	attribute-certificate-references	AttributeCertificateRefs	-	-	X	X	O	O	O	O	O	O
	Complete-revocation-references	CompleteRevocationRefs	-	-	X	X	Z	Z	O	O	Z	Z
	attribute-revocation-references	AttributeRevocationRefs	-	-	X	X	O	O	O	O	O	O
	Certificate-values	CertificateValues	/DSS/Certs Array /DSS/VRI/Cert Array	/DSS/Certs Array /DSS/VRI/Cert Array	X	X	Z	Z	O	O	Z	Z
	-	AttrAuthoritiesCertValues	-	-	X	X	O	O	O	O	O	O

	Revocation-values	RevocationValues	/DSS/CRLs Array /DSS/OCSPs Array /DSS/VRI/CRL Array /DSS/VRI/OCSP Array	/DSS/CRLs Array /DSS/OCSPs Array /DSS/VRI/CRL Array /DSS/VRI/OCSP Array	X	X	Z[5]	Z[6]	O	O	Z	Z
	-	AttributeRevocationValues	-	-	X	X	O	O	O	O	O	O
	CAdES-C-time-stamp	-	-	-	X	X	X	X	O	O	O	O
	-	SigAndRefsTimeStamp	-	-	X	X	Z	Z	O	O	Z	Z
	CAdES-C-time-stamped-certs-crls-references	RefsOnlyTimeStamp	-	-	X	X	X	X	O	O	O	O
	Archive-time-stamp	xadesv141:ArchiveTimeStamp	/Type /DocTimeStamp /SubFilter /ETSI.RFC3161	/Type /DocTimeStamp /SubFilter /ETSI.RFC3161	X	X	O	O	O	O	Z	Z

Z: İmza oluşturmada zorunlu bulunması gereken alan, imza doğrulamada imzaya eklenmişse zorunlu işleme alınması gereken alan

O: İmza oluşturmada isteğe bağlı bulunabilecek alan, imza doğrulamada imzaya eklenmişse isteğe bağlı işleme alınabilecek alan

X: İmza oluşturmada bulunmaması gereken alan

[5] Kesinleşme süresi sonrası SİL'in imza özelliğine eklenmesi zorunludur.

[6] İmza zamanındaki ÇiSDuP değeri imza özelliğine eklenir.

9. Periyodik Güncelleme (Arşivleme)

Elektronik imzalı belgenin uzun ömürlü olabilmesi için oluşturulduktan sonra sadece arşivlenerek saklanması mümkün değildir çünkü uzun ömürlü imza kullanımı için bir süreç gereklidir. İmzanın oluşturulmasında kullanılan ve güvenliğini sağlayan algoritmalar teknolojinin gelişmesi ve bilgisayarların hızlanması, yeni kriptoanaliz yöntemlerinin geliştirilmesi gibi sebeplerle zayıf hale gelebilir. Elektronik imza standartlarında [2], [3], [5] bu gibi durumlarda kullanılabilmesi için ES-A (Arşiv İmza) formatı geliştirilmiştir. İmzanın saklanması gereken süre içinde belirli zaman aralıklarında imzanın arşiv formatında güncellenmesi gereklidir. Temel olarak, arşivleme için kullanılan zaman damgası sertifikasının süresi bitmeden önce yeni bir zaman damgası sertifikası ile yeniden arşiv zaman damgası alınmalıdır. Bir dokümanın elektronik ortamda güvenli olarak saklanabilmesi için ihtiyaç duyulan süre boyunca arşiv imza ile korunması gerekir. Bu amaçla zaman damgası sertifikalarının süresinin uzun tutulması önerilmektedir.

Ek A - Kaynakça

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[2] ETSI TS 101 733: " Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[3] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

[4] ETSI TS 102 778-3: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

[5] ETSI TS 102 778-4: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile.

[6] ETSI TS 102 778-5: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures.

[7] CWA 14171: "General Guidelines for Electronic Signature Verification".

Ek B - Referanslar

[R.1] "Kısa Dönemli ve SİL Kontrollü Güvenli Elektronik İmza Politikaları (Profil P2)", Sürüm 1.0, 1 Ekim 2011, TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi.

[R.2] "Uzun Dönemli ve SİL Kontrollü Güvenli Elektronik İmza Politikaları (Profil P3)", Sürüm 1.0, 1 Ekim 2011, TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi.

[R.3] "Uzun Dönemli ve ÇİSDuP Kontrollü Güvenli Elektronik İmza Politikaları (Profil P4)", Sürüm 1.0, 1 Ekim 2011, TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi.

Kısa Dönemli ve SİL Kontrollü Güvenli Elektronik İmza Politikaları (Profil P2)

OID:

2.16.792.1.61.0.1.5070.3.1.1

Sürüm 1.0

Haziran 2012

İÇİNDEKİLER

1. Giriş....4
2. Politikaların Yönetimi....5
   2.1. Politikanın Adı ve Tanımı....5
   2.2. Politikaların Tanımlandığı Formatlar....5
   2.3. Politikaların Yayınlanması....5
   2.4. Politikaların Güvenliği....6
   2.5. Politikaların Güncellenmesi....6
   2.6. Politikaların Arşivlenmesi....6
   2.7. İletişim Bilgileri....6
3. Politikaların Uygulanması....7
   3.1. İmzalayan Taraftaki İşlemler....7
   3.2. İmzayı Doğrulayan Taraftaki İşlemler....7
4. İmza Politikaları....8
   4.1. Genel İmza Politikaları Bilgisi....8
      4.1.1. İmza Politikaları Yayınlayan İsmi....8
      4.1.2. İmza Politikaları Nesne Tanımlama Numarası....8
      4.1.3. İmza Politikaları Geçerlilik Süresi....8
      4.1.4. Yayın Tarihi....9
      4.1.5. Uygulama Alanı....9
   4.2. Genel Kurallar (Common Rules)....9
      4.2.1. İmzalayan Tarafla İlgili Kurallar....9
         4.2.1.1. Ayrık veya Bitişik İmza Kullanımı....9
         4.2.1.2. Zorunlu Eklenen İmzalı Özellikler....9
         4.2.1.3. Zorunlu Eklenen İmzasız Özellikler....12
         4.2.1.4. Zorunlu Eklenen Sertifika Referansları....13
         4.2.1.5. Zorunlu Eklenen Sertifikalar....13
      4.2.2. Doğrulayan Tarafla İlgili Kurallar....13

4.2.2.1. Zorunlu Eklenen İmzasız Özellikler 13
4.2.3. Sertifikalar ile İlgili Kurallar 14
4.2.3.1. Sertifikaların Güvenilirliği ile İlgili Gereksinimler 14
4.2.3.2. Sertifika İptal Kontrolleri ile İlgili Gereksinimler 14
4.2.4. Zaman Damgası ile İlgili Kurallar 14
4.2.4.1. Zaman Damgası Sertifikalarının Güvenilirliği ile İlgili Gereksinimler 14
4.2.4.2. Zaman Damgası Sertifikalarının İptal Kontrolleri ile İlgili Gereksinimler 15
4.2.4.3. Kesinleşme Süresi 15
4.2.4.4. Zaman Damgası Gecikme Süresi 15
4.2.5. Yetkiler ile İlgili Kurallar 15
4.2.6. Kullanılan Algoritmalar ile İlgili Kısıtlamalar 15
4.3. İmza Amacı ile İlgili Kurallar (Commitment Rules) 16

1. Giriş

Bu elektronik imza politikası dokümanında, imzanın oluşturulması ve doğrulanmasında uyulması gereken kurallara yer verilmiş, politikalar belirlenmiştir. Bu politikalar, CAdES [4], XAdES [6] veya PAdES ([7], [8], [9]) imza formatlarına uygun olarak oluşturulmuş elektronik imzalar için geçerlidir. İmza politikaları, elektronik imzayı oluşturan ve oluşturulan imzayı doğrulayarak imzalı belgeyi işleme alan taraflarca uygulanır. Elektronik imzayı oluşturan taraflar bu dokümanda anlatılan elektronik imza oluşturma politikalarına uygun olarak imzayı oluştururlar. Elektronik imzayı doğrulayan taraflar ise bu dokümanda anlatılan elektronik imza doğrulama politikalarına uygun olarak imzayı doğrularlar. İmza politikaları dokümanına uygun olarak imza oluşturan ve doğrulayan taraflar imza doğrulama işleminden aynı sonucu elde ederler. Bu güvenli elektronik imza politikaları dokümanı, tarafların üzerinde hemfikir oldukları bir anlaşma niteliğindedir.

Bu dokümanda anlatılan elektronik imza politikaları Türkiye'deki 5070 sayılı Elektronik İmza Kanunu ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 6 Ocak 2005'de 25692 sayılı Resmi Gazete'de yayınlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik " ile "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" ile uyumludur.

ETSI TR 102 272 [3] ve ETSI TR 102 038 [5] dokümanlarına uygun olarak oluşturulan bu politika dokümanına eşsiz bir nesne tanımlama numarası (Object Identifier-OID) verilmiştir.

"Elektronik İmza Kullanım Profilleri [1]" dokümanı referans alınarak oluşturulan Bu dokümanda kullanılan tanım ve kısaltmalar da aynı şekilde ifade edilmiştir.

2. Politikaların Yönetimi

Bu doküman, BTK ile TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi işbirliğiyle hazırlanmış ve BTK tarafından yayımlanmıştır.

2.1. Politikanın Adı ve Tanımı

Politikanın Adı: Kısa Dönemli ve SİL Kontrollü Güvenli Elektronik İmza Politikaları

Politikanın Sürüm Numarası: 1.0

2.2. Politikaların Tanımlandığı Formatlar

Elektronik imza politikaları aşağıdaki formatlarda tanımlanmıştır:

- İnsan tarafından okunabilir PDF formatı (bu doküman)
- CAdES için makine tarafından işlenebilir XML formatı
- XAdES için makine tarafından işlenebilir XML formatı

2.3. Politikaların Yayınlanması

Elektronik imza politikaları http://www.eimza.gov.tr internet sitesi üzerinden yayımlanır.

Bu doküman aşağıda belirtilen URL adresinden PDF formatında yayımlanır:

http://www.eimza.gov.tr/EimzaPolitikalari/216792161015070311.pdf

Bu dokümanda yer verilen elektronik imza politikalarının, CAdES ve XAdES için ayrı ayrı hazırlanmış XML formatındaki dosyaları,

http://www.eimza.gov.tr/EimzaPolitikalari/CMS_216792161015070311.xml

http://www.eimza.gov.tr/EimzaPolitikalari/XML_216792161015070311.xml

URL adreslerinden yayımlanır.

Yayınlanan politikaların en güncel versiyonuna, OID numarasından oluşan dosya isminin en sonunda yer alan versiyon bilgisinden erişilebilir.

2.4. Politikaların Güvenliği

http://www.eimza.gov.tr/EimzaPolitikalari/PDF_SHA256_216792161015070311.hash

URL adresinden bu dokümana ait SHA-256 özetleme algoritması kullanılarak oluşturulmuş özet değerine erişilebilir.

XML dosyalarının SHA-256 özetleme algoritması kullanılarak oluşturulan özet değerine ise dosyanın içinden erişilmesi mümkündür. XML dosyalarının özet değeri alınırken <signPolicyInfo> nodunun tamamının özet değerinin alınması gereklidir.

2.5. Politikaların Güncellenmesi

Elektronik imza politikaları güncellendiği tarihten itibaren eski versiyonun geçerliliği sona erer. Güncel politika dokümanlarının OID ve erişim adresleri

http://www.eimza.gov.tr/EimzaPolitikalari/GuncelPolitikalar.xml

URL adresinde yer alan XML dosyası içeriğinden elde edilebilir.

2.6. Politikaların Arşivlenmesi

Güncellenen politikaların eski versiyonları BTK tarafından arşivlenir ve arşivlenen eski versiyon dokümanlar ile bu dokümanlara ait özet değerler, belirtilen URL adresinden yayımlanmaya devam eder.

2.7. İletişim Bilgileri

Adres : Bilgi Teknolojileri ve İletişim Kurumu Yeşilırmak Sokak No:16
06430 Demirtepe/ANKARA

Tel : (312) 297 72 00

Faks : (312) 29471 45

URL : http://www.btk.gov.tr

3. Politikaların Uygulanması

3.1. İmzalayan Taraftaki İşlemler

CAdES ve XAdES tipinde imza oluşturan tarafın uygulamasında, bu politikalara ait

- Politikanın nesne tanımlama numarasının (OID),
- Bu dokümanda işaret edilen ilgili XML dosyasının SHA-256 özet değerinin,
- XML dosyasının erişileceği URL adresinin

imzalama işlemi sırasında imza dosyasının içeriğine, imzalı özellik olarak eklemesi gereklidir.

PAdES tipinde imza oluşturan tarafın uygulamasında ise, bu politikalara ait

- Politikanın nesne tanımlama numarası (OID),
- Bu dokümanın SHA-256 özet değeri,
- Bu dokümanın erişileceği URL adresi

imzalama işlemi sırasında imza dosyasının içeriğine, imzalı özellik olarak eklenir[1].

Bu şekilde imza dosyası, ETSI TS 101 733 V1.8.1, ETSI TS 101 903 V1.4.2 ve ETSI TS 102 778-3 V1.2.1 ile ETSI TS 102 778-5 V1.1.2 dokümanlarında tanımlanan "Politikaları Açık Olarak Belirtilmiş Elektronik İmza (*Explicit Policy Electronic Signatures)* (EPES)" imza formatlarına göre oluşturulur. Böylece elektronik imzanın, bu dokümanda anlatılan şartlara uygun olarak oluşturulduğunun belirlenmesi sağlanmış olur.

3.2. İmzayı Doğrulayan Taraftaki İşlemler

Elektronik imzayı doğrulayan tarafın uygulamasının, imza dosyası içerisinde yer alan OID'ye bakarak imzanın hangi politikaya uygun olarak oluşturulduğunu tespit etmesi, ilgili XML dosyasını (PAdES için bu dokümanı) elde ederek özetini

[1] NOT: PAdES için tanımlanmış bir imza politikaları formatı standardı bulunmadığından dolayı PAdES imza politikaları için ayrı bir XML dosyası oluşturulmamıştır. Bu politikalara uygun oluşturulmak istenen PAdES tipi imzaların politikalara uygunluğunun sağlanması uygulamanın gerçekleştirimine bırakılmıştır.

çıkarması ve bu özet değeri imza dosyası içerisinde yer alan özet değer ile karşılaştırarak doğruluğundan emin olması gereklidir.

İmzayı doğrulayan tarafın uygulamasının, imzalı belgeyi işleme almadan önce imza doğrulama işlemlerini bu politikalara uygun olarak gerçekleştirmesi, bu politikalara uygun olarak oluşturulmayan imzaların ise doğrulamaması gereklidir. Aynı zamanda da imza doğrulama işlemini gerçekleştiren uygulamanın, imza politikasına ait OID'yi, özet değerini ve erişilebileceği URL adres bilgilerini doğrulamayı yapan kullanıcıya göstermesi zorunludur.

4. İmza Politikaları

4.1. Genel İmza Politikaları Bilgisi

4.1.1. İmza Politikaları Yayınlayan İsmi

Bilgi Teknolojileri ve İletişim Kurumu

4.1.2. İmza Politikaları Nesne Tanımlama Numarası

OID: 2.16.792.1.61.0.1.5070.3.1.1

Güvenli Elektronik İmza Oluşturma ve Doğrulama İlkeleri{ joint-iso-itu-t(2) ülke(16) tr(792) BTK (1.61.0.1) Elektronik İmza(5070) Güvenli Elektronik İmza Kullanım Profilleri (3) Politika-1 (1) SürümNo-1 (1) }

4.1.3. İmza Politikaları Geçerlilik Süresi

Geçerlilik Başlangıç Zamanı: 02 / 07/ 2012 Saat: 00:00

Geçerlilik Bitiş Zamanı: Bu doküman, geçerli olmadığı duyuruluncaya kadar geçerlidir.

Bu doküman, yukarıda belirtilen geçerlilik başlangıç ve bitiş tarihleri arasında oluşturulan elektronik imzalara uygulanır. Geçerlilik bitiş tarihinden sonra bu dokümana referans verilen imzalar, bu politika dokümanı kapsamında değerlendirilmez. Ancak geçerlilik süresi dolmadan önce bu dokümana uygun olarak oluşturana elektronik imzalar geçerliliğini korumaya devam eder.

4.1.4. Yayın Tarihi

Bu dokümanın yayın tarihi 02/07/2012 tarih ve 2012/DK-15/299 sayılı Kurul Kararının yayımlanma tarihidir.

4.1.5. Uygulama Alanı

Bu dokümanın uygulama alanı, NES iptal kontrollerini SİL üzerinden yapan, zaman damgası alınabilen ve oluşturulan elektronik imzalı belgelerin imzada kullanılan NES'in kalan geçerlilik süresinden daha kısa bir süre saklanması gereken güvenli elektronik imza uygulamalarıdır.

4.2. Genel Kurallar (Common Rules)

4.2.1. İmzalayan Tarafla İlgili Kurallar

4.2.1.1. Ayrık veya Bitişik İmza Kullanımı

Elektronik imza oluşturulurken imzalan belgenin ve imzanın aynı ya da ayrı dosyalarda tutulmasına izin verilir. Ancak PAdES imzalarda imzanın ayrı dosyada tutulmasına izin verilmez.

4.2.1.2. Zorunlu Eklenen İmzalı Özellikler

İmzalayan tarafın, elektronik imzayı oluştururken Tablo 1'de belirtilen imzalı özellikleri

CAdES için ETSI TS 101 733 V1.8.1,

XAdES için ETSI TS 101 903 V1.4.2,

PAdES-CMS için ETSI TS 102 778-3 V1.2.1,

PAdES-XFA için ETSI TS 102 778-5 V1.1.2'in 5. bölümünde anlatıldığı şekilde imza dosyasına eklemesi gereklidir.

PDF içine gömülen imzalı XML dosyaları, ETSI TS 102 778-5 V1.1.2 dokümanının 4. Bölümü'nde anlatıldığı şekilde oluşturulmalı ve Tablo 1'deki XAdES için belirtilen özellikleri içermelidir.

Tablo- 1 Elektronik İmza Oluşturulurken Eklenecek İmzalı Özellikler

CAdES	XAdES
id-contentType OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)3 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat
id-messageDigest OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)4 }	/SignedInfo/Reference/DigestValue
id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) kcs(1) pkcs9(9) smime(16) id-aa(2) 47 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningCertificate
id-signingTime OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)5 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningTime
	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat/MimeType
id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1)pkcs9(9) smime(16) id-aa(2) 15 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SignaturePolicyIdentifier

PAdES-CMS	PAdES-XFA
id-contentType OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)3 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat
id-messageDigest OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)4 }	/SignedInfo/Reference/DigestValue
id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) kcs(1) pkcs9(9) smime(16) id-aa(2) 47 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningCertificate
M entry in the signature dictionary	CreateDate element defined within the XMP ns.adobe.com/xap/1.0/ namespace
-	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat/MimeType
id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1)pkcs9(9) smime(16) id-aa(2) 15 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SignaturePolicyIdentifier

NOT 1: SigningTime özelliği ile M entry ve CreateDate elementinin içeriğine kullanıcı makinasındaki sistem saatinden veya kurumdaki bir sunucudan alınan imzalama sırasındaki zaman bilgisi yazılır.

NOT 2: SigPolicyId / SignaturePolicyIdentifier alanına bu politika dokümana ait bilgiler yazılır.

4.2.1.3. Zorunlu Eklenen İmzasız Özellikler

İmzalayan taraf Tablo 2'de belirtilen imzasız özellikleri

- CAdES için ETSI TS 101 733 V1.8.1,
- XAdES için ETSI TS 101 903 V1.4.2,
- PAdES-CMS için ETSI TS 102 778-3 V1.2.1,
- PAdES-XFA için ETSI TS 102 778-5 V1.1.2'in 5. bölümünde anlatıldığı şekilde imza dosyasına eklemek zorundadır.

PDF içine gömülen imzalı XML dosyaları ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı şekilde oluşturulmalı ve Tablo 2'deki XAdES için belirtilen özellikleri içermelidir.

Tablo 2 Zorunlu Eklenen İmzasız Özellikler

CAdES	XAdES
id-aa-signatureTimeStampToken OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 14}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ SignatureTimeStamp

PAdES-CMS	PAdES-XFA
/Type/DocTimeStamp /SubFilter /ETSI.RFC3161	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ SignatureTimeStamp

4.2.1.4. Zorunlu Eklenen Sertifika Referansları

İmzalayan kişiye ait NES'in referansının

- CAdES ve PAdES-CMS için signingCertificateV2,
- XAdES ve PAdES-XFA için SigningCertificate

imza özelliği olarak imza dosyasına eklenmesi zorunludur.

PDF içine gömülen imzalı XML dosyalarına NES'in referansı, ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı gibi XAdES için belirtilen şekilde eklenmesi gereklidir.

NES güven zincirindeki ESHS sertifikalarının referanslarının yukarıda belirtilen alanlara eklenmesi zorunlu değildir.

4.2.1.5. Zorunlu Eklenen Sertifikalar

İmzalayan kişiye ait NES'in

- CAdES ve PAdES-CMS için imza dosyasının SignedData içindeki certificates alanına,
- XAdES ve PAdES-XFA için Signature içindeki KeyInfo alanına

eklenmesi zorunludur.

PDF içine gömülen imzalı XML dosyalarına NES, ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı gibi XAdES için belirtilen şekilde eklenmesi gereklidir.

NES güven zincirindeki ESHS sertifikalarının yukarıda belirtilen alanlara eklenmesi zorunlu değildir.

4.2.2. Doğrulayan Tarafla İlgili Kurallar

4.2.2.1. Zorunlu Eklenen İmzasız Özellikler

İmzayı doğrulayan taraf, imzalı belgeyi işleme almadan önce bu dokümanın 0. bölümünde belirtilen imzasız özellikler eklenmemişse, belirtilen tüm imzasız özellikleri imza dosyasına eklemek zorundadır.

4.2.3. Sertifikalar ile İlgili Kurallar

4.2.3.1. Sertifikaların Güvenilirliği ile İlgili Gereksinimler

5070 sayılı Elektronik İmza Kanunu ve ikincil düzenlemeler kapsamında BTK'ya bildirimde bulunarak Türkiye'de faaliyet göstermeye başlayan ESHS'lere ait kök güven zincirinden üretilmiş NES'lere güvenilir.

ESHS'lere ait tüm kök sertifikalara http://www.eimza.gov.tr/tr/kok internet adresinden erişilebilir.

Türkiye'de elektronik imza mevzuatı kapsamında faaliyet gösteren ESHS'lerin, NES'lere ilişkin yayınlamış oldukları politikalara güvenilir.

5070 sayılı Elektronik İmza Kanunu ve ilgili mevzuat ile

- Kök güven zincirinde kök ile NES arasında kaç adet ESHS alt kök sertifikası olması gerektiği,
- Sertifika politikaları ve
- Sertifikaların isim alanları

hususlarında bir düzenleme yapılmadığından herhangi bir sınırlama getirilmemiştir.

4.2.3.2. Sertifika İptal Kontrolleri ile İlgili Gereksinimler

NES ve sertifika güven zincirindeki ESHS'ye ait sertifikaların iptal kontrolleri SİL üzerinden yapılır.

4.2.4. Zaman Damgası ile İlgili Kurallar

4.2.4.1. Zaman Damgası Sertifikalarının Güvenilirliği ile İlgili Gereksinimler

Türkiye'de 5070 sayılı Elektronik İmza Kanunu ve ikincil düzenlemeler çerçevesinde BTK'ya bildirimde bulunarak faaliyete başlayan tüm ESHS'lere ait kök güven zincirinden üretilmiş zaman damgalarına güvenilir.

4.2.4.2. Zaman Damgası Sertifikalarının İptal Kontrolleri ile İlgili Gereksinimler

Zaman damgasını imzalayan ESHS sertifikası ile bu sertifikanın içinde bulunduğu sertifika, güven zincirindeki ESHS'ye ait sertifikaların iptal kontrolleri SİL üzerinden ya da tercih edilmesi halinde OCSP üzerinden yapılır.

4.2.4.3. Kesinleşme Süresi

Zaman damgası alındıktan sonra kesinleşme süresi 24 saat olarak uygulanır. Zaman damgası üzerindeki zamandan 24 saat sonra NES, zaman damgası sertifikası ve sertifika güven zincirindeki tüm ESHS sertifikalarının geçerlilik kontrolleri yapılarak sertifika doğrulama işlemleri kesinleştirilir. Sertifikaların geçerlilik kontrolleri yapılırken zaman damgası üzerindeki zaman bilgisi referans alınır. Sertifikaların zaman damgası alındığı tarihte geçerlilik süresinin sona ermiş olması veya iptal durumunda olması imzanın geçersiz kabul edilmesine sebep olur.

4.2.4.4. Zaman Damgası Gecikme Süresi

Zaman damgası, imza sahibi tarafından eklenen signingTime özelliği ile M entry veya CreateDate elementinin içeriğinde belirtilen imza zamanından en geç 2 saat sonra alınmalıdır.

4.2.5. Yetkiler ile İlgili Kurallar

Bu politika dokümanında yetkilendirmeler ile ilgili kurallar belirlenmemiştir.

4.2.6. Kullanılan Algoritmalar ile İlgili Kısıtlamalar

Güvenli elektronik imza oluşturma için kullanılabilecek algoritmalar, BTK tarafından yayınlanan “Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ”de belirlendiğinden bu politika dokümanında algoritma kısıtları ile ilgili kurallara yer verilmemiştir. Türkiye’de elektronik imza mevzuatı ile belirlenen algoritmaların kullanılması zorunludur.

4.3. İmza Amacı ile İlgili Kurallar (Commitment Rules)

Bu politika dokümanında imza amacı ile ilgili kurallar belirlenmemiştir

REFERANSLAR

[1] Elektronik İmza Kullanım Profilleri, Sürüm 1.0, 1 Ekim 2011, TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi.

[2] ETSI TR 102 041: Signature Policies Report

[3] ETSI TR 102 272: Electronic Signatures and Infrastructures (ESI); ASN.1 Format for Signature Policies

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

[5] ETSI TR 102 038: TC Security - Electronic Signatures and Infrastructures (ESI); XML Format for Signature Policies

[6] ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

[7] ETSI TS 102 778-3: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

[8] ETSI TS 102 778-4: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile.

[9] ETSI TS 102 778-5: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES Signatures.

Uzun Dönemli ve SİL Kontrollü Güvenli Elektronik İmza Politikaları (Profil P3)

OID:

2.16.792.1.61.0.1.5070.3.2.1

Sürüm 1.0

Haziran 2012

İÇİNDEKİLER

1. Giriş....4
2. Politikaların Yönetimi....5
   2.1. Politikanın Adı ve Tanımı....5
   2.2. Politikaların Tanımlandığı Formatlar....5
   2.3. Politikaların Yayınlanması....5
   2.4. Politikaların Güvenliği....6
   2.5. Politikaların Güncellenmesi....6
   2.6. Politikaların Arşivlenmesi....6
   2.7. İletişim Bilgileri....6
3. Politikaların Uygulanması....7
   3.1. İmzalayan Taraftaki İşlemler....7
   3.2. İmzayı Doğrulayan Taraftaki İşlemler....7
4. İmza Politikaları....8
   4.1. Genel İmza Politikaları Bilgisi....8
      4.1.1. İmza Politikaları Yayınlayan İsmi....8
      4.1.2. İmza Politikaları Nesne Tanımlama Numarası....8
      4.1.3. İmza Politikaları Geçerlilik Süresi....8
      4.1.4. Yayın Tarihi....9
      4.1.5. Uygulama Alanı....9
   4.2. Genel Kurallar (Common Rules)....9
      4.2.1. İmzalayan Tarafla İlgili Kurallar....9
         4.2.1.1. Ayrık veya Bitişik İmza Kullanımı....9
         4.2.1.2. Zorunlu Eklenen İmzalı Özellikler....9
         4.2.1.3. Zorunlu Eklenen İmzasız Özellikler....12
         4.2.1.4. Zorunlu Eklenen Sertifika Referansları....13
         4.2.1.5. Zorunlu Eklenen Sertifikalar....14
      4.2.2. Doğrulayan Tarafla İlgili Kurallar....14

4.2.2.1. Zorunlu Eklenen İmzasız Özellikler 14
4.2.3. Sertifikalar ile İlgili Kurallar 14
4.2.3.1. Sertifikaların Güvenilirliği ile İlgili Gereksinimler 14
4.2.3.2. Sertifika İptal Kontrolleri ile İlgili Gereksinimler 15
4.2.4. Zaman Damgası ile İlgili Kurallar 15
4.2.4.1. Zaman Damgası Sertifikalarının Güvenilirliği ile İlgili Gereksinimler 15
4.2.4.2. Zaman Damgası Sertifikalarının İptal Kontrolleri ile İlgili Gereksinimler 15
4.2.4.3. Kesinleşme Süresi 15
4.2.4.4. Zaman Damgası Gecikme Süresi 16
4.2.5. Yetkiler ile İlgili Kurallar 16
4.2.6. Kullanılan Algoritmalar ile İlgili Kısıtlamalar 16
4.3. İmza Amacı ile İlgili Kurallar (Commitment Rules) 16

1. Giriş

Bu elektronik imza politikası dokümanında, imzanın oluşturulması ve doğrulanmasında uyulması gereken kurallara yer verilmiş, politikalar belirlenmiştir. Bu politikalar, CAdES [4], XAdES [6] veya PAdES ([7], [8], [9]) imza formatlarına uygun olarak oluşturulmuş elektronik imzalar için geçerlidir. İmza politikaları, elektronik imzayı oluşturan ve oluşturulan imzayı doğrulayarak imzalı belgeyi işleme alan taraflarca uygulanır. Elektronik imzayı oluşturan taraflar bu dokümanda anlatılan elektronik imza oluşturma politikalarına uygun olarak imzayı oluştururlar. Elektronik imzayı doğrulayan taraflar ise bu dokümanda anlatılan elektronik imza doğrulama politikalarına uygun olarak imzayı doğrularlar. İmza politikaları dokümanına uygun olarak imza oluşturan ve doğrulayan taraflar imza doğrulama işleminden aynı sonucu elde ederler. Bu güvenli elektronik imza politikaları dokümanı, tarafların üzerinde hemfikir oldukları bir anlaşma niteliğindedir.

Bu dokümanda anlatılan elektronik imza politikaları Türkiye'deki 5070 sayılı Elektronik İmza Kanunu ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 6 Ocak 2005'de 25692 sayılı Resmi Gazete'de yayınlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik " ile "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" ile uyumludur.

ETSI TR 102 272 [3] ve ETSI TR 102 038 [5] dokümanlarına uygun olarak oluşturulan bu politika dokümanına eşsiz bir nesne tanımlama numarası (Object Identifier-OID) verilmiştir.

"Elektronik İmza Kullanım Profilleri [1]" dokümanı referans alınarak oluşturulan Bu dokümanda kullanılan tanım ve kısaltmalar da aynı şekilde ifade edilmiştir.

2. Politikaların Yönetimi

Bu doküman, BTK ile TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi işbirliğiyle hazırlanmış ve BTK tarafından yayımlanmıştır.

2.1. Politikanın Adı ve Tanımı

Politikanın Adı: Uzun Dönemli ve SİL Kontrollü Güvenli Elektronik İmza Politikaları

Politikanın Sürüm Numarası: 1.0

2.2. Politikaların Tanımlandığı Formatlar

Elektronik imza politikaları aşağıdaki formatlarda tanımlanmıştır:

- İnsan tarafından okunabilir PDF formatı (bu doküman)
- CAdES için makine tarafından işlenebilir XML formatı
- XAdES için makine tarafından işlenebilir XML formatı

2.3. Politikaların Yayınlanması

Elektronik imza politikaları http://www.eimza.gov.tr internet sitesi üzerinden yayımlanır.

Bu doküman aşağıda belirtilen URL adresinden PDF formatında yayımlanır:

http://www.eimza.gov.tr/EimzaPolitikalari/216792161015070321.pdf

Bu dokümanda yer verilen elektronik imza politikalarının, CAdES ve XAdES için ayrı ayrı hazırlanmış XML formatındaki dosyaları,

http://www.eimza.gov.tr/EimzaPolitikalari/CMS_216792161015070321.xml

http://www.eimza.gov.tr/EimzaPolitikalari/XML_216792161015070321.xml

URL adreslerinden yayımlanır.

Yayınlanan politikaların en güncel versiyonuna, OID numarasından oluşan dosya isminin en sonunda yer alan versiyon bilgisinden erişilebilir.

2.4. Politikaların Güvenliği

http://www.eimza.gov.tr/EimzaPolitikalari/PDF_SHA256_216792161015070321.hash

URL adresinden bu dokümana ait SHA-256 özetleme algoritması kullanılarak oluşturulmuş özet değerine erişilebilir.

XML dosyalarının SHA-256 özetleme algoritması kullanılarak oluşturulan özet değerine ise dosyanın içinden erişilmesi mümkündür. XML dosyalarının özet değeri alınırken <signPolicyInfo> nodunun tamamının özet değerinin alınması gereklidir.

2.5. Politikaların Güncellenmesi

Elektronik imza politikaları güncellendiği tarihten itibaren eski versiyonun geçerliliği sona erer. Güncel politika dokümanlarının OID ve erişim adresleri

http://www.eimza.gov.tr/EimzaPolitikalari/GuncelPolitikalar.xml

URL adresinde yer alan XML dosyası içeriğinden elde edilebilir.

2.6. Politikaların Arşivlenmesi

Güncellenen politikaların eski versiyonları BTK tarafından arşivlenir ve arşivlenen eski versiyon dokümanlar ile bu dokümanlara ait özet değerler, belirtilen URL adresinden yayımlanmaya devam eder.

2.7. İletişim Bilgileri

Adres : Bilgi Teknolojileri ve İletişim Kurumu Yeşilırmak Sokak No:16
06430 Demirtepe/ANKARA

Tel : (312) 297 72 00

Faks : (312) 29471 45

URL : http://www.btk.gov.tr

3. Politikaların Uygulanması

3.1. İmzalayan Taraftaki İşlemler

CAdES ve XAdES tipinde imza oluşturan tarafın uygulamasında, bu politikalara ait

- Politikanın nesne tanımlama numarasının (OID),
- Bu dokümanda işaret edilen ilgili XML dosyasının SHA-256 özet değerinin,
- XML dosyasının erişileceği URL adresinin

imzalama işlemi sırasında imza dosyasının içeriğine, imzalı özellik olarak eklemesi gereklidir.

PAdES tipinde imza oluşturan tarafın uygulamasında ise, bu politikalara ait

- Politikanın nesne tanımlama numarası (OID),
- Bu dokümanın SHA-256 özet değeri,
- Bu dokümanın erişileceği URL adresi

imzalama işlemi sırasında imza dosyasının içeriğine, imzalı özellik olarak eklenir[1].

Bu şekilde imza dosyası, ETSI TS 101 733 V1.8.1, ETSI TS 101 903 V1.4.2 ve ETSI TS 102 778-3 V1.2.1 ile ETSI TS 102 778-5 V1.1.2 dokümanlarında tanımlanan "Politikaları Açık Olarak Belirtilmiş Elektronik İmza (*Explicit Policy Electronic Signatures)* (EPES)" imza formatlarına göre oluşturulur. Böylece elektronik imzanın, bu dokümanda anlatılan şartlara uygun olarak oluşturulduğunun belirlenmesi sağlanmış olur.

3.2. İmzayı Doğrulayan Taraftaki İşlemler

Elektronik imzayı doğrulayan tarafın uygulamasının, imza dosyası içerisinde yer alan OID'ye bakarak imzanın hangi politikaya uygun olarak oluşturulduğunu tespit etmesi, ilgili XML dosyasını (PAdES için bu dokümanı) elde ederek özetini

[1] NOT: PAdES için tanımlanmış bir imza politikaları formatı standardı bulunmadığından dolayı PAdES imza politikaları için ayrı bir XML dosyası oluşturulmamıştır. Bu politikalara uygun oluşturulmak istenen PAdES tipi imzaların politikalara uygunluğunun sağlanması uygulamanın gerçekleştirimine bırakılmıştır.

çıkarması ve bu özet değeri imza dosyası içerisinde yer alan özet değer ile karşılaştırarak doğruluğundan emin olması gereklidir.

İmzayı doğrulayan tarafın uygulamasının, imzalı belgeyi işleme almadan önce imza doğrulama işlemlerini bu politikalara uygun olarak gerçekleştirmesi, bu politikalara uygun olarak oluşturulmayan imzaların ise doğrulamaması gereklidir. Aynı zamanda da imza doğrulama işlemini gerçekleştiren uygulamanın, imza politikasına ait OID'yi, özet değerini ve erişilebileceği URL adres bilgilerini doğrulamayı yapan kullanıcıya göstermesi zorunludur.

4. İmza Politikaları

4.1. Genel İmza Politikaları Bilgisi

4.1.1. İmza Politikaları Yayınlayan İsmi

Bilgi Teknolojileri ve İletişim Kurumu

4.1.2. İmza Politikaları Nesne Tanımlama Numarası

OID: 2.16.792.1.61.0.1.5070.3.2.1

Güvenli Elektronik İmza Oluşturma ve Doğrulama İlkeleri{ joint-iso-itu-t(2) ülke(16) tr(792) BTK (1.61.0.1) Elektronik İmza(5070) Güvenli Elektronik İmza Kullanım Profilleri (3) Politika-2 (2) SürümNo-1 (1) }

4.1.3. İmza Politikaları Geçerlilik Süresi

Geçerlilik Başlangıç Zamanı: 02 / 07/ 2012 Saat: 00:00

Geçerlilik Bitiş Zamanı: Bu doküman, geçerli olmadığı duyuruluncaya kadar geçerlidir.

Bu doküman, yukarıda belirtilen geçerlilik başlangıç ve bitiş tarihleri arasında oluşturulan elektronik imzalara uygulanır. Geçerlilik bitiş tarihinden sonra bu dokümana referans verilen imzalar, bu politika dokümanı kapsamında değerlendirilmez. Ancak geçerlilik süresi dolmadan önce bu dokümana uygun olarak oluşturana elektronik imzalar geçerliliğini korumaya devam eder.

4.1.4. Yayın Tarihi

Bu dokümanın yayın tarihi 02/07/2012 tarih ve 2012/DK-15/299 sayılı Kurul Kararının yayımlanma tarihidir.

4.1.5. Uygulama Alanı

Bu dokümanın uygulama alanı, NES iptal kontrollerini SİL üzerinden yapan, zaman damgası alınabilen ve oluşturulan elektronik imzalı belgelerin imzada kullanılan NES'in kalan geçerlilik süresinden daha uzun bir süre saklanması gereken güvenli elektronik imza uygulamalarıdır.

4.2. Genel Kurallar (Common Rules)

4.2.1. İmzalayan Tarafla İlgili Kurallar

4.2.1.1. Ayrık veya Bitişik İmza Kullanımı

Elektronik imza oluşturulurken imzalan belgenin ve imzanın aynı ya da ayrı dosyalarda tutulmasına izin verilir. Ancak PAdES imzalarda imzanın ayrı dosyada tutulmasına izin verilmez.

4.2.1.2. Zorunlu Eklenen İmzalı Özellikler

İmzalayan tarafın, elektronik imzayı oluştururken Tablo 1'de belirtilen imzalı özellikleri

CAdES için ETSI TS 101 733 V1.8.1,

XAdES için ETSI TS 101 903 V1.4.2,

PAdES-CMS için ETSI TS 102 778-3 V1.2.1,

PAdES-XFA için ETSI TS 102 778-5 V1.1.2'in 5. bölümünde anlatıldığı şekilde imza dosyasına eklemesi gereklidir.

PDF içine gömülen imzalı XML dosyaları, ETSI TS 102 778-5 V1.1.2 dokümanının 4. Bölümü'nde anlatıldığı şekilde oluşturulmalı ve Tablo 1'deki XAdES için belirtilen özellikleri içermelidir.

Tablo- 1 Elektronik İmza Oluşturulurken Eklenecek İmzalı Özellikler

CAdES	XAdES
id-contentType OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)3 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat
id-messageDigest OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)4 }	/SignedInfo/Reference/DigestValue
id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) kcs(1) pkcs9(9) smime(16) id-aa(2) 47 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningCertificate
id-signingTime OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)5 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningTime
	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat/MimeType
id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1)pkcs9(9) smime(16) id-aa(2) 15 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SignaturePolicyIdentifier

PAdES-CMS	PAdES-XFA
id-contentType OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)3 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat
id-messageDigest OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)4 }	/SignedInfo/Reference/DigestValue
id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) kcs(1) pkcs9(9) smime(16) id-aa(2) 47 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningCertificate
M entry in the signature dictionary	CreateDate element defined within the XMP ns.adobe.com/xap/1.0/ namespace
-	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat/MimeType
id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1)pkcs9(9) smime(16) id-aa(2) 15 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SignaturePolicyIdentifier

NOT 1: SigningTime özelliği ile M entry ve CreateDate elementinin içeriğine kullanıcı makinasındaki sistem saatinden veya kurumdaki bir sunucudan alınan imzalama sırasındaki zaman bilgisi yazılır.

NOT 2: SigPolicyId / SignaturePolicyIdentifier alanına bu politika dokümana ait bilgiler yazılır.

4.2.1.3. Zorunlu Eklenen İmzasız Özellikler

İmzalayan taraf Tablo 2'de belirtilen imzasız özellikleri

- CAdES için ETSI TS 101 733 V1.8.1,
- XAdES için ETSI TS 101 903 V1.4.2,
- PAdES-CMS için ETSI TS 102 778-3 V1.2.1 ve ETSI TS 102 778-4 V1.1.2,
- PAdES-XFA için ETSI TS 102 778-5 V1.1.2'in 5. bölümünde anlatıldığı şekilde imza dosyasına eklemek zorundadır.

PDF içine gömülen imzalı XML dosyaları ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı şekilde oluşturulmalı ve

Tablo 2'deki XAdES için belirtilen özellikleri içermelidir.

Tablo-2 Zorunlu Eklenen İmzasız Özellikler

CAdES	XAdES
id-aa-signatureTimeStampToken OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 14}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ SignatureTimeStamp
id-aa-ets-certificateRefs OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 21}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ CompleteCertificateRefs
id-aa-ets-revocationRefs OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 22}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ CompleteRevocationRefs
id-aa-ets-certValues OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)	/Signature/Object/ QualifyingProperties/ UnSignedProperties/

smime(16) id-aa(2) 23}	UnsignedSignatureProperties/ CertificatesValues
id-aa-ets-revocationValues OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 24}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ RevocationValues
-	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ SigAndRefsTimeStamp
PAdES-CMS	PAdES-XFA
/Type/DocTimeStamp /SubFilter /ETSI.RFC3161	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ SignatureTimeStamp
/DSS/Certs Array /DSS/VRI/Cert Array	/DSS/Certs Array /DSS/VRI/Cert Array
/DSS/CRLs Array /DSS/VRI/CRL Array	/DSS/CRLs Array /DSS/VRI/CRL Array

4.2.1.4. Zorunlu Eklenen Sertifika Referansları

İmzalayan kişiye ait NES'in referansının

- CAdES ve PAdES-CMS için signingCertificateV2,
- XAdES ve PAdES-XFA için SigningCertificate

imza özelliği olarak imza dosyasına eklenmesi zorunludur.

PDF içine gömülen imzalı XML dosyalarına NES'in referansı, ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı gibi XAdES için belirtilen şekilde eklenmesi gereklidir.

NES güven zincirindeki ESHS sertifikalarının referanslarının yukarıda belirtilen alanlara eklenmesi zorunlu değildir.

4.2.1.5. Zorunlu Eklenen Sertifikalar

İmzalayan kişiye ait NES'in

- CAdES ve PAdES-CMS için imza dosyasının SignedData içindeki certificates alanına,
- XAdES ve PAdES-XFA için Signature içindeki KeyInfo alanına

eklenmesi zorunludur.

PDF içine gömülen imzalı XML dosyalarına NES, ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı gibi XAdES için belirtilen şekilde eklenmesi gereklidir.

NES güven zincirindeki ESHS sertifikalarının yukarıda belirtilen alanlara eklenmesi zorunlu değildir.

4.2.2. Doğrulayan Tarafla İlgili Kurallar

4.2.2.1. Zorunlu Eklenen İmzasız Özellikler

İmzayı doğrulayan taraf, imzalı belgeyi işleme almadan önce bu dokümanın 4.2.1.3. bölümünde belirtilen imzasız özellikler eklenmemişse, belirtilen tüm imzasız özellikleri imza dosyasına eklemek zorundadır.

4.2.3. Sertifikalar ile İlgili Kurallar

4.2.3.1. Sertifikaların Güvenilirliği ile İlgili Gereksinimler

5070 sayılı Elektronik İmza Kanunu ve ikincil düzenlemeler kapsamında BTK'ya bildirimde bulunarak Türkiye'de faaliyet göstermeye başlayan ESHS'lere ait kök güven zincirinden üretilmiş NES'lere güvenilir.

ESHS'lere ait tüm kök sertifikalara http://www.eimza.gov.tr/tr/kok internet adresinden erişilebilir.

Türkiye'de elektronik imza mevzuatı kapsamında faaliyet gösteren ESHS'lerin, NES'lere ilişkin yayınlamış oldukları politikalara güvenilir.

5070 sayılı Elektronik İmza Kanunu ve ilgili mevzuat ile

- Kök güven zincirinde kök ile NES arasında kaç adet ESHS alt kök sertifikası olması gerektiği,
- Sertifika politikaları ve
- Sertifikaların isim alanları

hususlarında bir düzenleme yapılmadığından herhangi bir sınırlama getirilmemiştir.

4.2.3.2. Sertifika İptal Kontrolleri ile İlgili Gereksinimler

NES ve sertifika güven zincirindeki ESHS'ye ait sertifikaların iptal kontrolleri SİL üzerinden yapılır.

4.2.4. Zaman Damgası ile İlgili Kurallar

4.2.4.1. Zaman Damgası Sertifikalarının Güvenilirliği ile İlgili Gereksinimler

Türkiye'de 5070 sayılı Elektronik İmza Kanunu ve ikincil düzenlemeler çerçevesinde BTK'ya bildirimde bulunarak faaliyete başlayan tüm ESHS'lere ait kök güven zincirinden üretilmiş zaman damgalarına güvenilir.

4.2.4.2. Zaman Damgası Sertifikalarının İptal Kontrolleri ile İlgili Gereksinimler

Zaman damgasını imzalayan ESHS sertifikası ile bu sertifikanın içinde bulunduğu sertifika, güven zincirindeki ESHS'ye ait sertifikaların iptal kontrolleri SİL üzerinden ya da tercih edilmesi halinde OCSP üzerinden yapılır.

4.2.4.3. Kesinleşme Süresi

Zaman damgası alındıktan sonra kesinleşme süresi 24 saat olarak uygulanır. Zaman damgası üzerindeki zamandan 24 saat sonra NES, zaman damgası sertifikası ve sertifika güven zincirindeki tüm ESHS sertifikalarının geçerlilik kontrolleri yapılarak sertifika doğrulama işlemleri kesinleştirilir. Sertifikaların geçerlilik kontrolleri yapılırken zaman damgası üzerindeki zaman bilgisi referans alınır. Sertifikaların zaman damgası alındığı tarihte geçerlilik süresinin sona ermiş olması veya iptal durumunda olması imzanın geçersiz kabul

edilmesine sebep olur. İmzaya dahil olmayan imza özellikleri kesinleşme süresi sonunda imza dosyasına eklenir.

4.2.4.4. Zaman Damgası Gecikme Süresi

Zaman damgası, imza sahibi tarafından eklenen signingTime özelliği ile M entry veya CreateDate elementinin içeriğinde belirtilen imza zamanından en geç 2 saat sonra alınmalıdır.

4.2.5. Yetkiler ile İlgili Kurallar

Bu politika dokümanında yetkilendirmeler ile ilgili kurallar belirlenmemiştir.

4.2.6. Kullanılan Algoritmalar ile İlgili Kısıtlamalar

Güvenli elektronik imza oluşturma için kullanılabilecek algoritmalar, BTK tarafından yayınlanan "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"de belirlendiğinden bu politika dokümanında algoritma kısıtları ile ilgili kurallara yer verilmemiştir. Türkiye'de elektronik imza mevzuatı ile belirlenen algoritmaların kullanılması zorunludur.

4.3. İmza Amacı ile İlgili Kurallar (Commitment Rules)

Bu politika dokümanında imza amacı ile ilgili kurallar belirlenmemiştir.

REFERANSLAR

[1] Elektronik İmza Kullanım Profilleri, Sürüm 1.0, 1 Ekim 2011, TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi.

[2] ETSI TR 102 041: Signature Policies Report

[3] ETSI TR 102 272: Electronic Signatures and Infrastructures (ESI); ASN.1 Format for Signature Policies

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

[5] ETSI TR 102 038: TC Security - Electronic Signatures and Infrastructures (ESI); XML Format for Signature Policies

[6] ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

[7] ETSI TS 102 778-3: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

[8] ETSI TS 102 778-4: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile.

[9] ETSI TS 102 778-5: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES Signatures.

Uzun Dönemli ve ÇİSDuP Kontrollü Güvenli Elektronik İmza Politikaları (Profil P4)

OID:

2.16.792.1.61.0.1.5070.3.3.1

Sürüm 1.0

Haziran 2012

İÇİNDEKİLER

1. Giriş....4
2. Politikaların Yönetimi....5
   2.1. Politikanın Adı ve Tanımı....5
   2.2. Politikaların Tanımlandığı Formatlar....5
   2.3. Politikaların Yayınlanması....5
   2.4. Politikaların Güvenliği....6
   2.5. Politikaların Güncellenmesi....6
   2.6. Politikaların Arşivlenmesi....6
   2.7. İletişim Bilgileri....6
3. Politikaların Uygulanması....7
   3.1. İmzalayan Taraftaki İşlemler....7
   3.2. İmzayı Doğrulayan Taraftaki İşlemler....7
4. İmza Politikaları....8
   4.1. Genel İmza Politikaları Bilgisi....8
      4.1.1. İmza Politikaları Yayınlayan İsmi....8
      4.1.2. İmza Politikaları Nesne Tanımlama Numarası....8
      4.1.3. İmza Politikaları Geçerlilik Süresi....8
      4.1.4. Yayın Tarihi....9
      4.1.5. Uygulama Alanı....9
   4.2. Genel Kurallar (Common Rules)....9
      4.2.1. İmzalayan Tarafla İlgili Kurallar....9
         4.2.1.1. Ayrık veya Bitişik İmza Kullanımı....9
         4.2.1.2. Zorunlu Eklenen İmzalı Özellikler....9
         4.2.1.3. Zorunlu Eklenen İmzasız Özellikler....12
         4.2.1.4. Zorunlu Eklenen Sertifika Referansları....14
         4.2.1.5. Zorunlu Eklenen Sertifikalar....14
      4.2.2. Doğrulayan Tarafla İlgili Kurallar....14

4.2.2.1. Zorunlu Eklenen İmzasız Özellikler 14
4.2.3. Sertifikalar ile İlgili Kurallar 15
4.2.3.1. Sertifikaların Güvenilirliği ile İlgili Gereksinimler 15
4.2.3.2. Sertifika İptal Kontrolleri ile İlgili Gereksinimler 15
4.2.4. Zaman Damgası ile İlgili Kurallar 15
4.2.4.1. Zaman Damgası Sertifikalarının Güvenilirliği ile İlgili Gereksinimler 15
4.2.4.2. Zaman Damgası Sertifikalarının İptal Kontrolleri ile İlgili Gereksinimler 16
4.2.4.3. Kesinleşme Süresi 16
4.2.4.4. Zaman Damgası Gecikme Süresi 16
4.2.5. Yetkiler ile İlgili Kurallar 16
4.2.6. Kullanılan Algoritmalar ile İlgili Kısıtlamalar 16
4.3. İmza Amacı ile İlgili Kurallar (Commitment Rules) 17

1. Giriş

Bu elektronik imza politikası dokümanında, imzanın oluşturulması ve doğrulanmasında uyulması gereken kurallara yer verilmiş, politikalar belirlenmiştir. Bu politikalar, CAdES [4], XAdES [6] veya PAdES ([7], [8], [9]) imza formatlarına uygun olarak oluşturulmuş elektronik imzalar için geçerlidir. İmza politikaları, elektronik imzayı oluşturan ve oluşturulan imzayı doğrulayarak imzalı belgeyi işleme alan taraflarca uygulanır. Elektronik imzayı oluşturan taraflar bu dokümanda anlatılan elektronik imza oluşturma politikalarına uygun olarak imzayı oluştururlar. Elektronik imzayı doğrulayan taraflar ise bu dokümanda anlatılan elektronik imza doğrulama politikalarına uygun olarak imzayı doğrularlar. İmza politikaları dokümanına uygun olarak imza oluşturan ve doğrulayan taraflar imza doğrulama işleminden aynı sonucu elde ederler. Bu güvenli elektronik imza politikaları dokümanı, tarafların üzerinde hemfikir oldukları bir anlaşma niteliğindedir.

Bu dokümanda anlatılan elektronik imza politikaları Türkiye'deki 5070 sayılı Elektronik İmza Kanunu ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 6 Ocak 2005'de 25692 sayılı Resmi Gazete'de yayınlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik " ile "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" ile uyumludur.

ETSI TR 102 272 [3] ve ETSI TR 102 038 [5] dokümanlarına uygun olarak oluşturulan bu politika dokümanına eşsiz bir nesne tanımlama numarası (Object Identifier-OID) verilmiştir.

"Elektronik İmza Kullanım Profilleri [1]" dokümanı referans alınarak oluşturulan Bu dokümanda kullanılan tanım ve kısaltmalar da aynı şekilde ifade edilmiştir.

2. Politikaların Yönetimi

Bu doküman, BTK ile TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi işbirliğiyle hazırlanmış ve BTK tarafından yayımlanmıştır.

2.1. Politikanın Adı ve Tanımı

Politikanın Adı: Uzun Dönemli ve ÇİSDuP Kontrollü Güvenli Elektronik İmza Politikaları

Politikanın Sürüm Numarası: 1.0

2.2. Politikaların Tanımlandığı Formatlar

Elektronik imza politikaları aşağıdaki formatlarda tanımlanmıştır:

- İnsan tarafından okunabilir PDF formatı (bu doküman)
- CAdES için makine tarafından işlenebilir XML formatı
- XAdES için makine tarafından işlenebilir XML formatı

2.3. Politikaların Yayınlanması

Elektronik imza politikaları http://www.eimza.gov.tr internet sitesi üzerinden yayımlanır.

Bu doküman aşağıda belirtilen URL adresinden PDF formatında yayımlanır:

http://www.eimza.gov.tr/EimzaPolitikalari/216792161015070331.pdf

Bu dokümanda yer verilen elektronik imza politikalarının, CAdES ve XAdES için ayrı ayrı hazırlanmış XML formatındaki dosyaları,

http://www.eimza.gov.tr/EimzaPolitikalari/CMS_216792161015070331.xml

http://www.eimza.gov.tr/EimzaPolitikalari/XML_216792161015070331.xml

URL adreslerinden yayımlanır.

Yayınlanan politikaların en güncel versiyonuna, OID numarasından oluşan dosya isminin en sonunda yer alan versiyon bilgisinden erişilebilir.

2.4. Politikaların Güvenliği

http://www.eimza.gov.tr/EimzaPolitikalari/PDF_SHA256_216792161015070331.hash

URL adresinden bu dokümana ait SHA-256 özetleme algoritması kullanılarak oluşturulmuş özet değerine erişilebilir.

XML dosyalarının SHA-256 özetleme algoritması kullanılarak oluşturulan özet değerine ise dosyanın içinden erişilmesi mümkündür. XML dosyalarının özet değeri alınırken <signPolicyInfo> nodunun tamamının özet değerinin alınması gereklidir.

2.5. Politikaların Güncellenmesi

Elektronik imza politikaları güncellendiği tarihten itibaren eski versiyonun geçerliliği sona erer. Güncel politika dokümanlarının OID ve erişim adresleri

http://www.eimza.gov.tr/EimzaPolitikalari/GuncelPolitikalar.xml

URL adresinde yer alan XML dosyası içeriğinden elde edilebilir.

2.6. Politikaların Arşivlenmesi

Güncellenen politikaların eski versiyonları BTK tarafından arşivlenir ve arşivlenen eski versiyon dokümanlar ile bu dokümanlara ait özet değerler, belirtilen URL adresinden yayımlanmaya devam eder.

2.7. İletişim Bilgileri

Adres : Bilgi Teknolojileri ve İletişim Kurumu Yeşilırmak Sokak No:16
06430 Demirtepe/ANKARA

Tel : (312) 297 72 00

Faks : (312) 29471 45

URL : http://www.btk.gov.tr

3. Politikaların Uygulanması

3.1. İmzalayan Taraftaki İşlemler

CAdES ve XAdES tipinde imza oluşturan tarafın uygulamasında, bu politikalara ait

- Politikanın nesne tanımlama numarasının (OID),
- Bu dokümanda işaret edilen ilgili XML dosyasının SHA-256 özet değerinin,
- XML dosyasının erişileceği URL adresinin

imzalama işlemi sırasında imza dosyasının içeriğine, imzalı özellik olarak eklemesi gereklidir.

PAdES tipinde imza oluşturan tarafın uygulamasında ise, bu politikalara ait politikanın nesne tanımlama numarası (OID),

- Bu dokümanın SHA-256 özet değeri,
- Bu dokümanın erişileceği URL adresi

imzalama işlemi sırasında imza dosyasının içeriğine, imzalı özellik olarak eklenir[1].

Bu şekilde imza dosyası, ETSI TS 101 733 V1.8.1, ETSI TS 101 903 V1.4.2 ve ETSI TS 102 778-3 V1.2.1 ile ETSI TS 102 778-5 V1.1.2 dokümanlarında tanımlanan "Politikaları Açık Olarak Belirtilmiş Elektronik İmza (*Explicit Policy Electronic Signatures)* (EPES)" imza formatlarına göre oluşturulur. Böylece elektronik imzanın, bu dokümanda anlatılan şartlara uygun olarak oluşturulduğunun belirlenmesi sağlanmış olur.

3.2. İmzayı Doğrulayan Taraftaki İşlemler

Elektronik imzayı doğrulayan tarafın uygulamasının, imza dosyası içerisinde yer alan OID'ye bakarak imzanın hangi politikaya uygun olarak oluşturulduğunu tespit etmesi, ilgili XML dosyasını (PAdES için bu dokümanı) elde ederek özetini

[1] NOT: PAdES için tanımlanmış bir imza politikaları formatı standardı bulunmadığından dolayı PAdES imza politikaları için ayrı bir XML dosyası oluşturulmamıştır. Bu politikalara uygun oluşturulmak istenen PAdES tipi imzaların politikalara uygunluğunun sağlanması uygulamanın gerçekleştirimine bırakılmıştır.

çıkarması ve bu özet değeri imza dosyası içerisinde yer alan özet değer ile karşılaştırarak doğruluğundan emin olması gereklidir.

İmzayı doğrulayan tarafın uygulamasının, imzalı belgeyi işleme almadan önce imza doğrulama işlemlerini bu politikalara uygun olarak gerçekleştirmesi, bu politikalara uygun olarak oluşturulmayan imzaların ise doğrulamaması gereklidir. Aynı zamanda da imza doğrulama işlemini gerçekleştiren uygulamanın, imza politikasına ait OID'yi, özet değerini ve erişilebileceği URL adres bilgilerini doğrulamayı yapan kullanıcıya göstermesi zorunludur.

4. İmza Politikaları

4.1. Genel İmza Politikaları Bilgisi

4.1.1. İmza Politikaları Yayınlayan İsmi

Bilgi Teknolojileri ve İletişim Kurumu

4.1.2. İmza Politikaları Nesne Tanımlama Numarası

OID: 2.16.792.1.61.0.1.5070.3.3.1

Güvenli Elektronik İmza Oluşturma ve Doğrulama İlkeleri{ joint-iso-itu-t(2) ülke(16) tr(792) BTK (1.61.0.1) Elektronik İmza(5070) Güvenli Elektronik İmza Kullanım Profilleri (3) Politika-3 (3) SürümNo-1 (1) }

4.1.3. İmza Politikaları Geçerlilik Süresi

Geçerlilik Başlangıç Zamanı: 02 / 07 / 2012 Saat: 00:00

Geçerlilik Bitiş Zamanı: Bu doküman, geçerli olmadığı duyuruluncaya kadar geçerlidir.

Bu doküman, yukarıda belirtilen geçerlilik başlangıç ve bitiş tarihleri arasında oluşturulan elektronik imzalara uygulanır. Geçerlilik bitiş tarihinden sonra bu dokümana referans verilen imzalar, bu politika dokümanı kapsamında değerlendirilmez. Ancak geçerlilik süresi dolmadan önce bu dokümana uygun olarak oluşturana elektronik imzalar geçerliliğini korumaya devam eder.

4.1.4. Yayın Tarihi

Bu dokümanın yayın tarihi 02/07/2012 tarih ve 2012/DK-15/299 sayılı Kurul Kararının yayımlanma tarihidir.

4.1.5. Uygulama Alanı

Bu dokümanın uygulama alanı, NES iptal kontrollerini ÇİSDuP üzerinden yapan, zaman damgası alınabilen ve oluşturulan elektronik imzalı belgelerin imzada kullanılan NES'in kalan geçerlilik süresinden daha uzun bir süre saklanması gereken güvenli elektronik imza uygulamalarıdır.

4.2. Genel Kurallar (Common Rules)

4.2.1. İmzalayan Tarafla İlgili Kurallar

4.2.1.1. Ayrık veya Bitişik İmza Kullanımı

Elektronik imza oluşturulurken imzalan belgenin ve imzanın aynı ya da ayrı dosyalarda tutulmasına izin verilir. Ancak PAdES imzalarda imzanın ayrı dosyada tutulmasına izin verilmez.

4.2.1.2. Zorunlu Eklenen İmzalı Özellikler

İmzalayan tarafın, elektronik imzayı oluştururken Tablo 1'de belirtilen imzalı özellikleri

CAdES için ETSI TS 101 733 V1.8.1,

XAdES için ETSI TS 101 903 V1.4.2,

PAdES-CMS için ETSI TS 102 778-3 V1.2.1,

PAdES-XFA için ETSI TS 102 778-5 V1.1.2'in 5. bölümünde anlatıldığı şekilde imza dosyasına eklemesi gereklidir.

PDF içine gömülen imzalı XML dosyaları, ETSI TS 102 778-5 V1.1.2 dokümanının 4. Bölümü'nde anlatıldığı şekilde oluşturulmalı ve Tablo 1'deki XAdES için belirtilen özellikleri içermelidir.

Tablo- 1 Elektronik İmza Oluşturulurken Eklenecek İmzalı Özellikler

CAdES	XAdES
id-contentType OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)3 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat
id-messageDigest OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)4 }	/SignedInfo/Reference/DigestValue
id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) kcs(1) pkcs9(9) smime(16) id-aa(2) 47 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningCertificate
id-signingTime OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)5 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningTime
	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat/MimeType
id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1)pkcs9(9) smime(16) id-aa(2) 15 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SignaturePolicyIdentifier

PAdES-CMS	PAdES-XFA
id-contentType OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)3 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat
id-messageDigest OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs9(9)4 }	/SignedInfo/Reference/DigestValue
id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) kcs(1) pkcs9(9) smime(16) id-aa(2) 47 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SigningCertificate
M entry in the signature dictionary	CreateDate element defined within the XMP ns.adobe.com/xap/1.0/ namespace
-	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedDataObjectProperties/ DataObjectFormat/MimeType
id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1)pkcs9(9) smime(16) id-aa(2) 15 }	/Signature/Object/ QualifyingProperties/ SignedProperties/ SignedSignatureProperties/ SignaturePolicyIdentifier

NOT 1: SigningTime özelliği ile M entry ve CreateDate elementinin içeriğine kullanıcı makinasındaki sistem saatinden veya kurumdaki bir sunucudan alınan imzalama sırasındaki zaman bilgisi yazılır.

NOT 2: SigPolicyId / SignaturePolicyIdentifier alanına bu politika dokümana ait bilgiler yazılır.

4.2.1.3. Zorunlu Eklenen İmzasız Özellikler

İmzalayan taraf Tablo 2'de belirtilen imzasız özellikleri

- CAdES için ETSI TS 101 733 V1.8.1,
- XAdES için ETSI TS 101 903 V1.4.2,
- PAdES-CMS için ETSI TS 102 778-3 V1.2.1 ve ETSI TS 102 778-4 V1.1.2,
- PAdES-XFA için ETSI TS 102 778-5 V1.1.2'in 5. bölümünde anlatıldığı şekilde imza dosyasına eklemek zorundadır.

PDF içine gömülen imzalı XML dosyaları ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı şekilde oluşturulmalı ve

Tablo 2'deki XAdES için belirtilen özellikleri içermelidir.

Tablo-2 Zorunlu Eklenen İmzasız Özellikler

CAdES	XAdES
id-aa-signatureTimeStampToken OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 14}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ SignatureTimeStamp
id-aa-ets-certificateRefs OBJECT IDENTIFIER ::= {iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 21}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ CompleteCertificateRefs
id-aa-ets-revocationRefs OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 22}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ CompleteRevocationRefs

id-aa-ets-certValues OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 23}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ CertificatesValues
id-aa-ets-revocationValues OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 24}	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ RevocationValues
-	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ SigAndRefsTimeStamp

PAdES-CMS	PAdES-XFA
/Type/DocTimeStamp /SubFilter /ETSI.RFC3161	/Signature/Object/ QualifyingProperties/ UnSignedProperties/ UnsignedSignatureProperties/ SignatureTimeStamp
/DSS/Certs Array /DSS/VRI/Cert Array	/DSS/Certs Array /DSS/VRI/Cert Array
/DSS/CRLs Array /DSS/OCSPs Array /DSS/VRI/CRL Array /DSS/VRI/OCSP Array	/DSS/CRLs Array /DSS/OCSPs Array /DSS/VRI/CRL Array /DSS/VRI/OCSP Array

4.2.1.4. Zorunlu Eklenen Sertifika Referansları

İmzalayan kişiye ait NES'in referansının

- CAdES ve PAdES-CMS için signingCertificateV2,
- XAdES ve PAdES-XFA için SigningCertificate

imza özelliği olarak imza dosyasına eklenmesi zorunludur.

PDF içine gömülen imzalı XML dosyalarına NES'in referansı, ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı gibi XAdES için belirtilen şekilde eklenmesi gereklidir.

NES güven zincirindeki ESHS sertifikalarının referanslarının yukarıda belirtilen alanlara eklenmesi zorunlu değildir.

4.2.1.5. Zorunlu Eklenen Sertifikalar

İmzalayan kişiye ait NES'in

- CAdES ve PAdES-CMS için imza dosyasının SignedData içindeki certificates alanına,
- XAdES ve PAdES-XFA için Signature içindeki KeyInfo alanına

eklenmesi zorunludur.

PDF içine gömülen imzalı XML dosyalarına NES, ETSI TS 102 778-5 V1.1.2 dokümanının 4. bölümünde anlatıldığı gibi XAdES için belirtilen şekilde eklenmesi gereklidir.

NES güven zincirindeki ESHS sertifikalarının yukarıda belirtilen alanlara eklenmesi zorunlu değildir.

4.2.2. Doğrulayan Tarafla İlgili Kurallar

4.2.2.1. Zorunlu Eklenen İmzasız Özellikler

İmzayı doğrulayan taraf, imzalı belgeyi işleme almadan önce bu dokümanın 4.2.1.3. bölümünde belirtilen imzasız özellikler eklenmemişse, belirtilen tüm imzasız özellikleri imza dosyasına eklemek zorundadır.

4.2.3. Sertifikalar ile İlgili Kurallar

4.2.3.1. Sertifikaların Güvenilirliği ile İlgili Gereksinimler

5070 sayılı Elektronik İmza Kanunu ve ikincil düzenlemeler kapsamında BTK'ya bildirimde bulunarak Türkiye'de faaliyet göstermeye başlayan ESHS'lere ait kök güven zincirinden üretilmiş NES'lere güvenilir.

ESHS'lere ait tüm kök sertifikalara http://www.eimza.gov.tr/tr/kok internet adresinden erişilebilir.

Türkiye'de elektronik imza mevzuatı kapsamında faaliyet gösteren ESHS'lerin, NES'lere ilişkin yayınlamış oldukları politikalara güvenilir.

5070 sayılı Elektronik İmza Kanunu ve ilgili mevzuat ile

- Kök güven zincirinde kök ile NES arasında kaç adet ESHS alt kök sertifikası olması gerektiği,
- Sertifika politikaları ve
- Sertifikaların isim alanları

hususlarında bir düzenleme yapılmadığından herhangi bir sınırlama getirilmemiştir.

4.2.3.2. Sertifika İptal Kontrolleri ile İlgili Gereksinimler

NES iptal kontrollerinin ÇİSDuP'dan yapılması zorunludur. Sertifika güven zincirindeki ESHS'ye ait sertifikaların iptal kontrolleri SİL veya ÇİSDuP'dan birisi üzerinden yapılır.

4.2.4. Zaman Damgası ile İlgili Kurallar

4.2.4.1. Zaman Damgası Sertifikalarının Güvenilirliği ile İlgili Gereksinimler

Türkiye'de 5070 sayılı Elektronik İmza Kanunu ve ikincil düzenlemeler çerçevesinde BTK'ya bildirimde bulunarak faaliyete başlayan tüm ESHS'lere ait kök güven zincirinden üretilmiş zaman damgalarına güvenilir.

4.2.4.2. Zaman Damgası Sertifikalarının İptal Kontrolleri ile İlgili Gereksinimler

Zaman damgasını imzalayan ESHS sertifikası ile bu sertifikanın içinde bulunduğu sertifika, güven zincirindeki ESHS'ye ait sertifikaların iptal kontrolleri SİL veya ÇİSDuP'dan birisi üzerinden yapılır.

4.2.4.3. Kesinleşme Süresi

Zaman damgası alındıktan sonra kesinleşme süresi uygulanmaz. Zaman damgası alındıktan sonra NES, zaman damgası sertifikası ve sertifika güven zincirindeki tüm ESHS sertifikalarının geçerlilik kontrolleri yapılarak sertifika doğrulama işlemleri kesinleştirilir. Sertifikaların geçerlilik kontrolleri yapılırken zaman damgası üzerindeki zaman bilgisi referans alınır. Sertifikaların zaman damgası alındığı tarihte geçerlilik süresi içinde olmaması veya iptal konumunda olması imzanın geçersiz kabul edilmesine sebep olur. İmzaya dahil olmayan imza özellikleri sertifika geçerlilik kontrolleri sonunda imza dosyasına eklenir.

4.2.4.4. Zaman Damgası Gecikme Süresi

Zaman damgası, imza sahibi tarafından eklenen signingTime özelliği ile M entry veya CreateDate elementinin içeriğinde belirtilen imza zamanından en geç 2 saat sonra alınmalıdır.

4.2.5. Yetkiler ile İlgili Kurallar

Bu politika dokümanında yetkilendirmeler ile ilgili kurallar belirlenmemiştir.

4.2.6. Kullanılan Algoritmalar ile İlgili Kısıtlamalar

Güvenli elektronik imza oluşturma için kullanılabilecek algoritmalar, BTK tarafından yayınlanan "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"de belirlendiğinden bu politika dokümanında algoritma kısıtları ile ilgili kurallara yer verilmemiştir. Türkiye'de elektronik imza mevzuatı ile belirlenen algoritmaların kullanılması zorunludur.

4.3. İmza Amacı ile İlgili Kurallar (Commitment Rules)

Bu politika dokümanında imza amacı ile ilgili kurallar belirlenmemiştir.

verilmemiştir.

REFERANSLAR

[1] Elektronik İmza Kullanım Profilleri, Sürüm 1.0, 1 Ekim 2011, TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi.

[2] ETSI TR 102 041: Signature Policies Report

[3] ETSI TR 102 272: Electronic Signatures and Infrastructures (ESI); ASN.1 Format for Signature Policies

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

[5] ETSI TR 102 038: TC Security - Electronic Signatures and Infrastructures (ESI); XML Format for Signature Policies

[6] ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

[7] ETSI TS 102 778-3: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

[8] ETSI TS 102 778-4: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile.

[9] ETSI TS 102 778-5: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES Signatures.