TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

YENİ NESİL ÖKC SAYISAL SERTİFİKA YAŞAM DÖNGÜSÜ

Doküman Kodu
REH.01.03

Revizyon No
03

Revizyon Tarihi
20.06.2018

TASNİF DIŞI

YENİ NESİL ÖKC SAYISAL SERTİFİKA YAŞAM DÖNGÜSÜ

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
01	İlk çıkış.	01.07.2015
02	Doküman yeni şablona aktarılmıştır. Dokümanın eski revizyonları Kamu SM doküman yönetim sisteminde REHB-001-012 kodu ile yer almaktadır.	28.05.2018
03	İmla hataları düzeltilmiştir.	20.06.2018

Şekiller Listesi

Tablolar Listesi

İÇİNDEKİLER

1 Amaç ve Kapsam

Bu dokümanın amacı, Cihaz'ların güvenli haberleşmesinde kullanılacak sayısal sertifikaların Cihaz üreticileri tarafından TÜBİTAK BİLGEM Kamu SM'den talep edilmesi, bu sertifikaların Kamu SM tarafından oluşturulması, güvenli olarak Cihaz üreticisine gönderilmesi ve iptal edilmesi süreçlerinin ayrıntılı olarak anlatılmasıdır.

2 Tanımlar

Cihaz:	Mükellefe ait mali verileri elektronik ortamda güvenli olarak ileten Yeni Nesil Ödeme Kaydedici Cihazı
CMS:	RFC 3852'de yer alan, imzalama ve şifreleme için tanımlanmış Kriptografik Veri Biçimi standardı
CMS Envelope:	CMS standardında tanımlanmış şifreli veri yapısı
GİB:	Gelirler İdaresi Başkanlığı
Güvenli Oda:	Dışarısı ile etkileşimi engellenmiş ve erişimleri kontrol altında tutulan alan
İmzager:	TÜBİTAK BİLGEM tarafından geliştirilen ve elektronik imza oluşturmak için kullanılan yazılım
Kamu SM:	TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) bünyesinde elektronik sertifika hizmet sağlayıcısı olarak kurulmuş olan Kamu Sertifikasyon Merkezi
PFX:	PKCS#12 standardında tanımlanmış dosya biçimi
PKCS#12:	X.509 sertifikasıyla gizli/özel anahtarın elektronik ortamda güvenli olarak saklanması ve dağıtılması için tanımlanmış dosya biçimi standardı
Sertifika Talep Yetkilisi:	Cihaz üreticisi adına Kamu SM'den sertifika talebinde bulunabilecek kişi
Sertifika Talep Yetkilisi İmzalama Sertifikası:	Sertifika Talep Yetkilisi'nin Kamu SM'den sertifika talebinde bulunurken dosyaları imzalamak için kullanılacağı sertifika
Sertifika Yükleme Yetkilisi:	Cihaz üreticisi adına Kamu SM'den alınan sertifikaları Cihaz'lara yükleyecek kişi
Sertifika Yükleme Yetkilisi Şifreleme Sertifikası:	Cihaz üreticisine iletilecek PFX dosyalarının Kamu SM tarafından şifrelenmesinde ve Sertifika Yükleme Yetkilisi tarafından şifresinin çözülmesinde kullanılacak sertifika
TSM:	Üretici firmanın Cihaz'ları kontrol ettiği merkez

3 Sistemde Tanımlı Sertifikalar

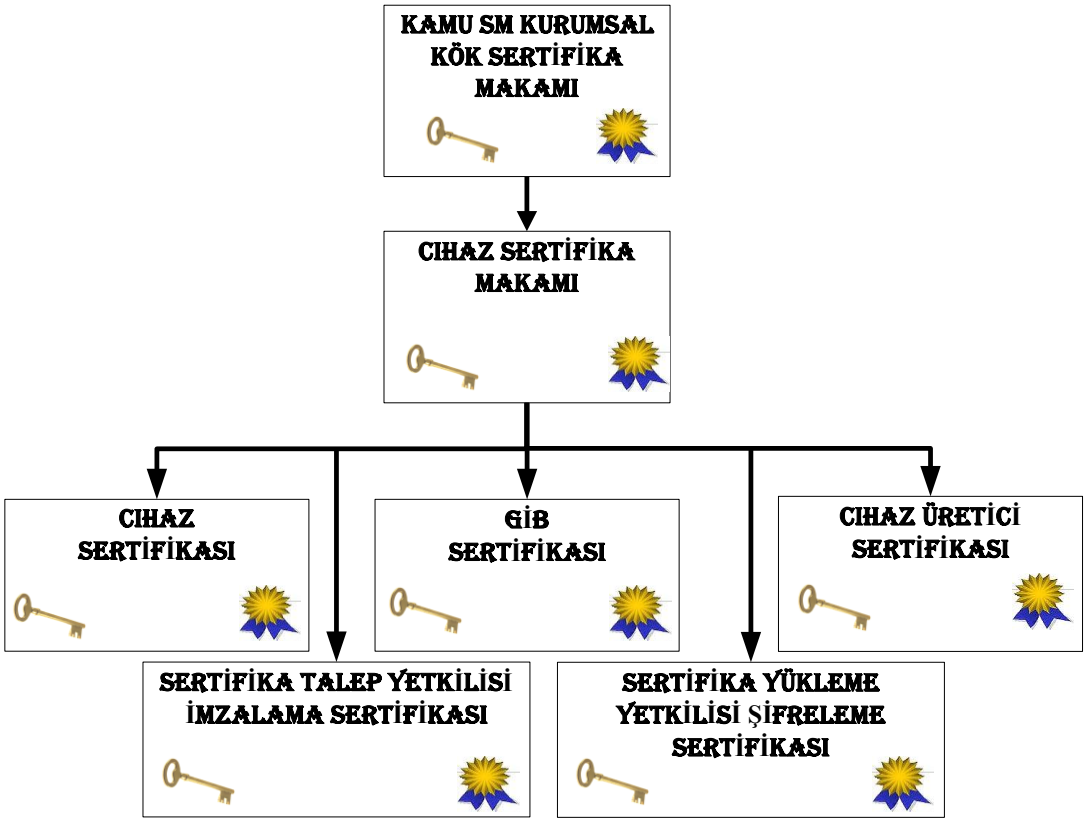
Dokümanda geçen kavramların tanımlamaları burada yapılmalıdır. Varsa kısaltmalar, açılımlarıyla beraber belirtilmelidir.

Sistemde kullanılacak sertifikalar **Error! Reference source not found.**'de, kurumlarla ilişkileri ise

'de verilmiştir.

Cihaz Sertifikası	Cihaz'ın kimliğini doğrulayan ve güvenli haberleşmesini sağlayan sertifikadır.
GİB Sertifikası	GİB kimliğini doğrulayan ve güvenli haberleşmesini sağlayan sertifikadır.
Cihaz Üretici Sertifikası	Cihaz üreticisine ait TSM'nin kimliğini doğrulayan ve güvenli haberleşmesini sağlayan sertifikadır.
Sertifika Yükleme Yetkilisi Şifreleme Sertifikası	PFX dosyalarının Kamu SM tarafından Sertifika Yükleme Yetkilisi için şifrelenmesinde ve Sertifika Yükleme Yetkilisi tarafından şifresinin çözülmesinde kullanılacak sertifikadır.
Sertifika Talep Yetkilisi İmzalama Sertifikası	Sertifika Talep Yetkilisi'nin Kamu SM'den sertifika talebinde bulunurken talep dosyalarını imzalamak için kullanacağı sertifikadır.
Test Sertifikaları	Cihaz üreticilerinin cihazı geliştirirken kullanacakları Cihaz sertifikalarıdır. Soft ve kartlı olarak üretilebilmektedir.

Tablo 1: Sistemde Kullanılacak Sertifikalar



Şekil 1: Anahtar ve Sertifikalar

4 Sertifikaların Talep Edilmesi

BİLGEM tarafından yapılacak gerekli denetimlerden (Cihaz'ların Yeni Nesil ÖKC Teknik Kılavuzu'nda belirtilen şartlara uyumluluk denetimi ve soft sertifikaların Cihaz'lara yükleneceği Güvenli Alan'ın Yeni Nesil ÖKC Sayısal Sertifika Koruma Kılavuzu'nda belirtilen şartlara uyumluluk denetimi) geçmiş, GİB tarafından onaylanmış ve onay yazısı Kamu SM'ye gönderilmiş Cihaz(lar) için Cihaz üreticileri, Kamu SM'den sertifika talebinde bulunabilecektir. Kamu SM'den sertifika talep edecek Cihaz üreticisi; firma bilgileri ile Sertifika Talep Yetkilisi ve soft sertifikalar için Sertifika Yükleme Yetkilisi olarak atanacak bir/birkaç kişinin bilgilerini Kamu SM'ye bildirecektir. Kamu SM ve Sertifika Talep Yetkilisi arasındaki haberleşme elektronik ortamda ve e-imzalı olarak yapılacağı için Sertifika Talep Yetkilisi'nin İmzalama Sertifikası sahibi olması gerekmektedir. Sertifika Talep Yetkilisi'nin, İmzalama Sertifikası'nı Kamu SM'den edinmesi ve ayrıca http://yazılım.kamusm.gov.tr adresinden ücretsiz sağlanacak olan İmzager yazılımını kullanması gerekmektedir. Sertifika Talep Yetkilisi, sertifika talep formunu İmzager ile imzalayıp Kamu SM'ye elektronik olarak iletecektir.

Sertifika Talep Yetkilisi tarafından doldurulmuş ve İmzager ile imzalanmış olarak Kamu SM'ye iletilen sertifika talep formu, Kamu SM'de ilgili kişiler tarafından incelenecektir. Sertifika talep formunda sertifikalandırılacak Cihaz'ın seri numarası ve sertifika tipi (soft/kartlı) belirtilmek zorundadır. Formdaki bilgiler ve imza kontrol edildikten sonra eksik veya yanlış bilgi varsa Sertifika Talep Yetkilisi e-posta yoluyla bilgilendirilecektir.

Kamu SM, sertifika talep formu bulunmayan veya ilgili form bulunmasına karşın bilgilerde eksiklik ve/veya formda tahrifat bulunan ya da imza bulunmayan vb. durumlarda sertifika üretimini gerçekleştirmeyecektir.

5 Sertifika Üretim Süreci ve Müşteriye Teslimi

5.1 Sertifika Üretimi

Sertifikalar, Sertifika Talep Yetkilisi tarafından sertifika talep formunun tam ve doğru bir şekilde Kamu SM'ye iletilmesinin ardından talebe göre soft veya kartlı olarak üretilecektir.

5.2 Sertifika Üretimi ve Elektronik Ortamda Teslimi

Cihaz'lar için üretilen soft sertifikalar, pfx (PKCS#12) formatında üretilecektir. Her bir Cihaz için bir adet pfx dosyası oluşturulacak ve pfx dosya içeriğinde özel-açık anahtar çifti ve sertifika bulunacaktır.

Pfx dosya adı ***<ÜreticiFirmaKodu><CihazSeriNo><@ÜreticiFirmaAdı>_<pfxParola>.pfx*** şeklinde olacaktır. Oluşturulan pfx dosyalarının her biri ayrı ayrı Sertifika Yükleme Yetkilisi/Yetkilileri Şifreleme Sertifikası ile şifrelenerek sftp protokolü ile Cihaz üreticisine gönderilecektir. Sertifika Yükleme Yetkilisi/Yetkilileri, Cihaz sertifikalarını Cihaz'a yüklemeden önce şifreli olan pfx dosyasının şifresini çözecek ve sonra pfx dosyasını Cihaz'a yükleyecektir.

Pfx dosyalarının her biri, ilgili Sertifika Yükleme Yetkilisi'nin/Yetkilileri'nin şifreleme sertifikası kullanılarak RFC 3852'de belirtilen CMS Envelope formatında şifrelenecektir. Şifreli dosyaların şifresinin çözülebilmesi için Cihaz üreticilerine ücretsiz yazılım, Kamu SM tarafından sağlanacaktır.

5.3 Akıllı Kartta Üretim ve Teslim

Cihaz'lar için üretilen sertifikalar akıllı kartlara yüklendikten sonra, akıllı kartlar ilgili üretici firmaya kurye aracılığıyla teslim edilecektir.

6 Aynı Cihaz İçin Yeniden Sertifika Üretilmesi

Cihaz sertifikasının silinmesi/bozulması gibi sertifikanın kullanılamaz hale geldiği durumlarda Cihaz'a yeni bir sertifikanın yüklenmesi gerekmektedir.

Sertifikanın akıllı karta yüklü olarak verildiği bir Cihaz'a yeni bir sertifikanın yüklenmesi söz konusu olduğunda, Kamu SM tarafından Cihaz için yeni bir sertifika üretilecek ve yeni bir akıllı karta yüklenerek üretici firmaya kurye ile gönderilecektir.

Sertifikanın soft olarak yüklendiği bir Cihaz'a sertifikanın yeniden yüklenmesi söz konusu olduğunda ise Cihaz için yeni bir sertifika üretilecek ve şifrelenerek üretici firmaya sftp ortamında iletilecektir.

Soft olarak Cihaz üretici firmaya ulaştırılan yeni sertifika Cihaz'a Güvenli Alan'da yüklenecektir. Soft Sertifika, Güvenli Alan dışında Cihaz'a yüklenmeyecektir.

7 Sertifikaların İptal Edilmesi

Cihaz'lar için üretilecek sertifikanın geçerlilik süresi Cihaz'ın geçerlilik süresi ile aynı olacaktır. Fakat bir mükellefin ticari faaliyetlerini sonlandırması, Cihaz'ın tamir edilemeyecek şekilde arızalanması, sertifikanın herhangi bir sebepten ötürü silinmesi ya da kullanılamayacak hale gelmesi, sertifikanın güvenilirliğinin yitirilmesi gibi durumlarda sertifikanın kötüye kullanılmasının engellenmesi için ivedi olarak iptal edilmesi gerekmektedir.

Cihaz sertifikasının iptal edilmesi gerektiği durumlarda, bu Cihaz'ın seri numarasını, GİB ya da üretici firma Kamu SM'ye bildirecek ve Kamu SM bu sertifikayı derhal iptal edecektir. Böylelikle bu sertifika, sertifika iptal listesine girecektir ve bilinçli veya bilinçsiz olarak kötüye kullanımın önüne geçilecektir. Kamu SM'ye bildirim, e-imzalı olarak yapılacaktır. Bu bildirimlerde gerekli kimlik doğrulama işlemleri yapıldıktan sonra sertifika iptal edilecektir.

8 Sertifikaların Amacı Dışında Kullanımı

Üreticilere teslim edilen sertifikaların amacı dışında kullanılması durumunda oluşacak olumsuz duruma neden olan kişi veya cihaz üreticisinin tespit edilebilmesi amacıyla Kamu SM ürettiği sertifikalara ait kayıtları tutacaktır. Gerektiği durumda bu bilgileri GİB ve adli kurumlarla paylaşacaktır. Cihaz üreticileri, aldıkları sertifikaların güvenli olarak kullanılmasından sorumludur.

9 Diğer Sertifikalar

Sertifika Talep Yetkilisi İmzalama Sertifikalarını ve Sertifika Yükleme Yetkilisi Şifreleme Sertifikalarını Kamu SM üretecektir. Bu sertifikaların her biri akıllı karta yazılarak ilgili Sertifika Talep/Yükleme Yetkilisi'ne teslim edilecektir.

GİB Sertifikaları ve Cihaz Üretici Sertifikaları da, Kamu SM tarafından üretilecektir. Bu sertifikaların üretilebilmesi için GİB ve Cihaz üreticileri kullanacakları HSM'lerinde anahtar çiftlerini ve bu anahtarlardan pkcs#10 istek dosyalarını oluşturacaklar ve Kamu SM'ye ileteceklerdir. Kamu SM bu istek dosyalarını işleyerek sertifikalarını oluşturacak, GİB ve Cihaz üreticilerine iletecektir.